Vehicle Immobilization Technologies: Best Practices for Industry and Law Enforcement

Final Report

U.S. Department of Transportation
Federal Motor Carrier Safety Administration

November 2007

FOREWORD

This study focused on the development of "best practices" associated with the use of Vehicle Immobilization Technologies (VITs) in support of hazardous material (hazmat) transportation, and commercial vehicle safety and security. A secondary objective was to develop a Concept of Operations for law enforcement based on project experiences.

The work performed under the project included:

- Conducting an extensive survey of VITs developers and vendors in both United States and Canada, including visits to several companies and organizations.
- Developing a database with VIT vendor and technical information (included in the companion CD).
- Interacting with organizations and stakeholders involved with previous VIT testing and evaluation, including law-enforcement, carriers, and industry organizations.
- Conducting demonstration tests, at a test track facility in South Carolina, of these technologies, including driver authentication, vehicle shutdown technologies, and others. (Two companion DVDs containing videos that summarize these demonstration tests are included with this report.)
- Conducting a VIT Stakeholder Workshop at the March 2007 Commercial Vehicle Safety Alliance conference (CVSA), followed by two industry-related and two law enforcement-related webinars.
- Performing three case studies involving current users of these technologies: one large high-value carrier, one large and one small hazmat carriers, and interviewing an insurance brokerage company providing services to the commercial vehicle transportation industry.

NOTICE

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or the use thereof.

The contents of this Report reflect the views of the contractor, who is responsible for the accuracy of the data presented herein. The contents do not necessarily reflect the official policy of the Department of Transportation.

This Report does not constitute a standard, specification, or regulation.

The United States Government does not endorse products or manufacturers named herein. Trade or manufacturers' names appear herein only because they are considered essential to the objective of this document.

Technical Report Documentation Page

1. Report No. **FMCSA-RRT-07-021**	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle

Vehicle Immobilization Technologies: Best Practices for Industry and Law Enforcement

5. Report Date

November 2007

6. Performing Organization Code

7. Author(s)

Oscar Franzese (ORNL), Helmut Knee (ORNL), Thomas Urbanik (UTK), Joseph Massimini (Purdue University), Randall Plate (ORISE)

8. Performing Organization Report No.

9. Performing Organization Name and Address

Oak Ridge National Laboratory
Bethel Valley Rd, Oak Ridge, TN 37831

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTMC7503-X-0047

12. Sponsoring Agency Name and Address

Department of Transportation
Federal Motor Carrier Safety Administration
Office of Research and Analysis
1200 New Jersey Ave. SE, Room 600 West
Washington, DC 20590

13. Type of Report and Period Covered

Final Report, May 2006 – September 2007

14. Sponsoring Agency Code

FMCSA

15. Supplementary Notes

This program was administered through the Federal Motor Carrier Safety Administration (FMCSA). The FMCSA Program Manager is Joseph DeLorenzo, HM Program Manager, FMCSA Midwestern Service Center.

16. Abstract

Since September 11, 2001, the U.S. Department of Transportation's FMCSA has been actively investigating methods to improve safety and security, as well as efficiency, in the trucking industry. To achieve these goals, FMCSA conducted various tests and evaluations of security technologies, including the 2004 Hazardous Materials Safety and Security Technology Operational Test, the Expanded Satellite Tracking, and the Untethered Trailer Tracking and Control Security projects. As a result of these studies, it was determined that additional technologies, including panic buttons, driver identification, and vehicle disabling could be deployed to obtain additional security benefits. In FY 2005, the House of Representatives Conference Report 108-792 stated that further testing of technologies, including vehicle disabling was necessary. FMCSA funded this project to support the Congressional need called out in the aforementioned report, and built it on the experience and lessons learned from previous field operational tests. The primary objective of this project was to develop "Best Practices" associated with the use of Vehicle Immobilization Technologies (VITs) in support of hazmat transportation, and commercial vehicle safety and security. A secondary objective was to develop a Concept of Operations for law enforcement based on project experiences. Conclusions from this study suggest that VITs are currently being used by early adopters in the trucking industry for the security of high-value goods and for the protection of drivers against theft and hijacking. Driver Authentication Technologies were shown to be the first and most important line of defense to improve security and are being deployed rapidly. In terms of best practices, several items were clearly shown to be key elements of an effective system to improve security, including prioritization of security-related messages from wireless communications systems, company protocols involving law enforcement in a vehicle shutdown, and smart vehicle immobilization technology that can act in accordance with surrounding conditions.

17. Key Words

Remote Vehicle Shutdown, Remote Vehicle Disablement, Driver Authentication Technologies

18. Distribution Statement

No restrictions

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	**Unclassified**	**161**	**N/A**

SI* (MODERN METRIC) CONVERSION FACTORS

APPROXIMATE CONVERSIONS TO SI UNITS					APPROXIMATE CONVERSIONS FROM SI UNITS				
Symbol	When You Know	Multiply By	To Find	Symbol	Symbol	When You Know	Multiply By	To Find	Symbol
		LENGTH					LENGTH		
in	inches	25.4	millimeters	mm	mm	millimeters	0.039	inches	in
ft	feet	0.305	meters	m	m	meters	3.28	feet	ft
yd	yards	0.914	meters	m	m	meters	1.09	yards	yd
mi	miles	1.61	kilometers	km	km	kilometers	0.621	miles	mi
		AREA					AREA		
in^{2}	square inches	645.2	square millimeters	mm^{2}	mm^{2}	square millimeters	0.0016	square inches	in^{2}
ft^{2}	square feet	0.093	square meters	m^{2}	m^{2}	square meters	10.764	square feet	ft^{2}
yd^{2}	square yards	0.836	square meters	m^{2}	m^{2}	square meters	1.195	square yards	yd^{2}
ac	acres	0.405	hectares	ha	ha	hectares	2.47	acres	ac
mi^{2}	square miles	2.59	square kilometers	km^{2}	km^{2}	square kilometers	0.386	square miles	mi^{2}
		VOLUME					VOLUME		
fl oz	fluid ounces	29.57	milliliters	ml	ml	milliliters	0.034	fluid ounces	fl oz
gal	gallons	3.785	liters	l	l	liters	0.264	gallons	gal
ft^{3}	cubic feet	0.028	cubic meters	m^{3}	m^{3}	cubic meters	35.71	cubic feet	ft^{3}
yd^{3}	cubic yards	0.765	cubic meters	m^{3}	m^{3}	cubic meters	1.307	cubic yards	yd^{3}
		MASS					MASS		
oz	ounces	28.35	grams	g	g	grams	0.035	ounces	oz
lb	pounds	0.454	kilograms	kg	kg	kilograms	2.202	pounds	lb
T	short tons (2,000 lbs)	0.907	megagrams	Mg	Mg	megagrams	1.103	short tons (2,000 lbs)	T
		TEMPERATURE (exact)					TEMPERATURE (exact)		
°F	Fahrenheit temperature	5(F-32)/9 or (F-32)/1.8	Celsius temperature	°C	°C	Celsius temperature	1.8 C + 32	Fahrenheit temperature	°F
		ILLUMINATION					ILLUMINATION		
fc	foot-candles	10.76	lux	lx	lx	lux	0.0929	foot-candles	fc
fl	foot-lamberts	3.426	candela/m2	cd/m2	cd/m2	candela/m2	0.2919	foot-lamberts	fl
		FORCE and PRESSURE or STRESS					FORCE and PRESSURE or STRESS		
lbf	pound-force	4.45	newtons	N	N	newtons	0.225	pound-force	lbf
psi	pound-force per square inch	6.89	kilopascals	kPa	kPa	kilopascals	0.145	pound-force per square inch	psi

*** SI is the symbol for the International System of Units. Appropriate rounding should be done to comply with Section 4 of ASTM E380.**

ACKNOWLEDGEMENTS

This project was sponsored by the Federal Motor Carrier Safety Administration (FMCSA) and the Tennessee Department of Safety (TDOS). The authors would like to thank Lt. Colonel Strawther, Capt. Binkley, and Lt. Robinson from TDOS for their valuable contributions in developing the Law Enforcement Concept of Operations.

FMCSA and the authors wish to gratefully acknowledge the contributions of all the companies that participated in the demonstration tests: Satellite Security Systems, Blue Bird Body Company, Qualcomm, MAGTEC, Celadon Trucking, International Truck and Engine/NAVISTAR, BSM Wireless, GlenHugh Enterprise, and Archetype. Their contributions of equipment, work force, and personal support made this formidable project a success. The authors also wish to thank the South Carolina Department of Public Safety; their participation added realism to the demonstration tests. The help provided by Mr. Gary Capps and Ms. Sheila Moore of Oak Ridge National Laboratory (ORNL) during the demonstration tests was invaluable to the success of the project.

Lastly, the authors would also like to thank all the other companies that participated in this project, the Commercial Vehicle Safety Alliance (CVSA) Hazmat and Transportation Security Committees, all the stakeholders that gave their time and input to this project, in particular, Dr. John Conley with the National Tank Truck Carriers Association, and Ms. Sheila Moore and Ms. Teresa Ferguson (ORNL) for the assistance provided during and after the CVSA Workshop.

The Law Enforcement Concept of Operation section of this report was authored by Dr. Thomas Urbanik, University of Tennessee at Knoxville; Appendix A was authored by Mr. Joseph Massimini, Purdue University; and Mr. Randall Plate, ORISE, contributed to the development of Appendix D.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

ACS	Acceleration Control System
AQ	Answered Questionnaire
AW	Automotive Wireless
ATA	American Trucking Associations
BB	Blue Bird Body Company
CHP	California Highway Patrol
COO	Concept of Operation
CVIEW	Commercial Vehicle Information Exchange Window
CVO	Commercial Vehicle Operations
CVSA	Commercial Vehicle Safety Alliance
DT	Demonstration Tests
DAT	Driver Authentication Technologies
DOT	Department of Transportation
EA	Eureka Aerospace
EER	Equal Error Rate
eVID	Electronic Vehicle Immobilization Device
FAR	False Acceptance Rate
FMCSA	Federal Motor Carrier Safety Administration
FOT	Field Operational Testing
FR	Functional Requirement
FRR	False Rejection Rate
GHE	GlenHugh Enterprise
GL	Global Log-in
GPS	Global Positioning System
GVWR	Gross Vehicle Weight Rating
HPEMS	High-Power Electromagnetic System for Stopping Vehicles
LED	Light Emitting Diode
LLNL	Lawrence Livermore National Laboratory
LPG	Laurens Proving Grounds
MCSAP	Motor Carrier Safety Assistance Program
MOPS	Measures of Performance
MSC	Monitoring and Support Center
NCIC	National Crime Information Center
NDA	Non-Disclosure Agreement
OEM	Original Equipment Manufacturer
OR	Owner Representative
ORNL	Oak Ridge National Laboratory
PSAP	Public Safety Answering Point
RFID	Radio Frequency Identification
S3	Satellite Security Systems
SD	Shutdown
SOS	Semi Onboard Shutdown
SQ	Submitted Questionnaire
ST	Safefreight Technology

TDOS	Tennessee Department of Safety
TI	Teleconference Interview
TMC	Technology and Maintenance Council
TSA	Transportation Security Administration
UIP	Unattended Idle Protect
UTK	University of Tennessee at Knoxville
UVW	Unloaded Vehicle Weight
VCC	Vehicle Command and Control
VDT	Vehicle Disabling Technologies
VO	Vehicle Owner
VIN	Vehicle Identification Number
VIT	Vehicle Immobilization Technology
VST	Vehicle Shutdown Technologies
VV	Visited Vendor
WM	Wireless Matrix

EXECUTIVE SUMMARY

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

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

- March 31, 2002: A 29-year-old driver for a propane distributor drove away with a 3,000-gallon bobtail. He made a telephone threat stating that he wanted to kill President George W. Bush and that he would use the bobtail as a "bomb".
- April 11, 2002: A terrorist driving a truck carrying liquefied natural gas ignited his cargo in front of a synagogue on the Tunisian Island of Djerba, killing 17 people, mainly German and French tourists. Al Qaeda claimed responsibility for the blast.
- May 16, 2002: A tractor-trailer carrying 10 tons of deadly cyanide in 96 drums was stolen after three armed men held up the vehicle north of Mexico City. Six drums were never found.
- May 2002: A fully loaded tanker truck pulled into Israel's largest fuel depot and suddenly caught fire due to an explosive charge connected to a cellular phone. The fire was extinguished, but had the truck exploded, destruction and death would have resulted.

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

FMCSA embarked on a program to improve HAZMAT security and safety by using regulatory measures, security assessments, and outreach efforts. Part of this effort was to sponsor an industry competitive procurement to conduct a national level field operational test (FOT). This resulted in FMCSA awarding a contract for a team led by the Battelle Memorial Institute (Battelle) (Deployment Team) to test currently existing major technologies that could offer solutions to minimize security risks of truck-based HAZMAT shipments. Supporting Deployment Team members included: QUALCOMM; the American Transportation Research Institute (ATRI); the Commercial Vehicle Safety Alliance (CVSA); Savi Technologies; the Biometrics Solutions Group (BSG); Total Security-US; and the Spill Center.

To evaluate the technologies tested in this FOT; their costs, benefits, and the operational processes required to be performed, the FMCSA, supported by the Intelligent Transportation Systems (ITS)/Joint Program Office (JPO), awarded an independent evaluation contract in August 2002. Science Applications International Corporation (SAIC) (Evaluation Team) led the independent evaluation for this HAZMAT FOT.

Overview of the Field Operational Test

This Hazardous Materials Safety and Security Technology Field Operational Test was focused on four different HAZMAT truck transportation scenarios representing the following industry segments:

- Bulk Petroleum
- Bulk Chemical
- Less-than-Truckload (LTL)
- Truckload Explosives industries

The scenarios were chosen based on the results of a hazardous materials risk and threat assessment that was conducted in the initial phase of this project by the Deployment Team, and was combined with a desire to test the technology in different types of industry. The risk and threat assessment methodology was used to identify the types of materials that were of highest concern, as well as the most likely attack scenarios (***theft*** of a material, ***interception/diversion***, and ***legal exploitation***). Specific vulnerabilities were also identified during this phase of the project, which served as the basis for selecting the technologies within each scenario.

As detailed in Table 1 on page 10, a wide variety of existing technologies were tested within each scenario. These technologies were integrated based on meeting specific functional requirements that FMSCA had set for the Deployment Team contract.[1] FMCSA also stipulated that these would need to be commercial off-the-shelf (COTS) technologies, such that they could conceivably be implemented rapidly by the motor carrier industry in the very near future.

The technologies were grouped together into several packages within each scenario. The grouping assisted in addressing the wide range of vulnerabilities identified in the risk/threat assessment, and for testing several different cost tiers reflecting a range of carrier deployment options based on market conditions. Based on this premise, the various technology components were separated into six technology tiers, ranging from a low-end cost of approximately **$800** per vehicle to a high-end of approximately **$3,500** per vehicle.

The technologies were matched to testing scenarios, which were developed to address the functional requirements and the threats and vulnerabilities identified in the Threat/Risk Assessment. With the overall goal of the FOT being to test technologies installed in 100 vehicles, each scenario tested a total of **25 vehicles**, with various combinations of technology installed on each vehicle. Table 2, on page 13, provides a summary of each scenario and the technology components to be tested by scenario.

1. INTRODUCTION

Since September 11, 2001, the U.S. Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA) has been actively investigating methods to improve safety and security, as well as efficiency, in the trucking industry. In order to achieve these goals, FMCSA has conducted various tests and evaluations of security technologies. The purpose of the 2004 Hazardous Materials Safety and Security Technology Field Operational Test (FMCSA, 2004a; 2004b; 2004c) was the quantification of the security costs and benefits of an operational concept that applies technology and improves enforcement procedures to hazardous materials (hazmat) transportation. Subsequently, FMCSA undertook the Expanded Satellite Tracking (FMCSA, 2006) and the Untethered Trailer Tracking and Control Security (FMCSA, 2005) projects. These projects used wireless communication systems with position tracking as the base technology and included the wireless transmission of tracking data to law enforcement and emergency responders, in addition to the carrier. It was determined that additional technologies, including panic buttons, driver identification, and vehicle disabling could be built onto the wireless communication system to obtain additional security benefits. In FY 2005, the House of Representatives Conference Report 108-792 (U.S. House, 2004) stated that further testing of technologies, including vehicle disabling, was necessary.

This Vehicle Immobilization Technology (VIT) Evaluation Project was conducted to support the Congressional need called out in the aforementioned report and was built on the experience and lessons learned from previous field operational tests. To that end, the Oak Ridge National Laboratory (ORNL), in partnership with the University of Tennessee at Knoxville (UTK) and the Tennessee Department of Safety (TDOS), conducted an assessment and demonstration testing of VITs for application to commercial vehicle hazmat transport in support of the FMCSA's goal of continued improvement of safety, security, and efficiency.

The high-level approach taken to conduct this study focused mainly on how the VITs are being deployed and used by the motor carrier industry. To that end, the project first identified technology providers that commercially offered hardware and services (i.e., technologies that were readily available) and that satisfied at least one of the five VIT functional requirements that were identified by FMCSA in previous studies. A wide variation of technologies and approaches to vehicle disablement and vehicle shutdown were identified and served as the basis to compile a preliminary list of "best practices." as well as other issues involved in the deployment and usage of VITs. These preliminary "best practices" and VIT issues were further discussed in different forums (e.g., the 2007 Commercial Vehicle Safety Alliance Conference, several industry and law-enforcement-focused webinars, and discussions with both large and small trucking companies) in an attempt to capture the perspectives of the primary VIT stakeholders. Those "best practices" also played a critical role in the development of a concept of operation (COO) for law enforcement application of VITs, which was developed by UTK in close collaboration with the Tennessee Department of Safety.

Section 2 of this report presents a discussion of the different VITs that are currently commercially available and also includes a few that are in the development stage. The section starts with a discussion of the components of a VIT system and their interactions, and continues with specific descriptions of the different technologies surveyed, touching on issues such as cost, installation, and maintenance, among others.

Section 3 focuses on the vehicle disabling and vehicle shutdown tests that were conducted as part of this project. This is a technical section that presents the different driver authentication technologies that were demonstrated by the participating vendors and discusses Vehicle Shutdown Technology (VST) parameters, such as the elapsed times between the instant the order to shutdown the vehicle was given and the time the vehicle came to a stop. The section also presents speed profiles of the test vehicles obtained while they were in the shutdown process. All of the demonstration tests were videotaped and are included in a companion DVD, with software that permits the user to see, in a dynamic way, the speed profiles and trajectories of the demonstration vehicles that participated in the VST tests. Also included is a copy of the VIT information database that includes data and information on all of the vendors that participated in this project (the ones that participated in the demonstration tests as well as many others) and that completed a survey about their technologies and systems.

In Section 4, the real-world experiences in the deployment and usage of VITs by large and small trucking companies are presented. Those include a large (3000+ trucks), high-value carrier, and two hazmat transportation companies: one large and one small. The section also includes a discussion with a large commercial insurance brokerage firm, providing risk management services, insurance, and bonds to commercial clients, including the transportation industry.

All of the information collected in Sections 2, 3, and 4, as well as the results of interactions with other stakeholders, contributed to the list of VIT Best Practices presented in Section 5. Due to the diversity in the organizations that provided input to this project, it would have been very difficult to arrive at an absolute group-consensus on how these identified "best practices" should be prioritized. Therefore, the interactions with the stakeholders focused mainly on the identification of VIT best practices and only secondarily on their prioritization. Nevertheless, Section 5 presents a prioritization of these different "best practices" according to their impacts on four main criteria: security, safety, reliability, and readiness for deployment.

Section 6 presents a law enforcement concept of operations for stopping moving vehicles using VSTs. This COO provides an appropriate protocol to avoid inadvertent activation, a list of steps and procedures to be followed before activation, and a checklist of organizations that should be coordinated with in order to ensure safe utilization.

The next section of this report, Section 7, summarizes the findings of this study. The last section is the References section, which is followed by five supporting appendices.

One of the early primary conclusions of the study was that the industry, as a whole, favors an approach that focuses on theft prevention—before a vehicle is actually underway. As a result, the project provided emphasis on the evaluation of driver authentication technologies to ensure verification of authorized personnel, as well as preventing hijack situations. Appendix A of the report presents a discussion of these driver authentication technologies that complement the ones showcased in the demonstration tests.

The remaining four appendices describe the Vendor Questionnaire (Appendix B) and the software to access the information collected in the demonstration tests and Vendor Questionnaire (Appendix D). Appendix C presents the schedule of events for the demonstration tests and a description of the different technologies and scenarios tested for each VIT provider; and Appendix E provides the list of all of the stakeholders that participated in this project.

2. TECHNOLOGY OVERVIEW

Vehicle Immobilization Technologies (VITs) are classified into two main categories, Vehicle Disabling Technologies (VDTs) and Vehicle Shutdown Technologies (VSTs), depending on the kinematic status of the vehicle at the time the immobilization process starts. VDTs are immobilization technologies that impede restarting a vehicle. They can be activated when the vehicle is moving or stationary, but the VDT will only immobilize the vehicle the next time an attempt is made to start it. VSTs, on the other hand, are technologies that cause a vehicle to loose power while it is moving and will cause it to eventually come to a stop, as well as impede the restarting of the vehicle after the technology has been triggered. While there are VIT systems that are composed only of a VDT, those that have vehicle shutdown capabilities always have vehicle disabling capabilities as well.

2.1 TECHNOLOGY COMPONENTS AND SUBSYSTEMS

The surveys conducted in this project, as well as the vendors' questionnaire results, indicated that although there are as many configurations and setups for a VIT system as there are vendors, the basic components are similar for all of them. Referring to Figure 1, at the core of any VIT system, there is (usually) an electronic vehicle immobilization device (eVID, indicated as item 1 in the figure) mounted somewhere in the engine compartment of the equipped vehicle. This device can be actuated remotely and/or locally to impair the performance of the vehicle (through, for example, an acceleration control, a throttle reduction, or a power reduction mechanism) up to a complete engine shutdown.

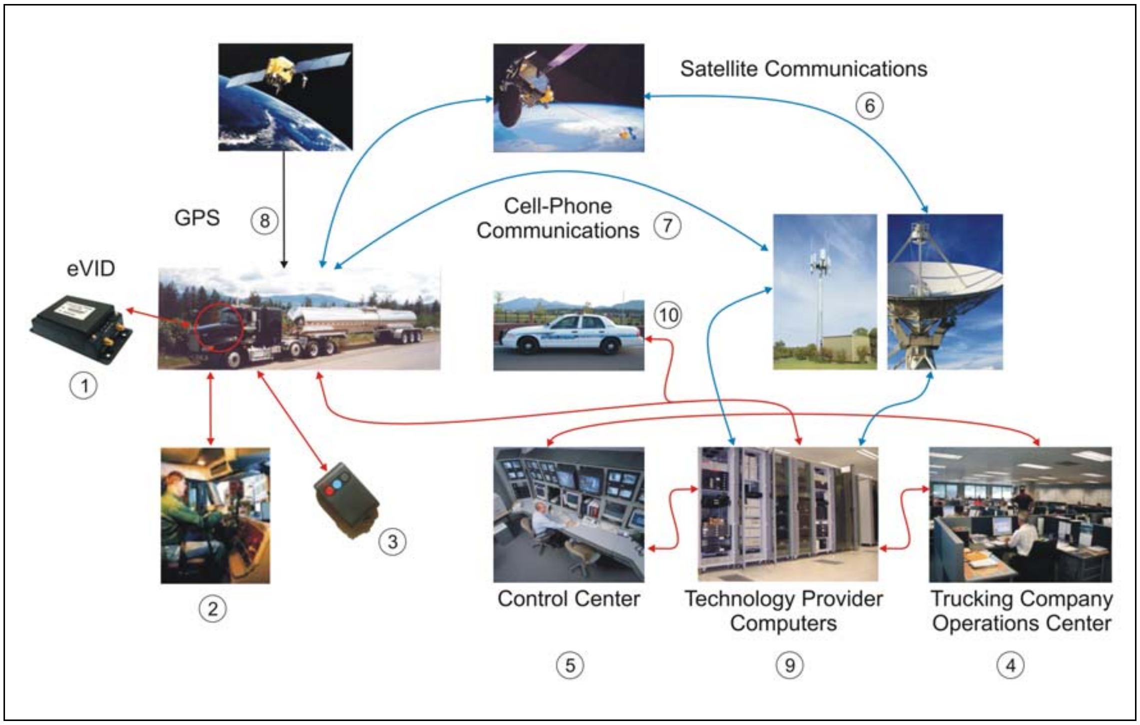

Satellite Communications
6
GPS
8
Cell-Phone Communications
7
eVID
10
1
2
3
Control Center
Technology Provider Computers
Trucking Company Operations Center
5
9
4

Figure 1. Components of a VIT System

In general, the default mode of the eVID is "active." That is, vehicles equipped with this technology cannot be started until the eVID is deactivated. The deactivation of the device can be achieved through different means (Item 2 in Figure 1) which range from keypads—the most common, where the driver enters a predefined code—to swipe cards and RFID (Radio Frequency Identification) tokens, up to biometric devices (note: for VIT systems, biometric devices were still in a research stage at the time this report was completed). A more detailed description of different driver authentication devices can be found in Appendix A. Usually, the eVID is activated automatically when the driver shuts down the engine, but it can also be triggered when one of the cabin doors is opened while the engine is running (hijack prevention mode).

Outside the cabin, with the engine idling, the eVID can be actuated locally (i.e., at a short range) by the driver of the vehicle. This is done through a key fob device (Item 3 in Figure 1) similar to those used to lock/unlock the doors of passenger cars, but usually requiring two buttons to be pressed at the same time to avoid unintentionally triggering the device. The eVID can also be actuated remotely by the dispatcher (Item 4 in Figure 1) or the technology provider (Item 5 in Figure 1) if the vehicle is equipped with a wireless communication system, generally satellite (Item 6 in Figure 1) or cell phone communications (Item 7 in Figure 1), or both. This remote actuation also requires a GPS (Global Positioning System) device (Item 8 in Figure 1) that provides location information of the equipped vehicle.

The flow of information to and from the equipped vehicle is as follows. From the vehicle, its position plus eVID status information is forwarded to the technology provider's computers (Item 9 in Figure 1) using the available communication links (Items 6 or 7 in Figure 1). Conversely, from the technology provider's computers and using the same communication links, messages can be sent to the eVID, including those that initiate the shutdown of the vehicle while it is moving.

For the case of a local vehicle disablement (for example, when the eVID enters into a tampering mode after a given number of authentication attempts have been made and failed), the device generally disables the vehicle without waiting to receive a message from the central computers (i.e., the decision is made locally). However, the device sends a message to the technology provider's computers indicating the problem at hand (in the previous example, conveying that the device has entered into a tampering mode). In some cases, this message is immediately forwarded to the owner of the vehicle through e-mails or phone messages, so the trucking company can take some action (e.g., contacting the driver to determine the nature of the problem). In other instances, the vendor's control center deals with the problem directly and, subsequently, notifies the owner. Figure 2 and Figure 3 show schematic diagrams of the information flows to and from the vehicle for VDT activation, with and without a VIT vendor control center, respectively.

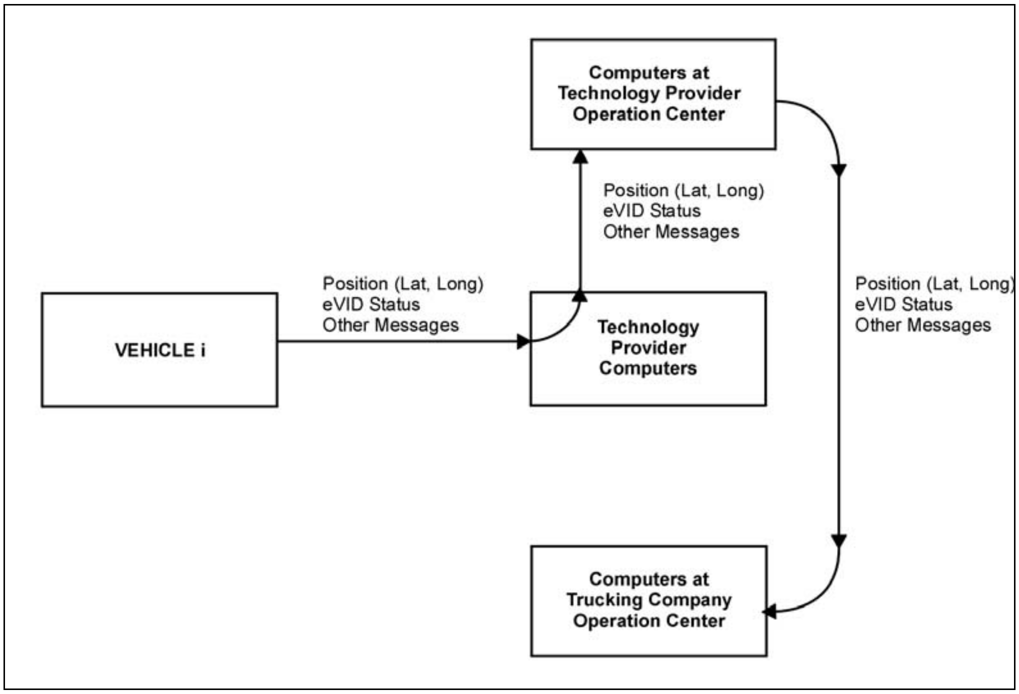


Figure 2. Information Flow for VDT Activation with a VIT Vendor Control Center

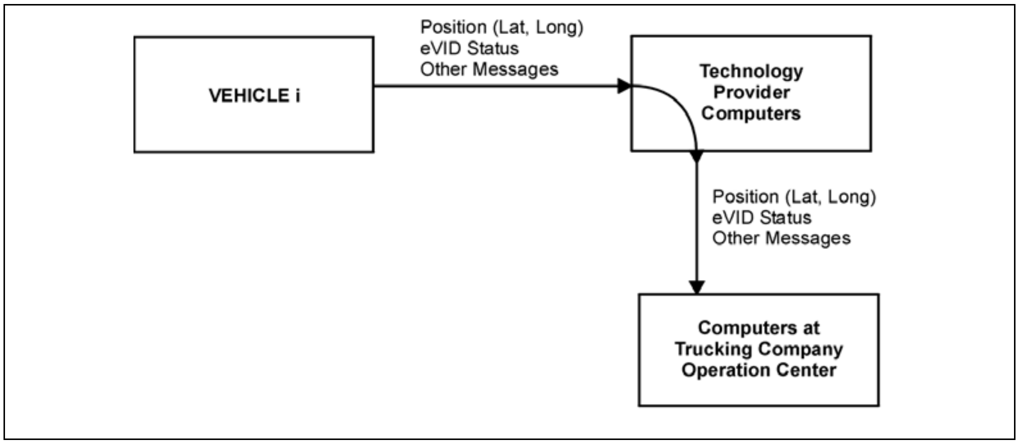


Figure 3. Information Flow for VDT Activation without a VIT Vendor Control Center

Regarding remote vehicle shutdowns, two different models are currently in use to trigger the process. In the first model, the trucking company's operation center (Item 4 in Figure 1) has direct access to the eVID (Item 1 in Figure 1) through the technology provider's computers (Item 9 in Figure 1) and the available communication links (Items 6 and/or 7 in Figure 1). The trucking company can then send a message to the eVID that initiates the shutdown (or disablement) process without any other exogenous intervention. Figure 4 presents the flow of information for this model in a simplified diagram (note: dashed lines indicate components that may or may not be present in this model).

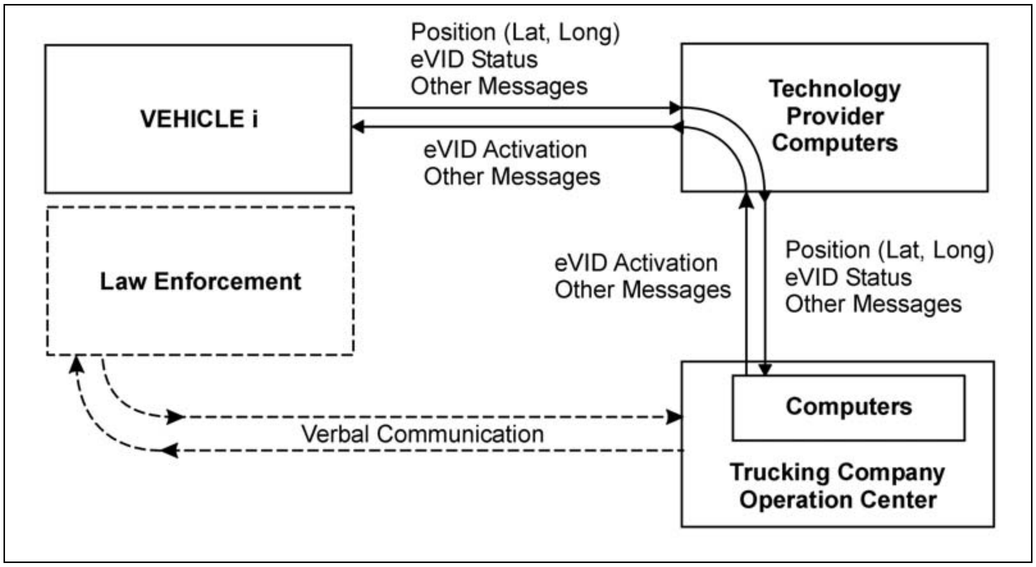


Figure 4. Information Flow for VST Activation with Dispatcher Control

The second model adds a technology provider's control center (Item 5 in Figure 1), which is the one that ultimately sends the message to the eVID to start the shutdown process. In this model, the technology provider's control center identifies the location of the vehicle in distress (Item 8 in Figure 1) and contacts the law enforcement organization with jurisdiction in that area. The shutdown process is initiated only when law enforcement personnel (Item 10 in Figure 1) are in visual contact with the truck and when they determine that is safe to do so. Of course, this involvement of law enforcement personnel is also possible in the first model, although it is a cumbersome process for the trucking company since it would have to have up-to-date contact information for all the law enforcement jurisdictions in the country.[1] A simplified diagram of the information flow for this case is presented in Figure 5.

[1] At the time of the publication of this report, there had been at least one reported remote shutdown of a heavy vehicle in the United States (see Section 4 of this report for additional details).

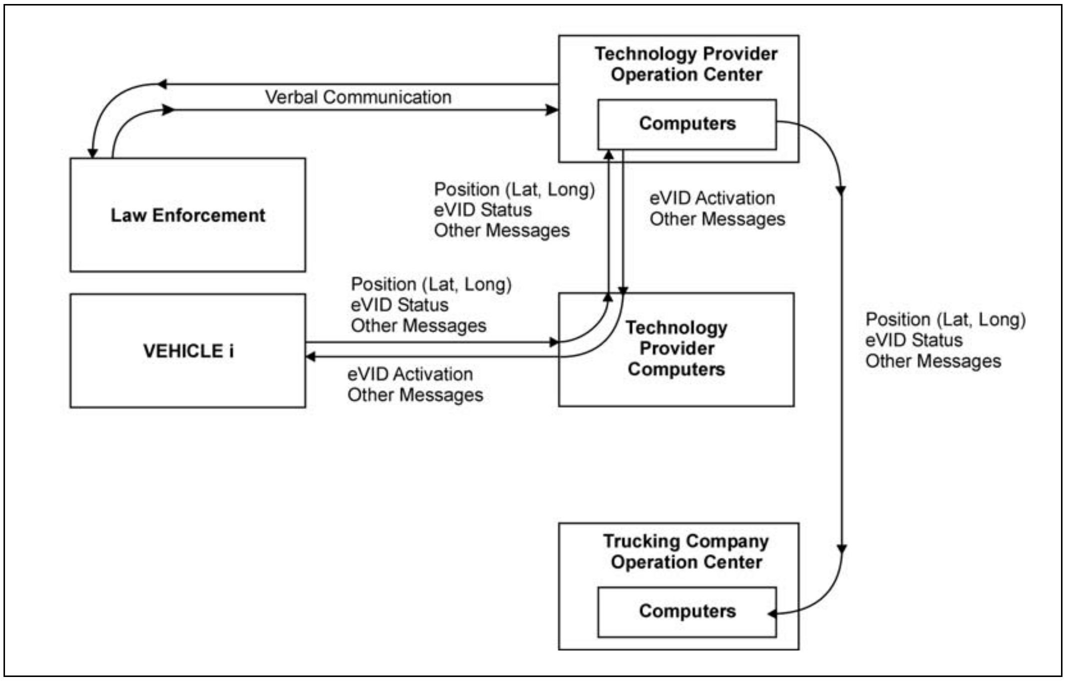


Figure 5. Information Flow for VST Activation with VIT Vendor Control

2.2 FUNCTIONAL REQUIREMENT MAPPING

As part of previous research efforts, FMCSA had identified five functional requirements (FRs) of interest for VITs. These FRs are:

FR1: Vehicle disablement if the vehicle senses an unauthorized driver
FR2: Vehicle disablement/shutdown in the event of a loss of signal
FR3: Remote vehicle disablement/shutdown by the driver
FR4: Remote vehicle shutdown by the dispatcher
FR5: Remote vehicle shutdown by law enforcement

Functional Requirement 1 falls into what has been defined in this document as a VDT, while FRs 4 and 5 are the main attributes of VSTs. FRs 2 and 3 would be applicable to both VDTs and VSTs, depending on whether the vehicle is stationary or moving.

This taxonomy is adopted in this report, although, as discussed later in this report, there is a strong stakeholder consensus that FR5 should always work in conjunction with FR4. That is, discussions with law enforcement personnel have indicated that it would be very difficult and impractical for law enforcement to remotely shutdown a vehicle without coordination with the dispatcher or some other party in possession of all the necessary information and control capabilities to trigger such an event. A more detailed discussion on this issue is presented in the Best Practice and Concept of Operation chapters of this report.

These five functional requirements can be mapped to the VIT system components and subsystems discussed in the last section. Figure 6 reproduces all the elements and interactions of a generic VIT system that was shown in Figure 1, but identifies which of these components and interactions are parts of the five functional requirements. While all of the FRs involve the eVID in this generic VIT system, FR1 is restricted to the truck cabin, the driver, and his/her interaction with the vehicle immobilization device. Notice that this particular FR can also be satisfied by means other than an eVID; that is, there are mechanical (e.g., brake locks) and other types of devices that can make the vehicle un-drivable unless the device is disengaged.

Functional requirement 2 implies the activation of the eVID when one or more of the communication links, either GPS or data transfer, become unavailable for a given period of time. In general, the VIT systems that satisfy this FR allow the user to define the interval of time that needs to elapse before a loss of signal causes a vehicle shutdown. Loss of signal can also produce a vehicle disablement if, for example, a communication wire (e.g., antenna wire) is physically severed or even if somebody tampers with the antenna itself (e.g., covers the antenna with a metal dome) while the truck is idling.

Remote disablement/shutdown by the driver (FR3) is accomplished, in general, by a key fob device that allows that driver to send a short range wireless message to the eVID for its activation. This can be achieved while the vehicle is idling (i.e., vehicle disablement) or if someone commandeers the vehicle while the driver is away but at a short range (i.e., vehicle shutdown), such is the case of a vehicle theft at a truck stop.

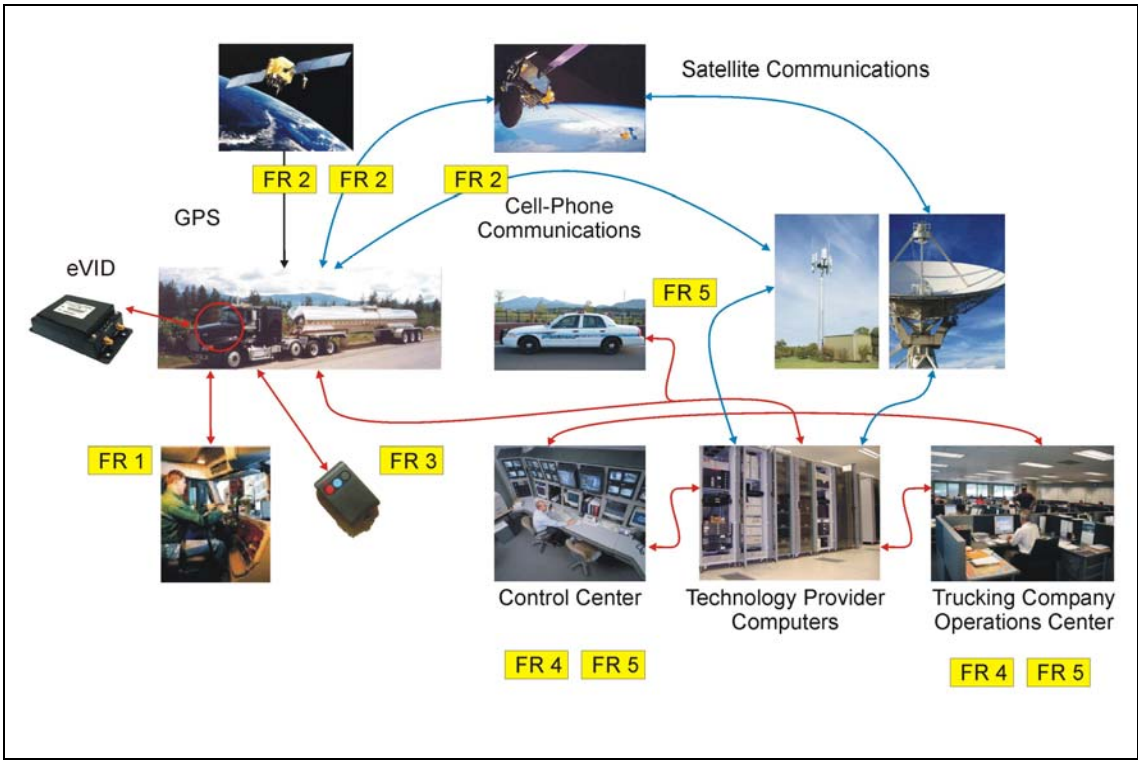

Satellite Communications
FR 2
FR 2
FR 2
GPS
Cell-Phone Communications
eVID
FR 5
FR 1
FR 3
Control Center
Technology Provider Computers
Trucking Company Operations Center
FR 4
FR 5
FR 4
FR 5

Figure 6. Mapping of FMCSA's Functional Requirements on a Generic VIT System

While the first three functional requirements involve VIT system components that are on the vehicle itself (e.g., in-cabin driver authentication devices for FR1, and antennas and communication systems for FR2) or at a very short distance (e.g., key fobs carried by drivers for FR3), FRs 4 and 5 involve VIT system components that can be located anywhere in the country. A remote vehicle shutdown relies on spatial information regarding the location of that vehicle and bidirectional communication links between centralized computers and the onboard eVID. Those computers can be accessed by an external control center and/or by the trucking company dispatcher. By mapping the vehicle's location information provided by the GPS device, it is possible to determine safe places to initiate the shutdown process or to provide information to law enforcement at the scene to identify the vehicle that is about to be shutdown. The bidirectional communication links with the vehicle serve to receive this spatial information and to send a message to the eVID to initiate the shutdown process.

2.3 TECHNOLOGY SCAN AND EVALUATION

The assessment and evaluation of the existing (or under development) VITs encompassed two main activities. The first consisted of a technology scan aimed at identifying those companies that were providing (i.e., commercializing) VIT technologies covering one or more of the FMCSA functional requirements described previously. Certain companies and research organizations with technologies under development were also included if a prototype of that technology existed at the time. The second activity focused on demonstrations of the different technologies provided by different vendors. For this activity, only companies with commercially available products were invited to participate in the demonstrations.

2.3.1 Technology Scan

The process of identifying companies that were developing vehicle disabling technologies commercially or that were underdevelopment and that could potentially satisfy one or more of the five FRs was initiated with a review of previous studies, including FMCSA's Hazmat Safety and Security Field Operational Test (FMCSA, 2004a), and through web-based searches. The identified companies were subsequently contacted through e-mail and/or phone calls to further refine the information collected and eliminate from the list those companies that, although technologically advanced, did not offer solutions that complied with one or more of the FRs. This process resulted in a down-selection of 28 companies and research organizations that are presented in Table 1, all of which received a questionnaire aimed at providing more specific technical and economic information regarding their particular technologies (see Appendix B for more details on this questionnaire).

Table 1. Initial List of VIT Companies Potentially Satisfying One or More FRs[2]

Company	Location	Interaction w/Vendor
1. Aircept	Irvine, California	AQ
2. AirIQ	Lake Forest, California	AQ
3. AirLink Inc.	Fremont, California	SQ
4. Automotive Wireless	Wayland, Michigan	AQ+TI
5. Base Engineering	New Brunswick, Canada	AQ
6. BSM Wireless	Ontario, Canada	AQ+DT
7. CGM Security Solutions, Inc	Punta Gorda, Florida	AQ
8. Enfora	Plano, Texas	SQ
9. Eureka Aerospace	Pasadena California	AQ+VV
10. GlenHugh Enterprise (Autowatch)	Ontario, Canada	AQ+T+DT
11. GPS Management	Brownsburg, Indiana	AQ
12. Homeland Security Technology Corporation	Ontario, Canada	SQ
13. Insite Technologies	Colorado Springs, Colorado	SQ
14. Integrated Decision Support Corporation	Richardson, Texas	SQ
15. International Truck and Engine Corporation	Chicago, Illinois	AQ+DT
16. Lat-Lon LLC	Sheridan, Colorado	SQ
17. MAGTEC Products, Inc	Alberta, Canada	AQ+DT
18. Pana-Pacific	Brentwood, Tennessee	SQ
19. Qualcomm	San Diego, California	AQ+VV+DT
20. Safefreight Technology Inc.	Edmonton, Alberta	AQ+TI
21. Satellite Security Systems	San Diego, California	AQ+V+DT
22. Spot Trac	Des Moines, Iowa	SQ
23. Telogis	Costa Mesa, California	SQ
24. Track Star International Inc.	New Hartford, New York	SQ
25. Trackn	Mission Viejo, California	AQ+VV
26. Vericom	Columbia, Maryland	SQ
27. Lawrence Livermore National Laboratory	Livermore, California	SQ+VV
28. Wireless Matrix (former MobileAria)	Mountain View, California	AQ+VV

SQ: Submitted questionnaire to vendor; AQ: Vendor answered questionnaire; VV: Visited vendor; TI: Teleconference interview; DT: Company participated in Demonstration Tests.
As of June 15th, 2007 Insite Tech (13) and Spot Trac (22) were no longer in business. Satellite Security System (21) is under business restructuring.

Sixteen companies, covering 19 different VIT products returned a completed questionnaire (companies with the label "AQ" in the third column of Table 1), and this information was compiled into a database attached to this report. Several of those companies were selected for a field visit by the project researchers ("VV" in the third column of) while other companies, due to time and location constraints, were contacted by phone ("TI" in the third column of Table 1) to further discuss their technology. Those interactions indicated that out of the 28 companies listed in Table 1, 19 were potential vendors for various forms of VITs. The VIT capabilities that were cited by their respective vendors ranged from the ability to disable a vehicle while it is parked to safely shutting down a vehicle while

[2] More details about these companies can be found in the attached VIT Vendors Database.

traveling at highway speeds. These capabilities were later demonstrated by six of the companies ("DT" in the third column of Table 1), with each of these six vendors showcasing technologies that covered at least four of the five identified FRs.

2.3.2 Technology Matrix

The information collected through the vendor's questionnaires, visits, and teleconferences is summarized in Table 2, with more details included in the database attached to this report. Fifteen companies indicated that their technology covered the driver authentication FR, with two of them (i.e., Ravelco and CGM Security Solutions) using keys to disable/enable the vehicle. Keypads are used by six companies (Base Engineering, BSM Wireless, International Truck and Engine, MAGTEC, Qualcomm, and Wireless Matrix); one company, Automotive Wireless, provides driver authentication through a display and RFID tags, with the latter also being used by GlenHugh Enterprise; two other companies (BSM Wireless and Satellite Security Systems) use swipe cards. None of the companies use biometric technologies, although Satellite Security System (which at the time that this report was being written was in a business reassessment process) was developing such an interface for its system.

Six technologies have the capability of implementing the disablement and/or shutdown of the vehicle if there is a loss of signal (FR2), either through a communications signal or GPS signal. It was found, however, that in practice this feature is never used, especially for the shutdown case. In fact, for those vendors that deal with loss of signal capabilities, their current protocol includes notification of a dispatcher who subsequently seeks a decision about vehicle disablement/shutdown.[3] Nevertheless, the technology provided by some vendors (e.g., MAGTEC, Qualcomm, BSM Wireless), can cause the disablement of the vehicle if a communication wire is physically cut. An illustration of this feature is included in the attached videos that documented the demonstration tests conducted under this project.

For FR3, some vendors indicated that their protocol is for the driver to contact the dispatcher to initiate the shutdown or disablement sequence. As defined in this project, the described protocol falls within the realm of FR4, or remote shutdown by a dispatcher. Other companies, however, provide devices that satisfy FR3. For example, through their key fob device, Wireless Matrix allows the driver to send a "Driver Panic" alert to the onboard eVID, which immediately notifies the call center and triggers the vehicle shutdown sequence. In case of a false alarm, the driver can notify the call center within a certain time period, so that the shutdown sequence is not initiated.

Thirteen companies indicated that their technology could remotely shutdown a vehicle at the discretion of the dispatcher. Two different models were identified for the triggering of the shutdown procedure. In both of them, the information from the vehicle to the dispatcher and from the dispatcher to the vehicle always flows through the vendors' computers. The difference involves how the shutdown procedure is initiated. In one of these two models, the technology vendor acts only as a collector and distributor of

[3] Because of the involvement of a dispatcher, the current handling of loss of signal events falls under FR4 (Remote Vehicle Shutdown by a Dispatcher).

information and is completely oblivious to how the system is used by their customers. In this case, the carrier's dispatcher, or any authorized company manager, simply sends a message (e.g., presses a button on a computer screen) to the specific vehicle in order to initiate the shutdown procedure. In the other model, the dispatcher goes through a control center, manned by the technology vendor or a third party, to trigger the vehicle shutdown procedure. Two companies, Wireless Matrix and Satellite Security Systems, operated under this model.

Regarding FR5 (remote vehicle shutdown by law enforcement) and with the exceptions of the Wattenburg Device (which can be activated directly by the physical tapping of the vehicle's bumper by the bumper of a law-enforcement vehicle) and the Eureka system, which operates as a "microwave gun," (more details about these devices are given below), none of the other vendors indicated that their technologies were currently involved in networks in which law-enforcement could independently disable a vehicle. Currently, when law enforcement is involved with VITs, it is done through the dispatcher or another party (e.g., vendor, call center), although some vendors indicated that granting direct, albeit limited, access to their system by law enforcement is feasible. The "Xs" in the FR5 column of Table 2 reflect discussions with vendors who indicated that working more closely with law enforcement in a more direct fashion would be desirable.

Several approaches are used to disable/shutdown an appropriately equipped vehicle. Those range from physically cutting, or opening, the air line to the service brakes (Wattenburg Device, CGM Security Solutions) to engine performance impairment, including acceleration control mechanisms (MAGTEC, Qualcomm), speed reduction (BSM Wireless), throttle control (Automotive Wireless, GlenHugh Enterprise, Wireless Matrix), and power reduction (International Truck and Engine) to complete engine disablement/shutdown, either immediately or after the next start-up of the vehicle (AirIQ, Automotive Wireless, BSM Wireless, Base Engineering, GlenHugh Enterprise, Ravelco, Satellite Security Systems, Trackn) to the destruction of onboard electronic components (Eureka Aerospace). Due to proprietary information protection, many of the remaining vendors did not provide information about how their technology achieves the disablement/shutdown of the vehicle equipped with their technology.

Table 2 also summarizes other important aspects of these technologies, including unit and licensing costs, installation and maintenance requirements, and robustness against hacking. Some vendors also provided information about the number of units deployed in the field at the time of the survey. That information is included in the attached database but not in Table 2, since it consists of the total number of VITs deployed for both commercial and passenger car vehicles. Referring to Table 2, the first column under "Costs and Other Considerations" shows the price of the equipment for just one unit (in general, all the vendors provide a quantity discount) and, where available, the installation cost and other one-time fees. Except for the HPEMS, which is in a prototype stage, the cost of the individual devices is below $2,000 and in many cases, below $500. Although at the time the survey was conducted, VIT customers only had the choice of buying the technology; since then, MAGTEC has started a leasing program that reduces the initial investment in the deployment of VITs and also permits customers to have access to the latest technology available.

Table 2. VIT Technology Matrix—Functional Requirements (FR), Vehicle Disablement Method (VDM), Costs and Other Considerations

Company Name	Product Name	FR 1	FR 2	FR 3	FR 4	FR 5	VDM: Restricts Fuel Flow	VDM: Disengages Starter	VDM: Locks Air Lines	VDM: Electronic Immobilizer	VDM: Other	Equip. + Installation Cost & Other One-Time Fees ($)	Yearly Fees ($)	Ease of Installation	Required Maintenance	Ease of Hacking
Aircept	MB 3000				X			X		X		399/75	n/a	M	N	D
AirIQ	Vehicle Disable		X	X	X	X		X		X		230	Varies	M	N	n/a
Automotive Wireless	SOS	X		X	X	X	X			X	X	1,700/TBA	TBA	D	S	M
Base Engineering	DAS 100	X							X	X	X	358/142	n/a	E	N	D
BSM Wireless	Guardian	X	X	X	X	X				X	X	Varies	Varies	M	S	D
CGM Security Solutions, Inc	TS4A	X							X			289	N	E	N	n/a
Eureka Aerospace	HPEMS (Prototype)					X		X		X	X	60,000	n/a	D	n/a	D
GlenHugh Enterprise	Autowatch 211Hi	X					X	X		X	X	85/35	420	D	n/a	D
	Autowatch 1R2	X					X	X		X	X	18/35	420	M	n/a	M
	Autowatch 573PPi	X								X	X	95	n/a	D	n/a	D
	Autowatch 898	X					X					120	n/a	D	n/a	D
GPS Management Systems	Aircept MB 3000				X			X		X		399/75	Varies	M	N	n/a
International Truck & Engine Corp.	AWARE(SM) - Under Dev	X		X	X						X	n/a	n/a	F	N	D
MAGTEC Products, Inc	MAGTEC M5K	X	X	X	X	X	X	X		X	X	1,300/515	480	D	N	D
Qualcomm	MAGTEC M5K	X	X	X	X	X	X	X		X	X	n/a	n/a	D	N	D
Ravelco	Ravelco Anti-Theft Device	X					X	X		X		359	N	M	N	D
Safefreight Technology Inc.	SecurityGuard/Smartfleet	X	X	X	X	X						700	Varies	E	N	D
Satellite Security Systems	GlobalGuard System	X		X	X	X				X		445	Varies	D	S	D
Trackn	MB 3000				X			X		X		399/75	n/a	M	N	D
Vericom	VeriGuard				X	X	X					n/a	n/a	V	S	M
Lawrence Livermore National Lab	Wattenburg Device					X			X			n/a	N	E	N	E
Wireless Matrix (ex-MobileAria)	TDSS	X	X	X	X	X	X			X		1,000/200	Varies	M	N	M

Ease of Installation: E(easy): User/less than 1 hr; M(moderately difficult): Professional/1 to 2 hrs; D(difficult): Professional/2+ hrs; F: factory installed; V: varies
Required Maintenance: N: None; S: Some maintenance required; P: Periodic maintenance required.
Ease of Hacking: E: Easy; M: Moderately difficult; D: Difficult.

Some of the vendors require a monthly fee to access their system, which, for those who provided this information, is less than $500/year. In cases where the communication system is already deployed, this amount can be substantially less (for example, Celadon Trucking, which was already using the Qualcomm communication and tracking system, added MAGTEC VIT technology for an additional $60/year/truck; see Section 4 of this report). The installation of the VIT device and associated hardware can be performed by the user for some of the technologies; although in general, this is done by the vendor or by the customer with vendor training. Depending on how long and the level of training required, each product was labeled as being easy to install (i.e., done by an untrained person in less than one hour), moderately difficult (i.e., installation performed by a trained professional and requiring between one-to-two hours), and difficult (i.e., installation performed by a trained professional and requiring longer than two hours). Most of the products presented in Table 2 do not require any maintenance; in some cases, however, the vendors indicated that periodic testing or other small maintenance tasks may be needed.

The last column of Table 2 shows an assessment, based on the information provided by the vendors, on how difficult it would be to hack or disconnect the VIT device. Notice that this labeling refers only to what has been defined here as the eVID and not to the other associated components that may be part of the system (i.e., communication system and GPS).

2.3.3 Technology Description

Several of the companies offering VIT devices were visited by the researchers to gather more in-depth information about the technologies and processes involved in vehicle disablement and shutdown. The main criterion in selecting these companies was the ability of their technology to satisfy the highest number of FMCSA identified FRs. However, budgetary and geographic constraints also played a relatively important role in the selection. Table 1 shows that there is a high concentration of VIT providers located in California (10 out of 28), followed by six companies in Canada, and two in Texas and in Colorado, and the remaining vendors located in other states. A decision was made to travel to California for direct visits to selected vendors, to conduct teleconferences with companies located in other areas, and to invite all the companies offering technologies covering most of the five FRs to participate in demonstration tests of remote vehicle disabling/shutdown technologies that were identified as part of this project.

Six companies were visited by the researchers and four others were contacted by phone. The visited companies included Satellite Security Systems, Wireless Matrix, Qualcomm, Trackn/Aircept, Eureka Aerospace, and the Lawrence Livermore National Laboratory (LLNL). The last two only covered FR5 and, therefore, did not meet the main selection criterion. However, out of all the companies/organizations listed in Table 1, Eureka Aerospace and LLNL were the only ones providing technology that could be directly triggered by law enforcement. Four other companies, MAGTEC, Automotive Wireless, GlenHugh Enterprise, and Safefreight Technology participated in extensive teleconference calls. A summary of the highlights of these visits and teleconferences is presented below.

Satellite Security Systems (S3)[4]

The system developed by S3 (GlobalGuard) has four main components: (1) the electronic vehicle disabling device, which is discretely embedded in a vehicle to deter hackers, (2) the GPS system, which reads spatial location information every 2 seconds (and can store up to one month's worth of location data onboard), (3) the communications system, which can be pager (ReFLEX), wireless (GSM), or satellite (INMARSAT), and (4) command center through which all the messages to and from the equipped vehicles are handled. This central system can be accessed by the users, allowing them to view vehicle position at any time and driver activity (e.g., on duty, off duty, stops, etc.) for any given date (with up to one year of data history), among other information.

The driver authentication process is through a swipe card (driver's license), although the company was starting to conduct research involving biometrics. In the case of an event requiring vehicle shutdown (initiated either by the driver or the dispatcher), the following procedure is used by S3:

1. The vehicle is located.
2. The center contacts the law enforcement agency with jurisdiction in that area where the vehicle is located (note: S3 maintains a national law enforcement database with over 80,000 entries).
3. The center talks to the officer in charge.
4. The officer gives the order to shutdown.
5. The center sends the shutdown message to device mounted on the vehicle.
6. An action report is completed. This action report includes a description of the event, plus all of the voice communications, data, and other relevant information.

The service is relatively inexpensive; for example, one of S3 customers with a small fleet (nine fuel tankers) paid $30/month/truck. This service allowed the customer to access the location information multiple times per day if needed.

Site Visit Demonstrations: Two demonstrations were presented during the team's visit to S3: a truck and a passenger car demonstration. The truck demo involved a tanker owned by Swain Oil,[5] a small (about nine tankers) hazmat transportation company. The truck could not be started without swiping the driver's license to allow the system to check whether he was an authorized driver. After the driver was successfully identified, he was able to start the truck. If the driver was not successfully authenticated, then the S3 call center would have been notified, tracking procedures activated, law enforcement contacted, and after the vehicle had been identified and surrounded, law enforcement personnel in the field would have given the order to disable (notice that under the S3 model, no disablement/shutdown is made directly by the carrier). An unsuccessful driver authentication was also demonstrated and once the vehicle was disabled, a call placed to the call center by an

[4] At the time this report was prepared, S3 was under business restructuring and their officers were not sure if the company was going to continue in the VIT business.

[5] Since this demonstration in August 2006, Swain Oil Transport has been sold and has changed management (April 2007).

authorized person (e.g., dispatcher) was necessary to re-enable the vehicle. A similar demonstration was conducted using a passenger car.

Project Demonstrations: S3 later participated in the demonstration tests that were conducted at Laurens Proving Grounds (LPG) in February 2007 under this project (to be discussed in more detail later in this report). S3 showcased their technology capabilities not only for vehicle disablement, but also for vehicle shutdown. Unfortunately, at the time this report was being compiled, S3 was in the process of reorganization and it was uncertain whether they would continue providing VIT technology and services.

Wireless Matrix (WM)

The WM system involves the following functions and resources: driver authorization via keypad entry, panic button capability (including shutdown sequencing), call center, vehicle tracking on demand, access control, tamper detection, and self diagnostics (Wireless Matrix, 2006). The system can be configured to meet customer's needs regarding these different services/capabilities.

A keypad is used by the driver to enter his/her authentication code. If a valid code is provided, then the throttle will be enabled and the vehicle can then be driven normally. If, on the other hand, an erroneous code is entered, the vehicle's throttle will not be engaged and a message will be sent to the call center indicating the erroneous attempt. In a distress situation, the driver can enter a special "under-duress" code that will enable the throttle momentarily; however, after 120 seconds, the throttle will become inactive and the vehicle will be go to an idling mode.

After an incident is verified, the information is sent to a Public Safety Answering Point (PSAP) service provider, who then contacts the appropriate law enforcement authority and the relevant people at the company that own the truck under distress. The vehicle can be disabled by the call center or by the driver; the carrier, through the call center, can also initiate the shutdown operation. However, the call center is the only authority that can re-enable the vehicle.

The WM system offers both wireless and satellite coverage. The company also has software technology that allows the system to switch from one communications platform to another based on a set of selected criterion, thus providing redundancy in communications and increasing the reliability of the system.

Other features of the system include geofencing capabilities (with boundary definitions that can reside in the central system or in the onboard computer), as well as tampering protection and self-diagnosis. System components, which are fabricated by WM, need no regular maintenance, and the worst situation encountered has been that WM has had to repair loose connections. WM installs the system and performs any maintenance if necessary. The cost of the unit is less than $1,000 per vehicle plus a monthly fee per vehicle.

Site Visit Demonstrations: WM's primary customer in the VIT area is a large, national hazmat transportation carrier. At the time of the visit, that carrier had about 400 trucks instrumented with the WM system. There was a demonstration with one of the trucks from this large hazmat customer. In that demonstration, the driver entered the distress code (i.e., under-duress code) and after two minutes the vehicle's throttle was disabled; that is, the truck was idling, but the driver could not accelerate. There was also a demonstration of the key fob for remote disablement/shutdown by the driver. At the end of the demonstration, the truck was re-enabled through the call center and the driver left the parking lot.

Qualcomm

VIT research and development at Qualcomm started in 1990 in Brazil because of the high number of theft incidents in that country. In 2002, FMCSA conducted a Field Operational Test in conjunction with the TMC (Technology and Maintenance Council) Commercial Vehicle Security Task and the California Highway Patrol (CHP), in which Qualcomm demonstrated the Brazilian-based technology. In 2004, Qualcomm's Vehicle Command and Control concept was developed (Qualcomm, 2007). In 2006, the Orange County Transportation Authority deployed a Qualcomm-based driver authentication and vehicle immobilization system that was tested successfully in a Transportation Security Administration (TSA) demonstration.

Because Brazil presents a different legal and operational environment from that of the United States, the technology used there cannot be deployed in the United States, and Qualcomm adopted MAGTEC technology (MAGTEC, 2005) for its VIT applications and deployments in North America in early 2006. This technology was integrated with Qualcomm's OmniTRACS® Mobile Communications System and later with the company's OmniVision^{TM} Mobile Computing Platform.

Regarding communications, 90% of Qualcomm customers use satellite communications and the remaining 10% use terrestrial (cellular) wireless communications (Qualcomm does not offer the capability of switching dynamically between these two communication networks).

The primary vehicle disabling/shutdown philosophy of Qualcomm is that the carrier is in control of their assets. Under this philosophy, truck shutdown will be managed by the respective carrier, and if a vehicle disablement/shutdown sequence is enacted, Qualcomm is not notified. Also, if law enforcement needs to be involved, it is the carrier's responsibility to communicate with them.

Site Visit Demonstrations: A demonstration of the Qualcomm capabilities (including vehicle disabling/shutdown capabilities) was provided to the team through the Qualcomm "Rolling Laboratory." The demonstration vehicle was equipped with Qualcomm OmniTRACS Mobile Communications System and it also had a terminal for the OmniVision system.

Qualcomm integrates with MAGTEC® VIT technology. Interaction with the MAGTEC M5K is predominantly handled by the 12-key, 4-LED keypad and audible alarm. The keypad is used to enter the (configurable and assigned) authentication codes for drivers and maintenance staff, as well as to perform some general predefined alert and safety functions. The LEDs and alarm allow operators to quickly recognize the MAGTEC M5K's current status and provides feedback when switching between modes.

The MAGTEC disablement technology is built around the Acceleration Control System™ (ACS). The ACS technology is designed primarily for vehicles that have over-the-air capability and can be initiated through integrated computer applications such as Qualcomm's VCC (Vehicle Command and Control). The Acceleration Control System prohibits acceleration beyond fixed intervals. These limits are based on the speed that the vehicle was traveling when an ACS command is issued, and is fully configurable in situ and over the air.

When the eVID is activated, the MAGTEC M5K keypad emits an audible warning for 30 seconds, after which the ACS process begins. During the speed reduction process, the keypad and vehicle lights flash in an SOS pattern to alert surrounding traffic, and the vehicle throttle is deactivated to assist in reducing the vehicle's speed. The throttle is only removed when the vehicle exceeds the speed threshold. In the event that a vehicle is moving down a slope and not decelerating, the throttle pedal is immediately returned to assist in shifting gears. The vehicle is continually forced to slower speeds incrementally until is reaches a top speed of 10 mph, which will be maintained for a specific (configurable) period of time. When the time expires, the vehicle is automatically shutdown and secured. During the shutdown process, the braking and steering systems are fully operable permitting the driver to continue operating the vehicle safely.

The MAGTEC M5K also provides an operational mode called Unattended Idle Protect™ (UIP). This system allows a vehicle to be secured while at idle with the same level of protection it would receive if actually shutdown and secured. The keys can be removed from the ignition, the cab locked, and the vehicle left running while the operator is away from the vehicle. To assist with vehicle idling regulations, the UIP can be configured to shutdown the vehicle after a specific amount of time. In order to exit UIP and begin operating the vehicle again, the operator must possess the ignition key and a valid authentication code.

The MAGTEC device also has provisions for both maintenance operations and local disabling. The maintenance setting allows the dispatcher to generate a one-time maintenance access code that can be used for a preset period of time. Duress codes entered by the driver will disable the truck after five minutes. Qualcomm does not theoretically support the concept of a driver distress signal, indicating that a driver-initiated but automated shutdown sequence, might compromise the safety of the driver. The device can also be programmed to send out an alarm without disabling or shutting down the vehicle when the under-duress code is entered.

Qualcomm, together with one of its customers, Celadon Trucking, participated in the demonstration tests that were conducted at LPG under this project (to be discussed in more detail later in this report), showcasing both their disabling and shutdown technology capabilities.

Trackn/Aircept

Trackn is a “distributor/enabler” of Aircept products (Trackn/Aircept, n.d.). Their primary customer base involves: (a) customers wishing to track vehicles, (b) geofencing, and (c) communication to vehicle owners when certain thresholds (speed, distance from a central point, mileage, etc.) are violated. The vehicles of interest to Trackn are passenger vehicles and some small vocational fleets, although Aircept has some independent customers that include large fleets.

There are close to 300,000 Aircept devices deployed, with about 8,000 to 10,000 being sold each month. The device offers an ignition disabling capability that the owner of the vehicle can activate manually or automatically, for example, if the vehicle exceeds a certain distance from a designated point. The eVID consists of a simple relay that is activated when a vehicle disabling signal is sent via the cellular communication system provided by Trackn (the company works with several commercial cellular communications providers). In that case, the next time that the vehicle is shut off, it cannot be re-started. Trackn indicated that although the device could be configured to shutdown a vehicle while in motion, such functionality has never been deployed by the company. Moreover, Trackn does not support such deployment because of safety issues.

The device costs $395 for the hardware/software, and another $100 for installation (done by a professional). The average cost of the service is about $30/month/vehicle, which includes 1,000 locate-requests (i.e., 1,000 spatial location queries), and it can be as low as $48/year (the range is $48 to $200 per year, although it can go higher if the user needs to query the system very often).

In summary, although this technology has vehicle disabling capabilities, its current markets are very different from the Hazmat Safety and Security market. In addition, the device does not validate a driver’s identity, but can protect assets that are Trackn equipped. Overall, this technology, while very good for its particular market niche, is inadequate at this time to support hazmat safety and security needs.

Lawrence Livermore National Laboratory (LLNL)

After September 11th, 2001, and in response to a mandate by the governor of California to investigate ways to counter the potential threat of a terrorist stealing or hijacking fuel tankers, LLNL developed a simple mechanical device (the Wattenburg Truck-Stopping Device; Lawrence Livermore National Laboratory, 2004) that would allow law enforcement to stop a tractor-trailer on demand. The concept involves the installation of that device on a trailer which, when activated by a series of bumper taps, would engage the trailers service brakes. Research and development on this device, reached a level of $1M, of which $750K was provided by the California Highway Patrol and $250K by LLNL. The device has been demonstrated several times in California and in Nevada on tankers and box trailers.

The device involves about $40 of hardware and can be installed in a matter of hours at a cost of about $260. Once installed, the trailer does not look differently than un-equipped trailers. If the device is accidentally tripped, a light comes on in the cab indicating that the first of the two required taps has been experienced. The driver must then go to the rear of the trailer and “reset” the device by inserting a rod into a hole in the bumper. A similar procedure is followed to reset the device if tapped twice (which would engage the service brakes). None of these devices were in operation at the time of the visit to LLNL and at that time there were no plans/strategies for marketing the device.

LLNL has also developed a version of the Wattenburg device that can be triggered wirelessly. This device is to be used at certain facilities where the trucks entering these facilities can be easily fitted with the device, which could be triggered wirelessly if the truck goes into areas where it is not authorized.

It is clear that the market for the Wattenburg devices is different from the market of wireless-based remote vehicle disabling technologies described previously. The Wattenburg device is a “last resort” type of device that can be utilized by law enforcement to stop a vehicle on demand. On the other hand, the device can be easily engaged by anyone, not just law enforcement. Thus, it does not provide sufficient robustness against foe misuse.

Eureka Aerospace (EA)

Originally funded by the Marine Corps, EA has developed a High-Power Electromagnetic System for Stopping Vehicles (HPEMS) (Eureka Aerospace, 2007). This prototype system uses microwave energy to disable a vehicle’s electronic microprocessors that control the engine’s vital functions and its transmitter can be mounted on buildings or other nonmobile structures, or conceptually even on law enforcement vehicles. At the time of this project’s interview with EA, they were in Phase 2 of a contract with the Los Angeles Sheriff’s Department to develop a mobile version of the HPEMS system.

This VIT device generates microwave radiation which, after striking the wires connected to a vehicle’s microprocessors, induces parasitic currents that disable the electronic components of those microprocessors. The system generates a 15-nanosecond pulse in the 300 MHz to 2.0 GHz range. This range was selected because any lower frequency would require a much larger power source, and any higher frequency would severely limit penetration. EA has found that to disable a vehicle requires being able to generate 10 KV/m at the vehicle site. This is well below the air ionization level (i.e., the maximum level that can be achieved without ionizing the air and generating sparks is 1MV/m) and would, therefore, not produce “sparking,” thus making the device theoretically safe to be used with fuel tankers.

The prototype was once used to disable a 1999 Honda Civic owned by the company. The results of this test indicated that with only one very short pulse of the device, the car was disabled. The vehicle did not shutdown completely, but it was difficult to drive since the engine revolutions were fluctuating. Regarding other types of vehicles, EA indicated that the effect of the device on diesel engines has not yet been studied. This type of engine does not have ignition controls, which is the main component that the HPEMS device disables, so for this application, it would be necessary to look at other engine-related components.

Visit to the EA Laboratory: The team visited the EA lab where parts of the prototype were shown; however, the prototype was not demonstrated. EA estimated that it would require $5M and two more years of effort to achieve the production stage.

Safefreight Technology (ST)

The ST vehicle immobilization technology consists of an onboard "box" that can receive input from 8-12 sensors (analog or digital signals) and that can also be tied to the vehicle's data bus, a GPS device, and a communications system that can use cell or satellite networks (Safefreight Technology, 2007). This is a web-based system that requires no software interface. Customers can choose between cell and satellite, or have both; in which case, an algorithm selects the one that is most cost-effective, thus ensuring almost 100% coverage at a minimum cost.

Customers may choose which types of sensors they want onboard (temperature, light, tank fill volume, etc.) that will function in conjunction with their device. ST consults with their customers to create response protocols that meet their customer's needs and that can be modified at a later time, if necessary. When the Response Center receives the "real-time" notification of a sensor violation, ST security specialists immediately implement the associated response protocol, which includes contacting key personnel and/or the authorities as identified by the client, in the order specified by the client. These protocols and systems are predetermined so that key personnel can be reached at their office, at home or on the road, or through a 24/7/365 call center. In addition to events triggered from onboard sensors, ST also provides geofencing and landmark mapping capabilities. ST has the ability to provide remote ignition lockout and driver authentication.

Other ST technologies include a version of their device that can function in a battery mode on an untethered trailer, and can be configured to get power from the tractor when mated. A portable version of the onboard "box," which operates on rechargeable batteries, has no external wires or antennas and does not require "line-of-sight" for GPS fixes. It can interface with wireless sensors onboard the tractor-trailer and has the ability to link to an electronic cargo manifest.

ST has over 1,000 units deployed in the United States and 1,500 in Canada. The vast majority of the units sold to date have been installed by the customer; ST provides installation instructions, a manual, and customer support. The cost of a base unit is $625-$700, plus $35 to $40/month/vehicle for reporting at a 2-minute interval. The cost of the dual reporting system adds $350 for a modem plus a "Sim card," and requires an additional service contract.

Automotive Wireless (AW)

AW technology initially included the remote start of a vehicle, door locking/unlocking, and other similar capabilities, and utilized a pager-based system (Automotive Wireless, 2007). With the AW system, a vehicle could be "called," and these functions could be performed at a distance via telephone or computer. At the time of this interview with AW, the company had a working model of their Semi Onboard Shutdown (SOS) system, which was also pager-based with the same capabilities mentioned earlier, plus the ability to connect the device with the vehicle's data bus. The eVID component of the system works by closing a valve to the fuel and thereby stopping the vehicle's engine.

The initial SOS pager system had one-way communication (i.e., from the user to the vehicle) and did not offer spatial location capabilities (i.e., the system did not include a GPS device). Because of the one-way communications, when a pager signal was sent to disable the vehicle, no confirmation of shutdown was provided by the system. And due to its lack of spatial location capabilities, only a visual confirmation of the vehicle location is possible. This makes the initial system cumbersome if not impossible to use within the parameters of what has been defined as a VIT system in this project. The system, however, could still be used in critical situations where law enforcement is present and the situation is such that it is imperative that the truck be shutdown.

At the time of the interview that was conducted with AW, the company had just partnered (merged) with an undisclosed company in the Chicago area, which specializes in cellular and satellite communications, GPS technology, and currently provides body, transmission, and universal controller units to Fortune 200 original equipment manufacturer (OEM) truck manufacturers. AW is currently developing and testing this SOS system prototype that provides GPS tracking, cellular communications, vehicle disablement and shutdown capabilities, driver identification/authentication, and access to a web interface for configuration. AW claims the SOS cellular offering is superior to those using satellite systems because large buildings can shadow the vehicle's line of sight to the satellite, resulting in loss of signal and, therefore, it delivers a more reliable metropolitan coverage. Over the air configuration and programming provides easy time-saving, OEM-approved system adjustments that eliminate the need for physical servicing and downtime. The AW SOS also has a reserved protocol that works in conjunction with the American Trucking Associations' (ATA's) Highway Watch program to further increase monitoring of the equipped vehicle in all coverage areas. The AW SOS platform has evolved from a simplistic pager-based environment, to a rugged cellular-based GPS system capable of OEM integration that eliminates system failures common to postproduction installation.

MAGTEC Products, Inc.

The MAGTEC® VIT technology provides various features and capabilities, including a driver authentication system, vehicle protection logic, hijack code, maintenance code, and an acceleration control system, among other features (MAGTEC, 2005). The MAGTEC Authentication System includes a keypad used by the driver to enter a pre-assigned PIN or a driver authentication code; without a correct code, the onboard eVID would not allow the truck to be started. The Protection Logic component is an automated vehicle disabling technology that allows the driver to leave the truck idling and will prevent any unauthorized person from driving that truck. The system also offers a hijack code or under-duress code, which once entered and after some predefined period of time, will send a distress message to the dispatcher. However, regardless of any communication system, the hijack feature will always work and disable/shutdown the vehicle; that is, once the hijack feature is activated by the driver, the vehicle will shutdown. The maintenance code feature allows the dispatcher to generate a one-time maintenance access code that can be used for a preset period of time (up to 99 hrs). If the truck is in maintenance mode and someone attempts to steal the vehicle, the truck will enter into a shutdown sequence after the maintenance period has expired.

The Acceleration Control System^{TM} (ACS) is the core of the MAGTEC VIT system. It is an eVID that restricts the acceleration capability of the vehicle, diminishing the maximum speed achievable by the vehicle by constant intervals triggered at predefined periods of time (see the Qualcomm section for more details about MAGTEC's ACS). These parameters, which define the shutdown process, are configurable over the air. This is a very important feature, particularly for FR5, which would allow the vehicle to be shutdown quickly if so required (for example, in less than a mile, instead of shutting down gently over several miles). MAGTEC's remote deceleration technology has not, as of yet, been used in a real situation, but their idle protection technology (which ultimately uses the same VIT) has been used many times.

MAGTEC indicated that a customer, if he or she so desires, could get a system that includes only the driver authentication portion of the technology without the disabling/shutdown technology. However, the VIT functionality portion of the technology is inherently part of the system and would be wired but not active. The VIT functionality could, in theory, be activated (if the vehicle has communication capabilities) even if the customer has not chosen to use that technology.

Other features include geofencing capabilities (for those vehicles equipped with GPS and communication systems), back office software and communication technologies for customers that do not want to go with complete packages (such as the one offered by Qualcomm), and, shortly, the availability of technology that will protect the trailer/cargo (at the present time, only the tractor is protected).

MAGTEC participated in the demonstration tests that were conducted at LPG under this project (to be discussed in more detail later in this report), showcasing its vehicle disablement and shutdown technologies among other capabilities.

GlenHugh Enterprise (GHE)

GHE provides a modular platform consisting of different modules that cover different FRs (GlenHugh Enterprise, 2007). Specifically, the GHE platform consists of four separate modules that provide different levels of protection and can be configured to any communications carrier.

Module 1 (573): The 573 PPI (Passive Proximity Immobilizer), with driver authentication, is the primary immobilization system that ensures that a truck cannot be started and driven by an unauthorized operator. Disabling up to three vital circuits of the vehicle, the 583 system will not allow an unauthorized driver to start and drive the vehicle. GHE makes available authentication codes for lost codes via toll-free and fleet identification. The 573 PPI is an Underwriters Laboratory of Canada certified device.

Module 2 (898): The 898 Safe-Stop Immobilizer, with driver authentication, allows the truck to idle with the key removed. If a thief attempts to steal the vehicle while it is idling, as soon as the brakes are disengaged, any change in the engine revolutions triggers an engine shutdown. This device is being used by many trucking companies and public service fleets.

Module 3 (211): For FRs 1, 3, and 4, GHE's anti-hijack technology is adaptive and can be customized to any specific fleet requirement triggered by various initiating events such as pressing a button or opening the driver's door, the latter being a main feature for the company's anti-hijack technology. The primary goal is focused on safely bringing the vehicle to a stationary position and to distance the driver from the hijacker as quickly as possible. The hijacker has to gain access to the truck cab and when the door or brake valve is opened, the shutdown sequence is automatically initiated. The driver then has the option to allow the vehicle to shutdown, cancel shutdown, or offer the hijacker access to an override button that will immediately send an alert signal to the dispatcher, indicating that an unauthorized driver has taken control of the vehicle. Once this is done, the dispatcher has the option to shutdown the vehicle. The shutdown sequence consists of slowly opening and closing the fuel line while the truck retains power. The truck comes to a slow, albeit jerky, stop as the vehicle runs out of fuel. The relay timing increases so that the moving vehicle's engine slows down until it stops. During this shutdown sequence, the truck lights are also flashing and the horn or siren is sounding loudly.

Module 4 (1r2): The 1r2 provides the dispatcher with the ability to prevent a vehicle equipped with this device from starting. This is achieved remotely via a message sent wirelessly to the vehicle. Once the message has been sent and the device is activated, the vehicle will not start and an alarm (buzzing sound) will be heard, indicating that the vehicle has been immobilized.

There are no GHE vehicle shutdown devices currently deployed in North America, but the company has other technologies deployed in Mexico, the United States, and Canada. The company has, however, an international market and has engaged in a small number of shutdowns in South Africa. In that country, there is an insurance-based requirement regarding truck security and, therefore, thousands of their products (not necessarily shutdown capable however) have been sold/deployed. Their system is also broadly used (and has been certified) in England, Australia, and Belgium. All of the installers of their products have to have background checks to ensure that the security of the GHE's systems is as high as possible.

GHE also participated in the demonstration tests that were conducted at LPG under this project (to be discussed in more detail later in this report). For these demonstrations, GHE partnered with Archetype as their GPS/communications provider.

3. DEMONSTRATION TESTS

One of the main objectives of this study was to further investigate the functionalities of VITs, focusing mainly on those VITs that were readily available or in the last stages of development and testing. The information collected through the questionnaires, as well as site visits and interviews with vendors and VIT developers permitted the identification of those companies that were marketing, or about to market, this type of technology. The first selection criterion used to reduce the set of technology companies from further investigation were those technologies that were in the research and development stage.

In addition to market readiness, it was also required that the technology could be tested in a real-world environment. One of the questions included in the vendor/developer survey was related to the willingness/capability of the company to demonstrate their products in different settings, going from their own vehicles and laboratories to independent testing (see Table 3). The vendor-provided information was used as a second selection criterion to further eliminate from consideration vendors with technologies that were not easily testable. The products that met these two criteria, along with the ability of the technology to satisfy one or more of FMCSA's identified FRs, were the focus of additional analyses.

All of the vendors that satisfied these three basic criteria were invited to demonstrate, in a quasi-real world environment (i.e., a test track environment), how their VITs could perform the identified VIT FRs. The main goal of the demonstration testing was to gain practical information about VIT operations for input into the development of VIT best practices for both the technology itself and the operational use of the technology, and a concept of operations for the use of this technology by law enforcement. Within this main goal, the demonstration testing had several subobjectives. These were to:

1. Gain unique and first-hand understanding of how different VITs are triggered and activated.
2. Acquire actual speed-of-activation/usage and lag-time data.
3. Understand the effects of different VITs on the level of vehicle controllability after activation (for VSTs).
4. Understand the effects of different VITs on the level of vehicle re-enablement after activation (for both VSTs and VDTs).
5. Gain a better understanding of the impacts of the technologies on the level of interference with the traffic stream once activated (for both VSTs and VDTs).
6. Gain insights on the impacts of VITs on the driving task, including driver's opinions on VIT functionality.

Table 3. Available VIT Developers Testing Capabilities (Testing Modes)

Company Name	Vendor-Owned Vehicle	Vendor-Owned Lab	Independent On-Vehicle	Independent Laboratory
Aircept				
AirIQ	X		X[1]	X[1]
Automotive Wireless	X		X[1]	X[1]
Base Engineering	X	X	X[1]	X[1]
BSM Wireless	X		X[1]	X[1]
CGM Security Solutions, Inc	X		X	X
Eureka Aerospace	X	X	X[1]	X[1]
GlenHugh Enterprise	X		X	X
GPS Management Systems				
International Truck & Engine Corp.	X	X	X[1]	X[1]
MAGTEC Products, Inc	X	X	X[1]	X[1]
Qualcomm	X	X	X[1]	X[1]
Ravelco				
Safefreight Technology Inc.	X	X	X	X
Satellite Security Systems	X		X[1]	X[1]
Trackn	X		X[1]	X[1]
Vericom	X	X		
Lawrence Livermore National Lab				
Wireless Matrix (ex-MobileAria)	X	X	X[1]	X[1]

[1] With conditions such as Non-Disclosure Agreement (NDA), Loaned Material Agreement, installation done by vendor, etc. (see attached database).

3.1 DEMONSTRATION TESTS DESCRIPTION

In order to achieve the objectives described in the previous section, a VIT test plan was developed and demonstration tests, in which nine companies participated, were conducted at the Laurens Proving Grounds, a test track facility in South Carolina.

In keeping with the differences between VDTs and VSTs and their FRs—recall that VDTs are technologies that impede restarting a vehicle, while VSTs are technologies that cause a vehicle to lose power and come to a stop while moving—a two-phase test plan was developed. The first phase (Phase I) focused on VSTs with the objective of demonstrating remote vehicle shutdowns by a dispatcher and law enforcement (i.e., FRs 4 and 5). Although not part of the identified FRs, Phase I was also used to demonstrate geofencing capabilities for those companies that provided this technology. Geofencing capabilities consist of the deployment of a virtual boundary on a geographic region that can trigger an event when that boundary is crossed. This event could be, for example, the triggering of the onboard VST device when the vehicle has crossed a virtual boundary around a protected facility.

The second part of the demonstration tests, Phase II, concentrated on VDTs, with special emphasis on driver authentication. Since in some cases, the remote vehicle disablement by the driver (FR3) can be triggered while the vehicle is moving, the demonstration of this type of technology was tested in both Phase I (vehicle moving) and Phase II (vehicle stationary).

The test series and FR combinations relative to Phases I and II testing are listed in Table 4. All of the VST demonstration tests (Phase I) were performed at the test track, while demonstrations involving static vehicles (Phase II) were conducted off of the test track. For safety reasons, vehicles participating in Phase I demonstration tests using technologies that completely shutdown the engine were required to undergo a preliminary test in which the VST was activated while the vehicle was traveling at a slow speed (e.g., 10-15 mph). Depending on the observed controllability of the vehicle after the VST was triggered, it was determined whether it was safe to conduct a second series of demonstration tests at a higher speed (35-45 mph). As described below, those vehicles equipped with engine shutdown technologies were highly controllable and none of the second series of demonstration tests had to be cancelled.

Table 4. Demonstration Test Matrix

Test Series	Technology Type	Test Phase	Test Track Test	Test Speed	Functional Requirements
0	VST	I	Yes	10-15 mph	5/4/3
1	VST	I	Yes	35-45 mph	5/4
2	VST	I	Yes	35-45 mph	5/4
3	VST/VDT	I	Yes	TBD at Test Time	3
4	VDT/VST	II	No	0 mph	3
5	VDT	II	No	0 mph	1

Demonstration Vehicles: The participating vendors provided their own demonstration vehicles—or vehicles of their customers equipped with their technology—for the demonstration tests. Those vehicles, because of the nature of the project, were required to be heavy trucks or busses. Prior to the test, the vendors also submitted information regarding the type of VST that was going to be demonstrated, as well as details about the necessary steps to trigger the device, including a description of the protocol that was normally followed and phone numbers and other means of communications that were to be used to trigger the onboard VST device during the demonstration tests. This information was necessary since, as described below, the shutdown of the vehicles was controlled by the project researchers who mimicked the actions that law enforcement would take in the field under situations that would require stopping a moving vehicle equipped with this type of technology.

For the demonstration tests, no restrictions were imposed on vehicle weight, other than indicating, prior to the test, that if their vehicles were going to be fully-loaded (i.e., at their maximum legal gross vehicle weight rating, GVWR), empty (unloaded vehicle weight, UVW), or loaded at any other level between UVW and GVWR. No hazardous materials were allowed on the test track.

Data Acquisition: No specialized instrumentation for data acquisition was installed in the participating vehicles other than a GPS device[6] connected to a laptop computer that stored the information. Specifically, a Racelogic VBOX data acquisition system was used to measure the speed and position of the moving vehicle at 10.0 Hz (i.e., a sampling frequency of one measurement every 0.1 second). This spatial information allowed for the determination, in a precise manner, of the trajectory followed by the demonstration vehicle after the VST device had been activated. The information collected was used to evaluate the effects of the VST on vehicle maneuverability.

In addition to the GPS device, a set of stopwatches were used to determine the latency of the system (i.e., the elapsed interval of time between the moment the order to activate the VST device is given and the point in time when the actual activation occurs). A two-way communication radio was also used to communicate with the driver and/or to onboard testing personnel in order to determine when the device was actually activated. This information was used to corroborate the data collected through the GPS and the information provided by the vendors regarding their own demonstrations (i.e., the timestamp messages that were generated between the vehicle and the vendor's computers during the demonstrations).

An integral part of the data collected during the test events was the videotaping of the demonstrations to document the trajectory and behavior of the vehicle after the activation of the VST device. Two cameras were used to record the total vehicle during the test maneuvers. That is, these cameras recorded the approaching and departing paths of the vehicle under the test, with a sufficient angle to allow for total viewing of the vehicle at critical points during the testing. In addition, a third camera was installed inside the cab of the tractor to document the driver's reactions during the test event, and a fourth one was onboard a South Carolina State Highway Patrol vehicle that participated in the tests. The raw footage was edited and summarized into two video productions of the demonstration tests (a short, eight-minute video, showing the driver authentication and vehicle shutdown technologies, and a longer, 20-minute video that captured how the different vendors satisfied all or most of the FRs). These two videos are part of this report.

Event Venue: The demonstration tests were conducted at the Laurens Proving Grounds (LPG) in South Carolina. LPG is a vehicle testing facility operated by Michelin Americas Research and Development Corporation, providing services to all of Michelin's North

[6] Usually, vendors provide GPS capabilities with their VST products, which in general operate with a low data acquisition rate (once every few seconds). The GPS equipment used in the test was a temporary device, quickly installed by ORNL on the test vehicle at the beginning of the demonstration, that gathered positional information at a higher rate (10.0 Hz).

American operations. The 3,000-acre site has over a dozen special tracks that simulate the entire spectrum of driving conditions and road hazards. About 50 employees, including engineers, technicians, test drivers, mechanics, electricians, testing support specialists, utility workers, and administrative personnel work at the facility. LPG, which has been operating since 1976, is located in Laurens County, South Carolina, about 40 miles from Greenville. An aerial photograph of the site is presented in Figure 7, while Figure 8 shows a schematic diagram of Test Track 8 at LPG, which was used for the demonstration tests.

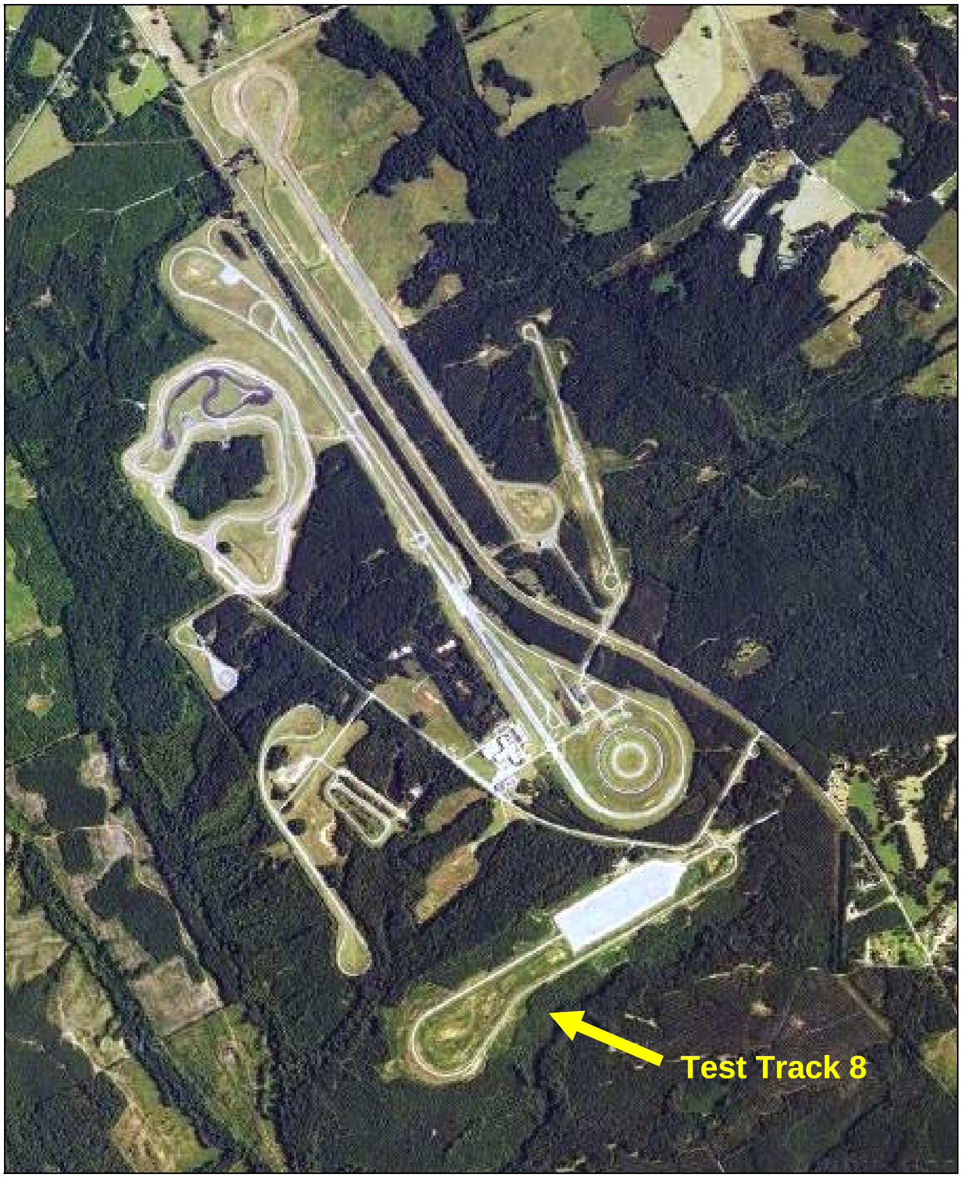


Figure 7. Laurens Proving Grounds (LPG)

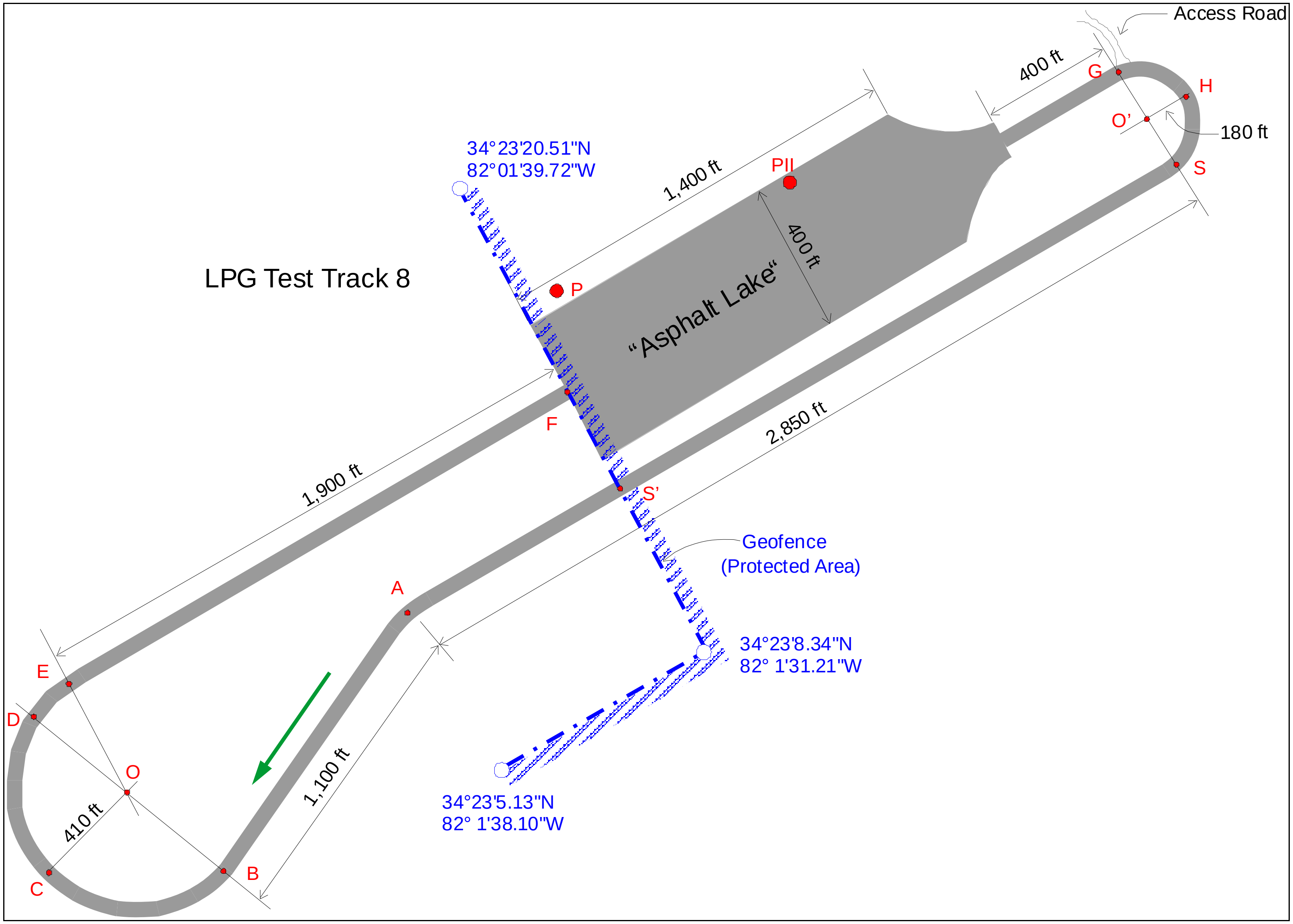


Figure 8. Schematic Diagram of Test Track 8 at LPG Used for the Demonstration Tests

3.1.1 Test Track Testing (Phase I)

Each one of the vehicles participating in Phase I of the tests performed several tests at arterial speeds (i.e., 30 to 45 mph), demonstrating how their VST device accomplished the shutdown of the vehicle. For technologies that used engine shut-off as the mechanism for disabling the vehicle, the first test was conducted at a relatively slow speed (i.e., 10 to 15 mph) and was used to assess the maneuverability and controllability of the vehicle after shutdown. In all cases it was determined that the vehicle could be safely maneuvered; therefore, a second test(s) was conducted at normal arterial speed (i.e., 30 to 45 mph). The arterial speed tests (no demonstration tests were conducted at highway speed for safety reasons) mimicked the activation of the VST device by the dispatcher and/or law enforcement personnel (i.e., FR4 and FR5). For those vendors that offered technology that allows the shutdown of the vehicle by the driver (i.e., FR3), a third test was conducted demonstrating this capability.

The drivers of all of the demonstration vehicles were either employees of the respective vendors or the vendors' customer. Before testing was initiated, all of the demonstration vehicles entered the test track (i.e., LPG Test Track 8, see Figure 8) through the access road close to point G and completed several laps to get familiar with the test track layout. The vehicles were then parked off of the test track at point F.

VST Demonstration at Slow Speed

This evaluation was conducted to determine a vehicle's response to the activation of the VST device while moving at a slow speed and was only conducted for those technologies that completely shutdown the engine. The results of this first test were used to determine the total activation time of the VST device (i.e., the time from when the order to activate was given to the time when the device was actually activated). This was done to assess the maneuverability of the vehicle and to determine whether a test at a higher speed could be conducted with a reasonable level of safety.

Setup: A pylon was placed on the shoulder of the test track at Point E to indicate the VST device trigger point. This allowed sufficient distance to the next curve (i.e., 3,700 ft to point G), with the "asphalt lake" (starting at point F) in between, such that even in the case of very poor vehicle maneuverability, there would be no safety concerns. (Note: the green arrow shown in Figure 8 indicates the direction of travel.) A member of the research team traveled in a South Carolina State Highway Patrol vehicle that shadowed the demonstration vehicle, while another member was in the cabin of the test vehicle.

Procedure: From their parked position, the demonstration vehicle started to travel in a clockwise direction, such that when it reached point E, it was moving at approximately 15 mph. At that time the procedure order to activate the VST device was given from the highway patrol car. The order was communicated wirelessly (using two-way radio communications) to simulate a real-world scenario in which a highway patrolman would call for the shutdown of the vehicle when he had determined that it is safe to do so. The time that elapsed between the instant that the order was given and the alarm inside the demonstration vehicle sounded (indicating that the eVID was activated) was recorded. Also recorded was the elapsed time between the activation of the eVID and the instant that the driver felt that the power to the vehicle was lost.

Once the vehicle came to a stop, the research team corroborated that it was not possible by the driver to re-start the vehicle. Subsequently, the order was given to re-enable the vehicle in the same fashion as was done to shutdown the vehicle. The time that elapsed between the instant that the research team gave the order to re-enable the vehicle and the instant the driver was able to re-start the vehicle was also recorded. This data will be presented later in the report.

VST Demonstration at Normal Arterial Speed

This test series was performed at normal arterial speed (i.e., 35 to 45 mph) instead of at a slow speed. Since for all demonstrations the results of the first test indicated that the vehicle could be safely shutdown while moving (i.e., its controllability did not degrade significantly), this second test series was performed by all of the participating vendors.

Setup: The setup for this second test was similar to that of the first one, with the exception that the order to shutdown was given in a quasi-random fashion, although always in the segment C-D-E, and sometimes in the first part of segment E-F (see Figure 8). Again, this was done in such a way that the VST device would be activated while the vehicle was traveling on a straight segment; both for safety reasons and to better assess its maneuverability through visual observation and the positional information gathered by the onboard installed GPS device.

Procedure: The procedure used in this test was the same as in the Slow Speed Demonstration Test. From their parked position, the demonstration vehicle started to travel in a clockwise direction, such that when it reached the segment C-D-E, it was moving at a speed between 35 and 45 mph. At some point when the vehicle was traveling on this segment, a research team member, following in the South Carolina State Highway Patrol vehicle, gave the order to shutdown the vehicle. As in the previous test, elapsed times to activation and stopping were recorded. The vehicle re-enabling procedure was repeated and the elapsed time was recorded.

VST Geofencing Capability Demonstrations

Although geofencing was not one of the identified FRs, those vendors who provided this feature and wanted to demonstrate it were allowed to do so.

Setup: A week prior to the tests, a boundary (or geofence) defined by three latitude-longitude points (see Figure 8) was provided to the vendors so they could include this information in their central and/or onboard systems.

Procedure: Although this test started in a similar way as the two previous ones, the triggering of the eVID was done automatically when the vehicle crossed the defined geofence and entered into the protected area.

The time that elapsed between the instant that the vehicle crossed the geofence (point F in Figure 8) and when the onboard alarm sounded (indicating the activation of the VST device) was recorded. Also recorded was the time that elapsed between the sound of the onboard alarm and the instant that the driver sensed the vehicle was shutdown.

For those vendors that did not have their VIT device connected to their geofencing capabilities, the research team requested the set of timestamp messages that were passed between the vehicle and the central computer as the former crossed the geofence. This allowed the measuring of the latency time that it took the system to become aware that the vehicle had crossed the geofence boundary. Under the conservative assumption that it would take the same amount of time[7] for the onboard device to receive a shutdown message from the central computer, it is possible to determine how far inside the protected area a vehicle could travel before the onboard device is activated. In addition, the vehicle would travel for another number of seconds (determined in the previous tests) until the shutdown process would be initiated, plus the time it takes to get to a complete stop (also determined in the previous tests).

VST FR3 Demonstration

This demonstration test was only conducted for these technologies that allow the shutdown of the vehicle remotely by the driver with his/her intervention (i.e., through a key fob) or without it (i.e., by not providing authentication). Technologies that allow for the shutdown of the vehicle by the driver using the same protocol as was addressed in the previous demonstrations were not tested here.

Setup: The setup for this demonstration test was similar to that of the previous tests. Depending on the capability being demonstrated, the driver played the role of a thief and another participant played the role of the authorized driver (person outside the vehicle). In other cases, a second person played the role of a hijacker.

Procedure: Two different procedures were proposed to demonstrate FR3 VST capabilities, depending on the type of technology being showcased.

Theft Case: The test would start with the vehicle idling and the driver outside the cab. The driver, playing the role of a thief, would enter the cab and start driving the vehicle. If the vehicle could not be driven by a non-authenticated driver, then the test was not conducted here, since this type of technology (i.e., VDT) was to be tested in Phase II.

Once the vehicle was moving, if the VST was to be triggered by the authorized driver (role played by another participant) through a key fob or another similar mechanism, then the VST was activated. Elapsed times were measured between the activation time, the instant that the VST is actually activated, and the time the vehicle came to a stop.

Hijack Case: Normally, in hijack cases the VST devices do not get activated immediately because such activation could contribute to jeopardizing the life of the driver. A signal is sent to a control center, through the introduction of an under-distress code or other means. From this point forward, the situation becomes similar to those analyzed in the two previous tests (i.e., remote vehicle shutdown).

For the hijack demonstrations, the sequence was initiated with the vehicle idling (parked close to point E on segment E-F, see Figure 8) and the driver being inside of the cab. A second person,

[7] This elapsed time takes into account the communication time between vehicle and central computer, plus the time that it takes for the central computer to determine that the geofence has been crossed. If these computations are performed onboard, as applied to some of the vendors, then the elapsed time to determine that the geofence has been crossed is almost 0.

playing the role of a hijacker, entered the cab and instructed the driver to start moving the vehicle. At that point, the driver triggered the device using the protocol provided by the vendor of the technology. Elapsed times were measured between the activation time, the instant that the VST was actually activated, and the time the vehicle came to a stop. Vehicle re-enabling time was also measured.

3.1.2 Stationary Vehicle Tests (Phase II)

The second part of the demonstration tests was conducted on the "asphalt lake," close to the area where the test observers were stationed (point PII in Figure 8). Although the demonstration tests of this second phase covered FR1, FR3, and for those companies offering this capability, FR2, the emphasis was on driver authentication devices.

No specialized instrumentation for data acquisition was installed in the participating vehicles. However, all of the demonstrations were videotaped and are included in the videos attached to this report.

VDT Demonstrations

There are many different technologies that satisfy FR1 and, to a lesser degree, FR3. Because of this, no rigid protocols were used for the demonstration tests of Phase II. Instead, each vendor was allowed to showcase their vehicle disabling technologies as they considered appropriate. There were, however, restrictions on the time (see Schedule of Events in Appendix C) for these demonstrations, and each vendor was required to provide, in advance, a list of the technologies that would be demonstrated for driver authentication and other VDTs. No particular data was gathered during Phase II (other than measuring vehicle re-enabling times), but the demonstrations were documented via videotape.

3.2 DEMONSTRATION TESTS RESULTS

Nine companies participated in the VIT demonstration tests that were conducted at the LPG facility on February 27, 2007. These companies included six VIT vendors/developers: Satellite Security Systems, MAGTEC, Qualcomm, International Truck and Engine Corporation, BSM Wireless, and GlenHugh Enterprise; two customers using VIT products: the Blue Bird Body Company, a Satellite Security Systems customer, and Celadon Trucking, a customer of Qualcomm; and a GPS tracking service provider company: Archetype, a partner of GlenHugh Enterprise. The event lasted one day and was attended by representatives from FMCSA, TSA, TDOS, South Carolina Department of Public Safety, and OEM companies, as well as ORNL and UTK researchers. Appendix C presents the schedule of events and program for the demonstration tests.

As described previously, the vendors provided their own vehicles for the demonstrations or used vehicles belonging to one of their customers. Table 5 presents a detailed description of the vehicles that were used in the demonstration tests.

Table 5. Demonstration Vehicles

VIT Vendor	Communi-cation System	Vehicle Type and Information	Total Weight (lb)	Owner
Satellite Security Systems	Cellular	School Bus	20,000	Blue Bird Body Co
MAGTEC	Cellular	Class-8 Truck Kenworth T800	30,000	MAGTEC
Qualcomm	Satellite	2005, Freightliner, Columbia	18,000	Celadon Trucking
International Truck & Engine	Cellular	2005 International 4300 SBA 4x2	26,000	International
BSM Wireless	Cellular*	Tandem Axle Truck	26,000	Leased
GlenHugh Enterprise	Cellular	2001, Mack CH613 E7427	30,000	Leased

*Dual mode analog and digital cellular.

3.2.1 Driver Authentication Demonstrations (FR1)

All of the participating companies demonstrated their driver authentication technologies. Two companies, S3 and BSM Wireless, used cards for driver authentication. In the case of S3, a magnetic card reader served as the device to identify the driver (Figure 9); however, at the time of the demonstration, this company was conducting research to add a biometric device for increased security. BSM Wireless, on the other hand, used a two-step driver authentication process. The first step required the driver to use a proximity card (RFID tag) that is waved in front of the driver authentication device (Figure 10).

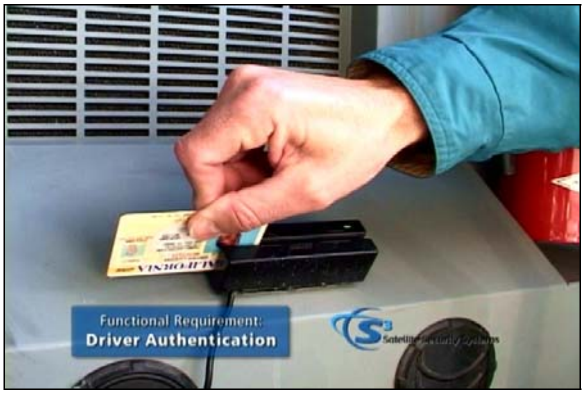


Figure 9. S3 Driver Authentication Swipe Card

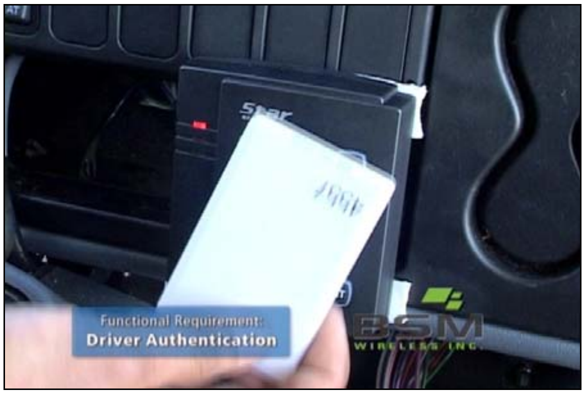


Figure 10. BSM Wireless Driver Authentication Stage 1: Proximity Card

Once the system has accepted the driver as being a valid driver for that vehicle, then he/she must enter a numerical identification code to allow the vehicle to be drivable (Figure 11). The code is also transmitted to the backend application for driver verification and historical logs. The system uses a synthesized voice to guide the user during the authentication process.

Qualcomm (which deploys MAGTEC's VIT technology in their system) also uses a keypad to allow the driver to enter an identification code (Figure 12). The vehicle could be left unattended with the engine idling. However, if a thief were to attempt to drive the vehicle before entering a valid code, as soon as the parking brake is released, the engine would shutdown (Figure 13).

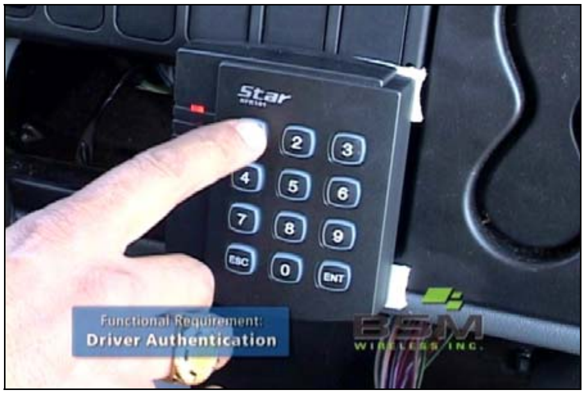


Figure 11. BSM Wireless Driver Authentication Stage 2: Keypad Code Entry

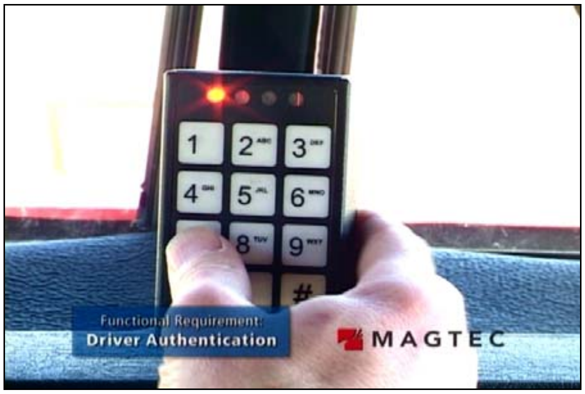


Figure 12. MAGTEC Driver Authentication Keypad Code Entry

A similar procedure is utilized by International Truck and Engine, which also includes a keypad for driver authentication. However, since in this case, the technology is developed by an OEM, the device is integrated in the vehicle dashboard. In Figure 14, the row of keys immediately underneath the radio/CD player is used for driver authentication purposes. As in the previous case, if someone tried to drive away without entering a valid authentication code, the engine would shut off as soon as the parking brake is released.

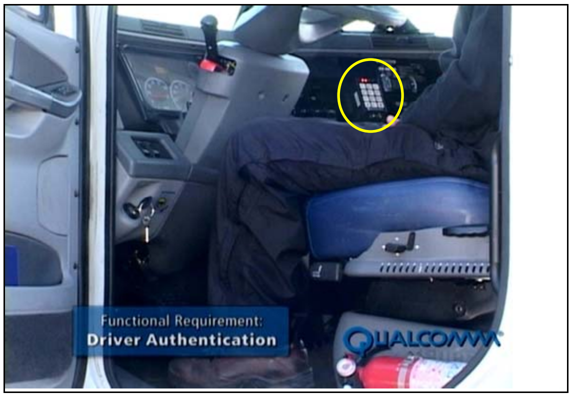


Figure 13. Qualcomm and Celadon Trucking Driver Authentication Keypad Code Entry

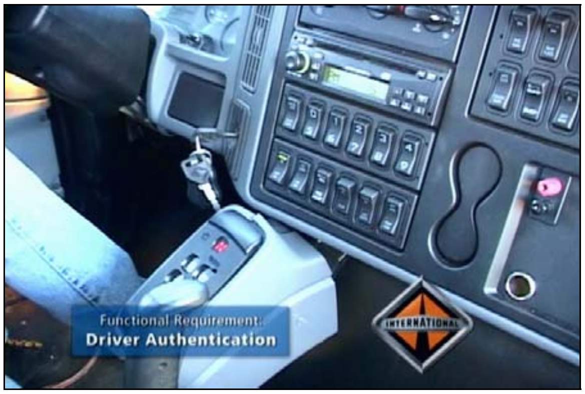


Figure 14. International Truck and Engine Driver Authentication Keypad Code Entry

The last demonstrating company, GlenHugh Enterprise, showcased their autoWATCH VIT technology, which, for driver authentication, uses a transponder device shown in Figure 15. The driver has to be in possession of this device to be able to move the vehicle. The vehicle can be left unattended with an idling engine. If someone tries to drive that vehicle and that person is not in possession of the transponder (the transponder has to be inside the vehicle's cabin), the engine will shut off as soon as the parking brake is released.

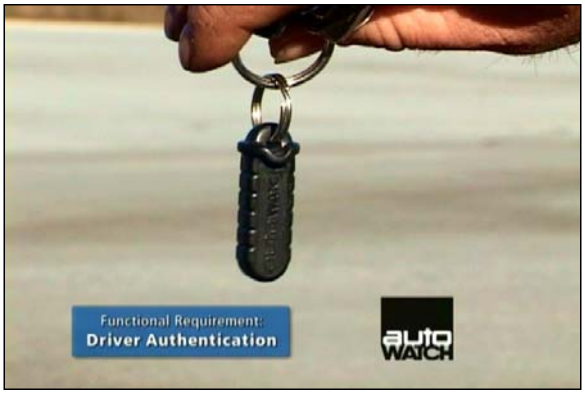


Figure 15. GlenHugh Driver Authentication Transponder

3.2.2 Loss of Signal Vehicle Disablement Demonstrations (FR2)

None of the companies that demonstrated their products at this event offer automatic vehicle shutdown if a loss of signal occurs, not because of technical impediments, but due to safety concerns. For example, a vehicle might be stopped in an urban area with tall buildings and urban canyons, where it is very easy to lose communication/GPS signals, or in an area with low coverage of cell towers. For such cases, however, some of the companies indicated that it is possible to implement a minimum interval of time with no signal that will be accepted before the vehicle is disabled/shutdown.

Nevertheless, two companies demonstrated how their VIT products disabled the vehicle in case of a loss of signal. MAGTEC showed how tampering with the wires (see Figure 16 in which a communication wire is being cut off) would immediately shut off the engine and send out a tampering message. MAGTEC also demonstrated how it was not possible to drive the vehicle (i.e., the engine would shut off) if someone tried to cover the communication/GPS antenna, for example, with the bucket that can be seen on the lower left corner of Figure 16. This capability is disabled by default; when enabled, the vehicle will continue operating without signal until the time threshold is reached (configurable from 1 to 120 minutes), at which point the vehicle will automatically activate the eVID.

A similar demonstration was provided by BSM Wireless wherein the cable to the GPS antenna was cut and the truck engine was shut off (Figure 17). An alarm message was also sent out indicating the GPS antenna cable was cut.

Figure 16. MAGTEC Vehicle Disablement Due to Wire Tampering

Figure 17. BSM Wireless Vehicle Disablement Due to Loss of Signal

3.2.3 Vehicle Disablement by Driver Demonstrations (FR3)

Two companies demonstrated vehicle disablement by the driver. Satellite Security Systems included a panic button in their Blue Bird school bus demonstration vehicle. When that button was activated (Figure 18), a distress message was sent to the central system, which was immediately forwarded, by e-mail, cell phone, or other means, to the person(s) designated by the company using the technology. MAGTEC and Qualcomm also offer the ability to enter a distress or "under-duress" code as well as a "hijack" code through their driver authentication keypad. Similarly, International Truck and Engine provides a feature that allows the driver to send a notification to a control center. This alert is sent, regardless of the ignition status of the vehicle, and the control center can then disable the vehicle remotely.

BSM Wireless demonstrated the use of a key fob device to disable/shutdown the vehicle, as well as arming and disarming its alarm system (Figure 19). The device has a range of approximately 100 ft. The company also provides the capability to enter an "under-duress" code that sends a silent alert and message to persons designated by the carrier. The BSM Wireless system also monitors all doors and the tractor's hood for unauthorized entry. During the demonstration, opening any of the rear doors on the vehicle caused the vehicle engine to be disabled and a message transmitted to the backend application (and e-mails distributed to anyone who is to be notified of the breach).

GlenHugh Enterprise demonstrated a VIT feature for hijack cases. Their system is armed every time the vehicle's engine is turned on or every time a door is opened. The lawful driver must therefore disarm the system upon entry. In the case of a hijack, as soon as the cabin door is opened, the system will be armed. The driver can then give the vehicle control to the hijacker and exit the cabin. The vehicle will be drivable for a few minutes before it is completely shutdown.

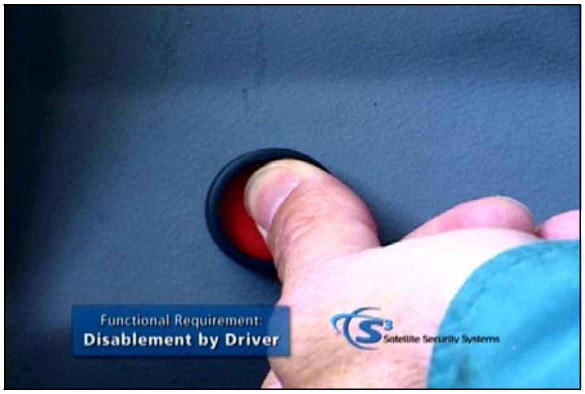


Figure 18. S3 Panic Button

Figure 19. BSM Wireless Key Fob Device

3.2.4 Remote Vehicle Shutdown Demonstrations (FR4 and FR5)

A large part of the event was devoted to the demonstration of remote vehicle shutdown technologies. At the present time, the remote shutdown of a vehicle is always accomplished through the company dispatcher and/or through the VIT vendor control center (see Section 2 for more details), and law enforcement are currently not allowed to accomplish this task independently. While this satisfies FMCSA FR4 (remote vehicle shutdown by dispatcher), FR5 (remote shutdown by law enforcement) has to be accomplished through the same channels as FR4. Section 6 of this report presents, in detail, a concept of operations for law enforcement, but to summarize the current procedures here, law enforcement may or may not be involved depending on the company that owns the VIT-equipped vehicle and the VIT vendor protocols.

The VST demonstration tests were conducted under the assumption that a vehicle shutdown would be performed with law enforcement in visual contact with the distressed vehicle. Therefore, the order to shutdown the vehicle was always initiated from the highway patrol car that shadowed the truck to be shutdown. In a real-world situation, the order would be given when the officer determines that it is safe to initiate the shutdown procedure. For the tests, the order was done in a quasi-random fashion to test system latencies and vehicle maneuverability after shutdown.

The spatial information collected during the tests was used as input to a software utility, developed by ORNL for this project that permits dynamic viewing of the trajectory of the vehicles and the speed profile as they performed the runs. The software, which is included in the attached CD, is described in Appendix D.

S3 VST Demonstrations

Satellite Security Systems demonstrated their vehicle shutdown technology in conjunction with one of its customers, the Blue Bird Body Company (BB). Figure 20 presents the four views of the demonstration tests that were captured by the four deployed cameras: the view from inside of the cabin (upper left corner); the view from the South Carolina State Highway Patrol vehicle (upper right corner) from which the order to shutdown was always given (except in the geofence tests in which the triggering of the eVID was done automatically); and the views from two cameras positioned at strategic places on the “asphalt lake” to capture the vehicle trajectory after shutdown.

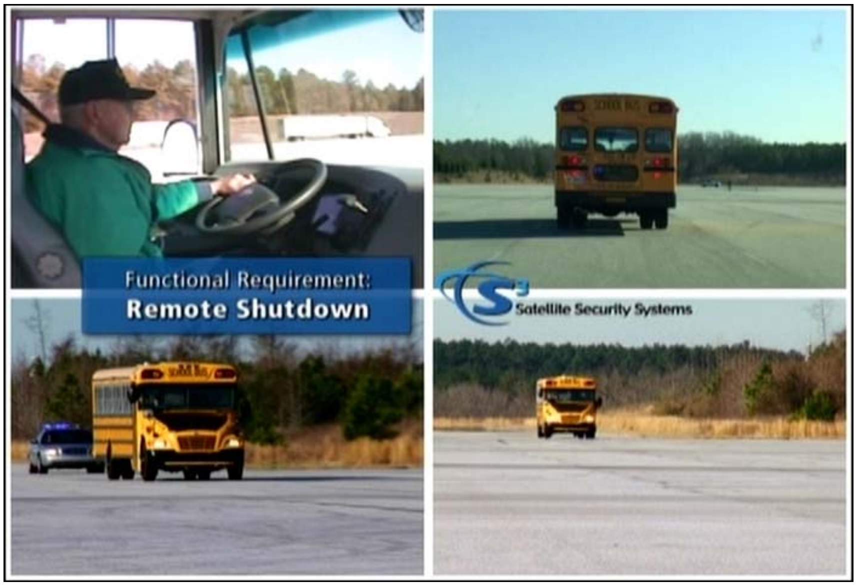


Figure 20. S3 and Blue Bird VST Demonstration Test

S3 and BB performed four runs demonstrating their vehicle shutdown capabilities. The results of these runs are presented in Table 6. Because S3 used a technology that completely shuts off the engine while the vehicle is moving, a first run was conducted at a slow speed as explained in the previous section. After it was determined that the vehicle was fully controllable following the engine shutdown, three more runs at arterial speeds were conducted.

In Table 6, each run is presented in three columns. The first one is the clock time (i.e., the Eastern Daylight Time at which the different test events occurred). These times are shown in hours, minutes, and seconds. The second column is the cumulative, or elapsed time, subsequent to the order to activate the device (i.e., the order to shutdown the vehicle) was given. Elapsed times are shown in minutes and seconds. The last column shows the speed, in miles-per-hour, at which the vehicle was traveling when the particular test event occurred.

The first column of the table (the left most column) is a list of test events. It should be noted that in general, the events are different for different technologies. Nevertheless, the order to shutdown (SD) is always the first test event for any technology. Notice also that this event was initiated from the law enforcement vehicle or by crossing the geofence for those companies that demonstrated that capability. In the case of S3, it was always initiated from the highway patrol vehicle. The second test event is the sound of the alarm inside the cabin of the vehicle being shut down, which indicated that the eVID was activated. The third event is the actual shutdown of the vehicle engine. The next event is the time at which the driver applied the brakes. Because of time constraints, when the researcher traveling inside the shutdown vehicle observed that it was traveling at a very slow speed, he asked the driver to apply the brakes and to bring the vehicle to a final stop. The time at which the vehicle stopped was noted as the next event.

The next row in Table 6 shows a computation of the deceleration rate, measured in ft/sec^2, to which the vehicle was subjected to from the instant that the engine was shutdown to when the brakes were applied.

After the vehicle came to a stop, the onboard researcher asked the driver to re-start the vehicle and confirmed that it was not possible to do so (i.e., the vehicle was effectively immobilized). Sometime after that, the researcher that was traveling inside the law enforcement vehicle gave the order to re-enable (RE) the vehicle, which is shown as the next test event (notice that the elapsed time counter is reset when this test event occurs). The last test event in the table shows the time at which the driver was able to re-start the vehicle.

Table 6. Satellite Security Systems VST Test Results—Slow Speed (Run 1) and Arterial Speed (Runs 2–4)

	Run 1 Clock Time [hh:mm:ss]	Run 1 Elapsed Time [mm:ss]	Run 1 Speed [mph]	Run 2 Clock Time [hh:mm:ss]	Run 2 Elapsed Time [mm:ss]	Run 2 Speed [mph]	Run 3 Clock Time [hh:mm:ss]	Run 3 Elapsed Time [mm:ss]	Run 3 Speed [mph]	Run 3 Clock Time [hh:mm:ss]	Run 3 Elapsed Time [mm:ss]	Run 3 Speed [mph]
Order to SD	09:00:40	00:00	19.50	09:10:38	00:00	27.90	09:17:34	00:00	32.90	09:24:24	00:00	30.10
Alarm	09:00:51	00:11	11.50	09:10:47	00:09	28.40	09:17:48	00:14	29.00	09:24:36	00:12	28.00
Vehicle SD	09:00:55	**00:15**	10.10	09:11:16	**00:38**	28.40	09:18:12	**00:38**	27.20	09:24:53	**00:29**	30.20
Brakes App.	09:01:08	**00:28**	6.44	09:11:50	**01:12**	8.30	09:19:11	**01:37**	2.41	09:25:32	**01:08**	12.20
Veh. Stop	09:01:14	**00:34**	0.00	09:11:56	**01:18**	0.00	09:19:15	**01:41**	0.00	09:25:39	**01:15**	0.00
Dec. (fps^2)			**0.41**			**0.87**			**0.62**			**0.68**
Order to RE	09:01:37	00:00	0.00	09:12:39	00:00	0.00	09:19:53	00:00	0.00	09:25:45	00:00	0.00
Veh. RE	09:01:54	**00:17**	0.00	09:12:58	**00:19**	0.00	09:20:07	**00:14**	0.00	09:26:00	**00:15**	0.00

Consider, for example, Run 2 of Table 6. The order to shutdown the vehicle was given at 9:10:38 AM while it was traveling at 27.9 mph. This test event is also marked on the speed profile of this run shown in Figure 21, in which the last two minutes of the run are shown, and in Figure 22, as the first yellow circle in the direction of travel. The next event, that is, the sound of the alarm, occurred at 9:10:47, or nine seconds after the order to shutdown was given, while the vehicle was traveling at 28.4 mph. The engine shutdown occurred at 9:11:16, or 38 seconds after the order was issued, while the vehicle was traveling at 28.4 mph and at a location marked by the second yellow circle in Figure 22.

After engine shutdown occurred, Figure 21 shows a constant deceleration rate that, for this particular run, was computed to be 0.87 ft/sec^2. Notice, however, that the deceleration rate was constant up to about 10 mph, at which point it changed to a lower deceleration rate. As illustrated in Figure 22, the brakes were applied after this point, and the reported deceleration rate is computed using the speed at the time when the brakes were applied as the ending speed. If the vehicle continued traveling with the deceleration rate that it attained after the speed crossed the 10 mph threshold, the vehicle would have come to a stop at about 9:12:22 AM,[8] or one minute and forty-four seconds after the order to shutdown was given, traveling a distance of 2,700 ft. Instead, because the brakes were applied at 9:11:50, it stopped at 9:11:56, or one minute and eighteen seconds after the order was issued. A similar speed profile (i.e., constant deceleration rate from shutdown to a speed of 10 mph, followed by a lower deceleration rate, but also

[8] This calculation assumed a flat surface, as was the case at the test track. Downslopes or upslopes can change the stopping time and distance considerably.

constant) was observed for Run 3. In Run 4, the brakes were applied when the vehicle was traveling above 10 mph (12 mph as shown in Table 6). If stopping distance computations similar to that of Run 2 are made (i.e., no brake application), the vehicle would have traveled 2,600 and 2,780 ft in Runs 3 and 4, respectively from the instant that the order to shutdown was given to the instant the vehicle came to a stop.

For the last set of test events in Run 2, nineteen seconds elapsed from the instant that the order to re-enable the vehicle was given to the instant at which the driver was able to re-start the bus.

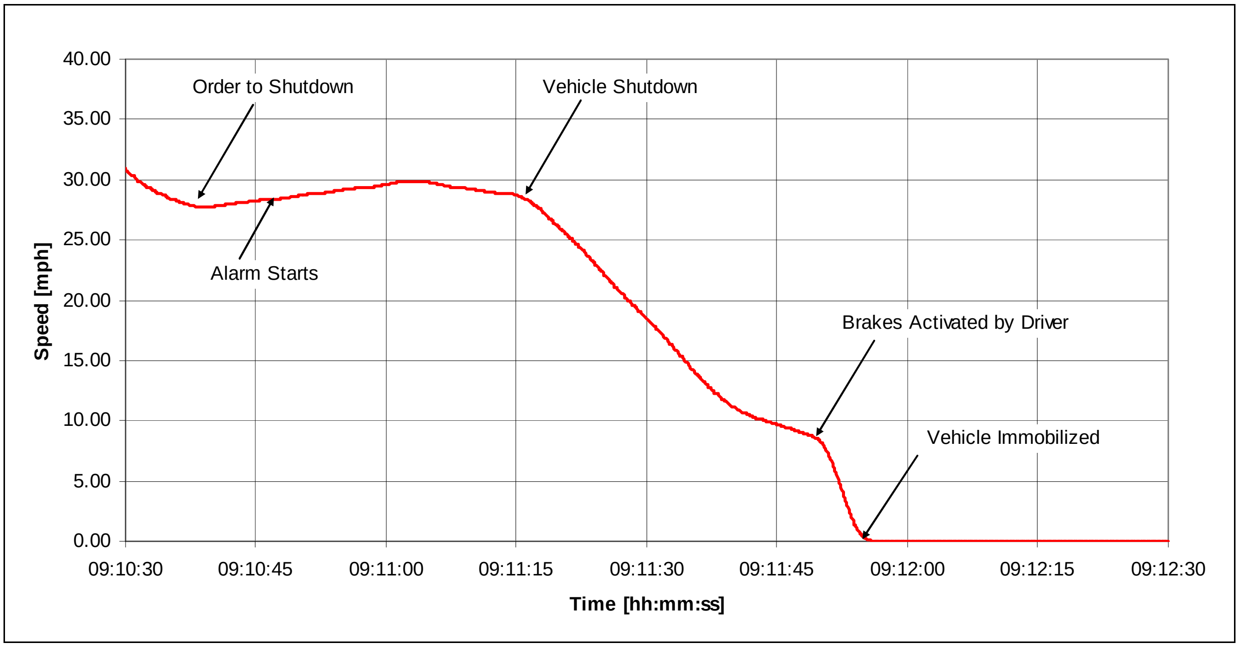


Figure 21. S3 and Blue Bird VST Demonstration Test at Arterial Speed Run 2 Speed Profile

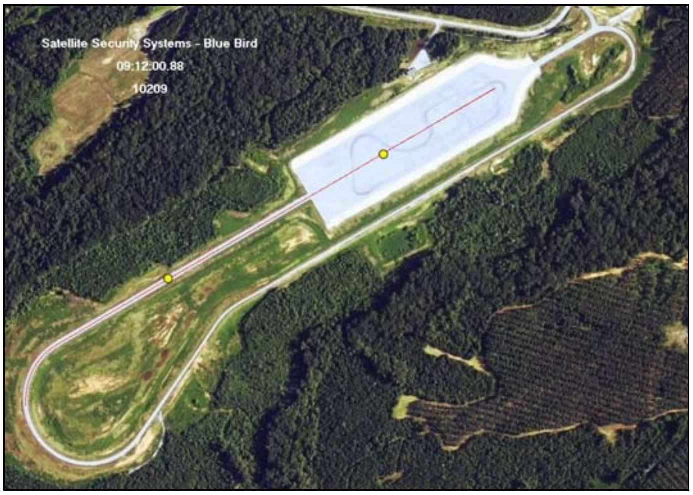


Figure 22. S3 and Blue Bird VST Demonstration Test at Arterial Speed Vehicle Trajectory Immediately before Stopping (Run 2)

Figure 22 presents the trajectory (shown in red and overlaid on the test track) that the bus followed during the two minutes previous to coming to a complete stop. As can be seen from that figure, the vehicle followed a straight line trajectory. Figures 23 and 24 present the speed profiles corresponding to Runs 3 and 4, respectively (see Table 6).

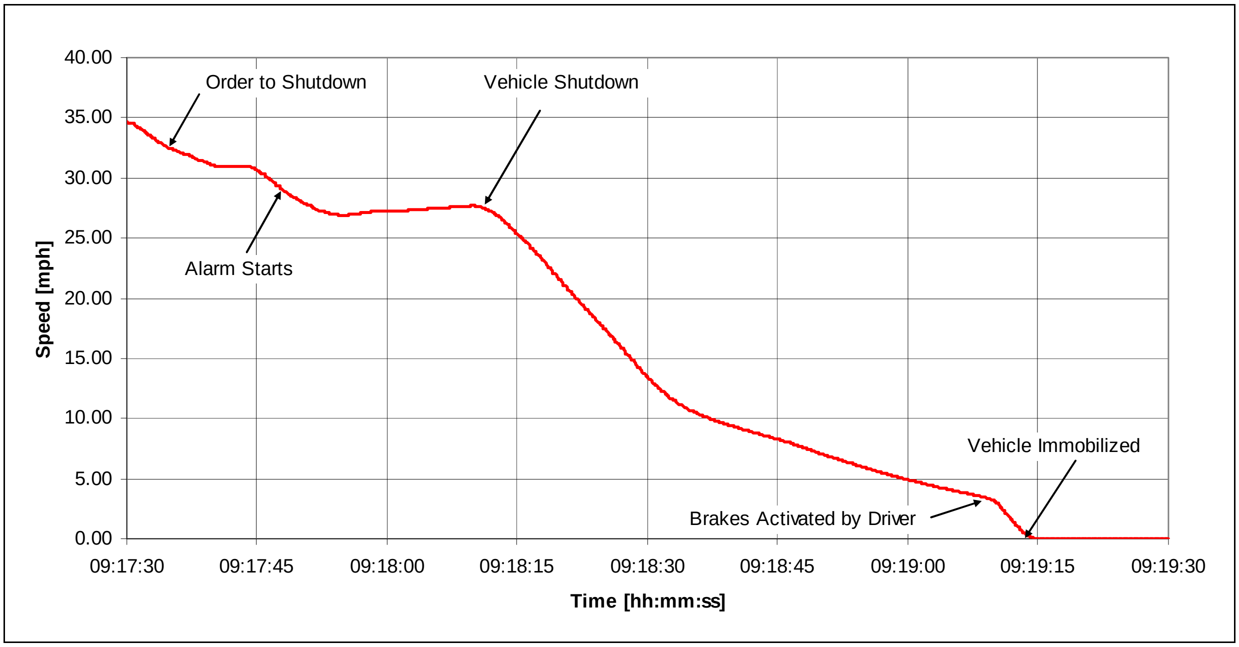


Figure 23. S3 and Blue Bird VST Demonstration Test at Arterial Speed Run 3 Speed Profile

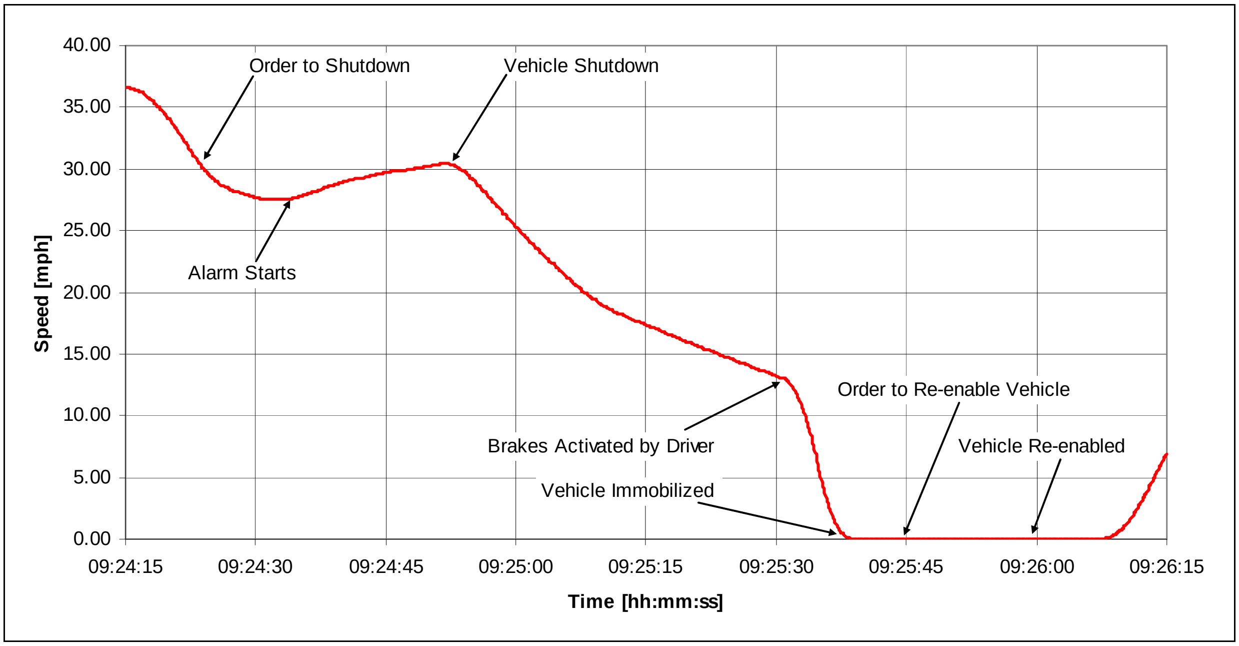


Figure 24. S3 and Blue Bird VST Demonstration Test at Arterial Speed Run 4 Speed Profile

The results of these VST tests show that on average, the S3 VIT required 30 seconds between the instant that the order to shutdown the vehicle was given to the instant that the engine was shut off, and 16 seconds to re-enable the vehicle. The average deceleration rate after shutdown was 0.64 ft/sec^2.

MAGTEC/Qualcomm VST Demonstrations

MAGTEC and Qualcomm demonstrated their technology with class-8 trucks, the former with their own vehicle and the latter with one of their customers, Celadon Trucking Company. While the VDT demonstrations were conducted using these two trucks, all of the VST demonstrations were showcased with the MAGTEC truck. However, during the first part of the test (Run 1 in Table 7) the control and activation of VIT device was accomplished through the Qualcomm system, while in the other two runs, MAGTEC was in control. Figure 25 shows the views from the four cameras during one of the MAGTEC/Qualcomm demonstration tests.

As explained in Section 2, the technology used by MAGTEC (i.e., the Acceleration Control System) does not result in an engine shutdown, but rather in a speed decrement (i.e., a controlled speed reduction) at given intervals of time. Once a speed decrement has been actuated, a new speed ceiling is implemented and it is not possible for the driver to travel at a speed higher than that ceiling (except if the vehicle is on a down grade). The length of the intervals of time at which the speed decrements are actuated is a parameter of the system and can be changed (even wirelessly). For the demonstration tests, the time intervals for enacting the speed decrements were shorter than what is usually specified in the MAGTEC and Qualcomm systems because of time constraints (each company had 45 minutes to demonstrate their VSTs). Other than a reduction of the total time of the test run, no other aspects of the technology were affected. For the tests, MAGTEC/Qualcomm implemented a six-minute cycle from device activation to the limp mode. As an example of a "real-world" implementation, the Celadon truck used by Qualcomm to demonstrate driver authentication had a twenty-minute seven-step cycle vehicle shutdown implementation. Each step had a duration of 45 seconds, for a total of 5 minutes before the truck enters into a limp mode (10 mph), and an extra 15 minutes at that speed before it is completely shutdown.

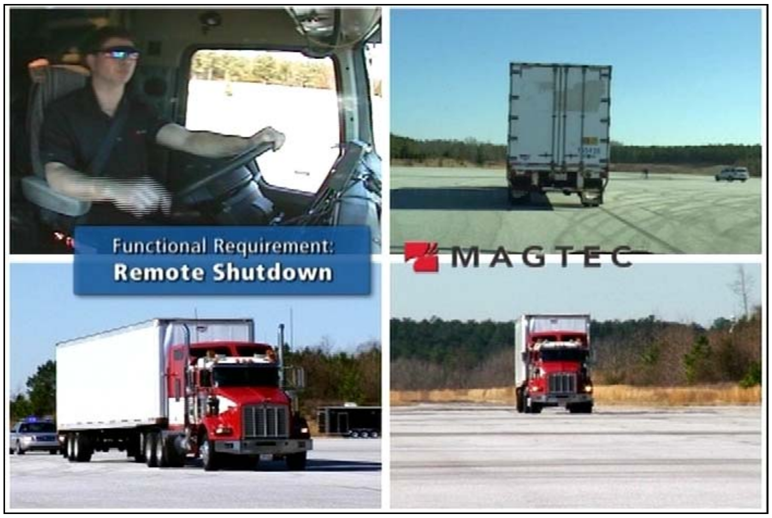


Figure 25. MAGTEC VST Demonstration Test

Table 7 shows the results of three test runs at arterial speed. Because the technology used by MAGTEC is different from that of S3 (and other vendors), the test events in Table 7 (leftmost column) are different from those shown in Table 6, with the exception of the first two items—that is, the order to shutdown and the sound of the alarm inside the cabin, respectively. Notice, however, that while in Runs 1 and 2 the order to shutdown was given from the law enforcement vehicle, in Run 3 the driver enters a distress code that results in the activation of the eVID.

The information presented in Table 7 is also depicted graphically in Figure 26, Figure 27 and Figure 28, which show the speed profiles for the last eight minutes of the three runs. In these figures, it is possible to discern the different speed thresholds that the vehicle experiences while the steps down were being actuated. The figures also show the instant that the vehicle entered the "limp mode" status, which imposes an upper speed limit of 10 mph. For example, Figure 26 shows that after the limp mode was enacted, the driver tried to accelerate, but he was not able to break the 10 mph barrier.

As in the case of S3, the average deceleration rate reported in Table 7 is computed between the instant that the first speed decrement was actuated to the time that the brakes were applied by the driver. Notice, however, that in this case, this is a pseudo deceleration rate since the driver could still accelerate within the upper limit imposed by each threshold. This deceleration rate is presented here for completeness since it is shown as part of the tests that were conducted for all of the other companies. For the same reason, it is only possible to compute an approximate upper bound of the distance that a truck with this VST would travel before coming to a stop. Assuming a flat terrain, a limp mode interval of 15 minutes (similar to the one implemented for the Celadon truck), and that the driver would keep a speed of 10 mph during this interval, the traveled distances for Runs 1 and 2 would have been approximately 24,800 ft (4.70 miles) and 25,700 ft (4.87 miles), respectively, since the order to shutdown was given to the point where the vehicle would have come to a stop. It should be noted that the MAGTEC parameters can be modified over-the-air and on-the-fly without causing any system problems. This functionality provides users with the ability to quickly adjust settings and shut the vehicle down in the event of an emergency.

In the hijack demonstration, Run 3 in Table 7 and Figure 28, the VIT device was triggered by the driver entering a distress or "under-duress" code. As can be seen in Figure 28, the vehicle behaved in a similar fashion as was the case for the two previous runs.

Table 7. MAGTEC/Qualcomm VST Tests Results—Qualcomm Demo (Run 1), MAGTEC Demo (Run 2), and Hijack Demo (Run 3)

	Run 1 Clock Time [hh:mm:ss]	Run 1 Elapsed Time [mm:ss]	Run 1 Speed [mph]	Run 2 Clock Time [hh:mm:ss]	Run 2 Elapsed Time [mm:ss]	Run 2 Speed [mph]	Run 3 Clock Time [hh:mm:ss]	Run 3 Elapsed Time [mm:ss]	Run 3 Speed [mph]
Order to SD*	10:24:22	00:00	41.20	10:48:01	00:00	24.70	10:59:20	00:00	0.00
Alarm	10:24:45	00:23	41.90	10:48:06	00:05	23.00	11:02:34	03:14	29.10
1st Speed Decrement	10:25:58	**01:36**	38.10	10:49:09	**01:08**	40.10	11:03:13	**03:53**	39.80
2nd Speed Decrement	10:26:55	**02:33**	28.80	10:50:39	**02:38**	30.20	11:03:28	**04:08**	30.20
3rd Speed Decrement	10:28:08	**03:46**	19.30	10:52:15	**04:14**	21.00	11:04:41	**05:21**	19.80
Limp Mode	10:29:34	**05:12**	9.96	10:53:52	**05:51**	12.50	11:06:07	**06:47**	10.20
Brakes Applied	10:30:40	**06:18**	9.48	10:55:06	**07:05**	9.43	11:06:53	**07:33**	8.66

	Run 1 Clock Time [hh:mm:ss]	Run 1 Elapsed Time [mm:ss]	Run 1 Speed [mph]	Run 2 Clock Time [hh:mm:ss]	Run 2 Elapsed Time [mm:ss]	Run 2 Speed [mph]	Run 3 Clock Time [hh:mm:ss]	Run 3 Elapsed Time [mm:ss]	Run 3 Speed [mph]
Vehicle Stopped	10:30:55	**06:33**	0.00	10:55:20	**07:19**	0.00	11:06:58	**07:38**	0.00
Dec. (fps^2)			**0.15**			**0.13**			**0.21**
Order to RE	10:32:10	00:00	0.00	10:55:45	00:00	0.00			
Vehicle RE	10:41:40	**09:30**	0.00	10:58:05	**02:20**	0.00			

*For Run 3, the under-duress code triggered the device.

The vehicle re-enabling tests were conducted for Runs 1 and 2. In Run 1, it took over nine minutes from the moment the order to re-enable was given to the instant when the driver was able to start the vehicle. This was the case because after five failed attempts to enter the driver authentication code due to a temporary technical glitch (i.e., a communication delay in the satellite system), the device entered into a tampering mode and required a second message from the central system to allow the re-enabling process to be started again.

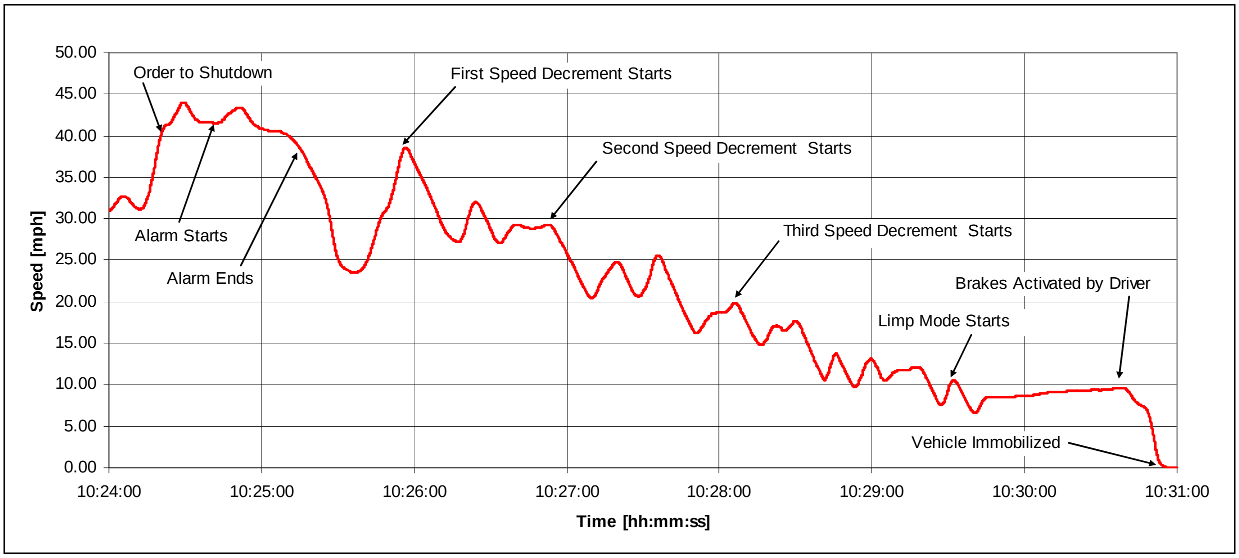


Figure 26. Qualcomm VST Demonstration Test at Arterial Speed Run 1 Speed Profile

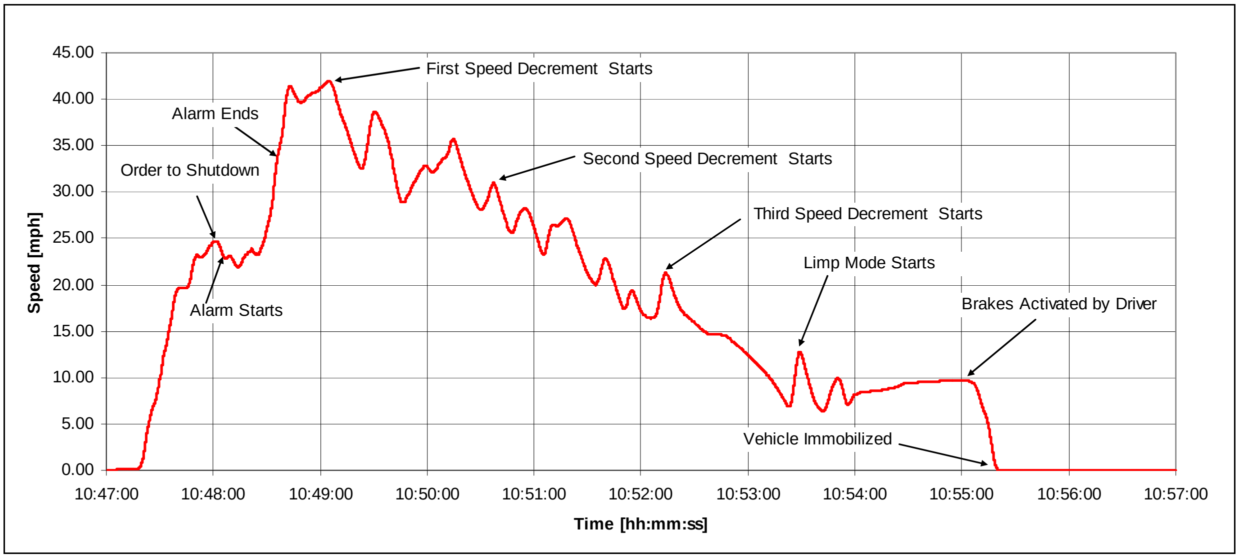


Figure 27. MAGTEC VST Demonstration Test at Arterial Speed Run 2 Speed Profile

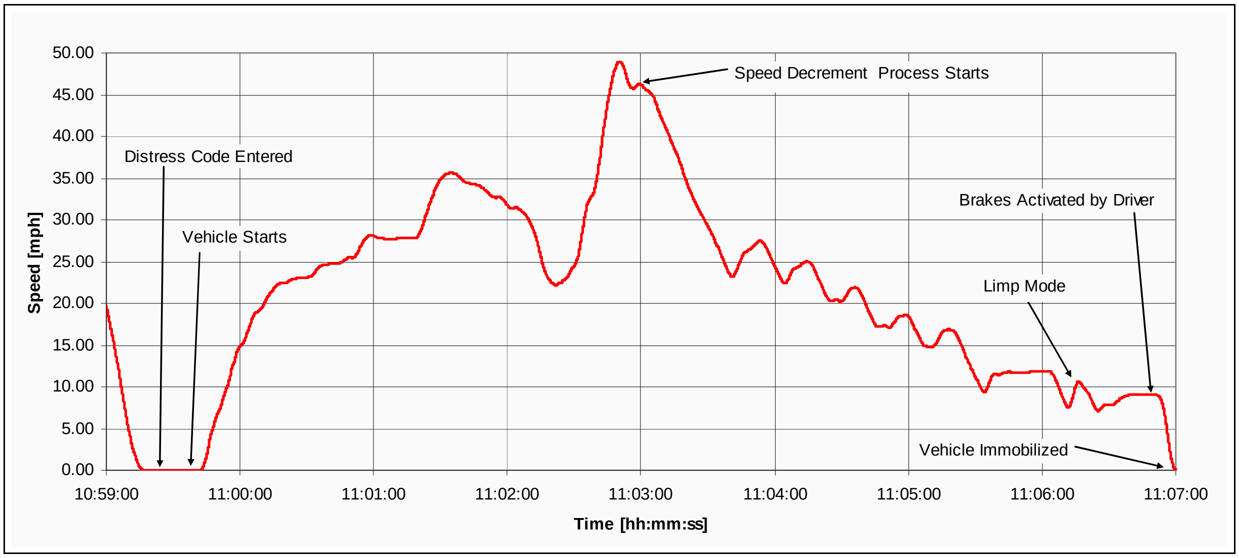


Figure 28. MAGTEC Demonstration Test at Arterial Speed Run 3 (Hijack Case) Speed Profile

The results of these VST tests show that on average, the MAGTEC vehicle immobilization technology required five minutes and 57 seconds from the instant that the order to shutdown the vehicle was given (or the "under-duress" code was entered) until the instant that the vehicle reached the limp mode speed of 10 mph. As explained earlier, this total time is a variable that can be imposed to the system and configured or modified on-the-fly. The average deceleration rate after shutdown was 0.16 ft/sec^2, although this is highly correlated to the total time to reach the limp mode. Re-enablement under normal conditions required two minutes and 20 seconds, and could be close to ten minutes if mistakes are made while entering the authentication code (after five attempts, the system enters into a tampering mode). For the hijack case (Run 3), the time elapsed between the instant that the distress code is entered and instant when the eVID gets activated (three minutes for the demonstration) is a configurable parameter of the system.

International Truck and Engine VST Demonstrations

International Truck and Engine presented a VIT that can be readily and wirelessly adapted to different situations (International Truck and Engine, n.d.). In their VST demonstration tests (Figure 29), International showed three different levels of engine impairment to accomplish a vehicle shutdown. Those included a straight engine shutdown (Run 1 in Table 8 and Figure 30 and Figure 31); a severe, 75%, engine depower (Run 2 in Table 8 and Figure 32); and an extreme engine depower (Run 3 in Table 8 and Figure 33). A fourth test with a two-step (75% and 10%) engine depower was also scheduled but, because of time constraints, had to be cancelled. Remote and local re-enabling were also demonstrated by International Truck and Engine.

The information presented in Table 8 is arranged similarly to that of Table 6 and Table 7 for the S3 and MAGTEC/Qualcomm demonstrations, respectively. Again, and due to the differences in the way the immobilization technology works in various vendor technologies, the test events on the first column of Table 8 are slightly different from those of Table 6 and Table 7. One main difference is that the vehicle came to a stop without any significant brake application by the driver and, therefore, that test event is not included in the table (note, brakes were applied at the end of Run 3 when the vehicle had traveled at close to five mph for about two minutes after the end of the extreme depower period).

Figure 29. International Truck and Engine VST Demonstration Test

Run 1 shows the information for a vehicle shutdown procedure with the engine shut off. This particular run presented the highest deceleration rate of all the demonstrations, 1.87 ft/sec^2. However, the vehicle was perfectly controllable after the engine shutdown occurred. Figure 31 shows the trajectory that the vehicle followed (shown as a red line over the test track) during the last 90 seconds of the run, where the first yellow circle marks the place where the order to shutdown was given by law enforcement (12:45:42 PM), and the second yellow circle marks the place where the engine shutdown commenced (12:46:47 PM). Subsequently, the vehicle traveled in a straight line 603 ft in 25 seconds before coming to a stop.

Stopping distance computations, assuming a flat terrain (such as the one at the test track), indicated that the demonstration vehicle traveled 3,330 ft and 4,230 ft for Runs 1 and 2, respectively, from the instant that the order to shutdown was given to the instant the vehicle came to a complete stop.

Table 8. International Truck and Engine VST Tests Results—
Engine Shutdown (Run 1), Severe (75%) Depower (Run 2), and Extreme Depower (Run 3)

	Run 1 Clock Time [hh:mm:ss]	Run 1 Elapsed Time [mm:ss]	Run 1 Speed [mph]	Run 2 Clock Time [hh:mm:ss]	Run 2 Elapsed Time [mm:ss]	Run 2 Speed [mph]	Run 3 Clock Time [hh:mm:ss]	Run 3 Elapsed Time [mm:ss]	Run 3 Speed [mph]
Order to SD	12:45:52	00:00	34.30	12:55:30	00:00	33.20	13:05:31	00:00	32.10
Alarm	12:45:59	00:07	34.90	12:55:38	00:08	35.10	13:05:41	00:10	30.70
Start of Depower				12:55:48	**00:18**	35.20	13:05:50	**00:19**	31.10
End of Depower							13:06:25	**00:54**	4.95
Vehicle SD	12:46:47	**00:54**	31.20	12:56:42	**01:12**	25.90			
Vehicle Stop	12:47:11	**01:19**	0.00	12:56:57	**01:27**	0.00	13:08:45	**03:14**	0.00
Dec. (fps^2)			**1.87**			**0.75**			**1.10**
Order to RE	12:47:23	00:00	0.00	12:57:27	00:00	0.00	13:09:00	00:00	0.00
Vehicle RE	12:52:14	**04:51**	0.00	12:57:40	**00:13**	0.00	13:09:27	**00:27**	0.00

[1] Remote vehicle re-enable.
[2] Local vehicle re-enable.

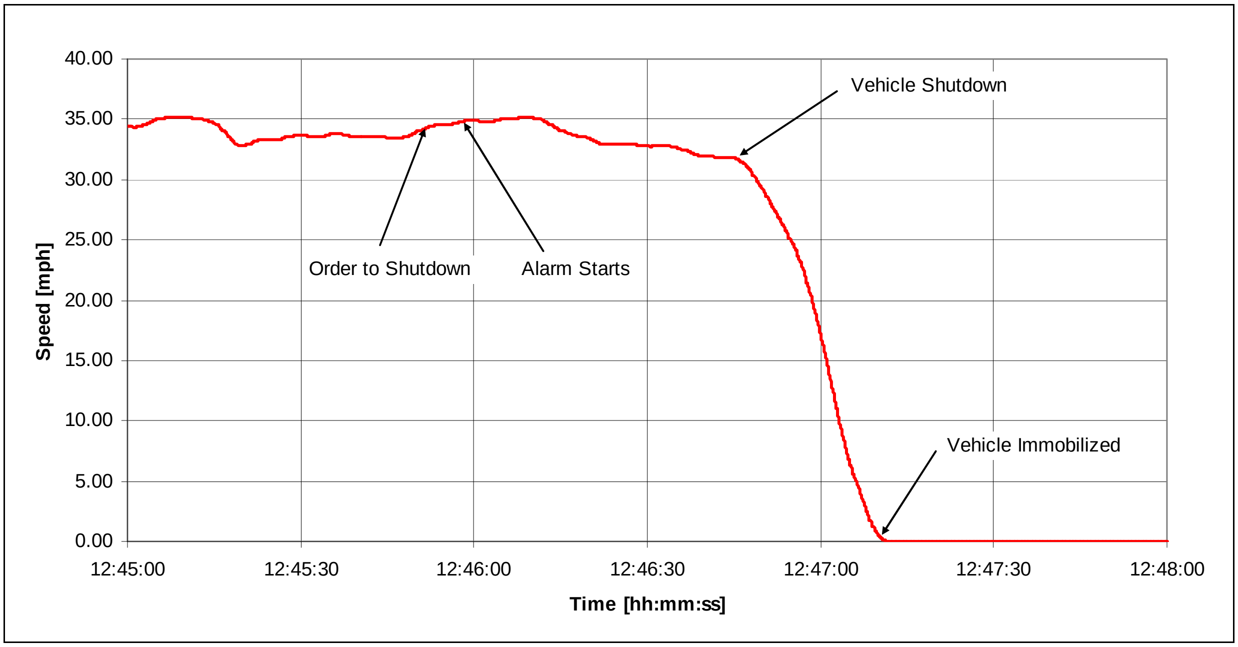


Figure 30. International Truck and Engine VST Demonstration Test at Arterial Speed Run 1 (Engine Shutdown) Speed Profile

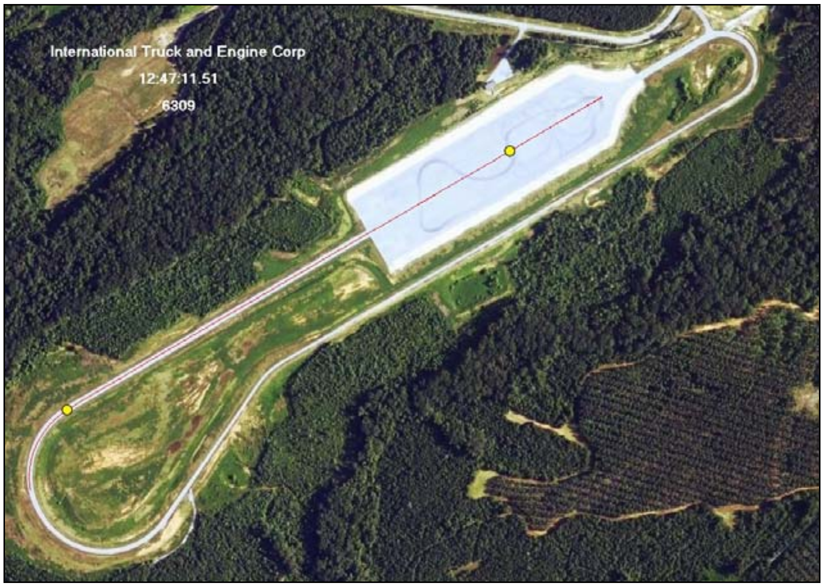


Figure 31. International Truck and Engine VST Demonstration Test at Arterial Speed Vehicle Trajectory Immediately before Stopping (Run 1)

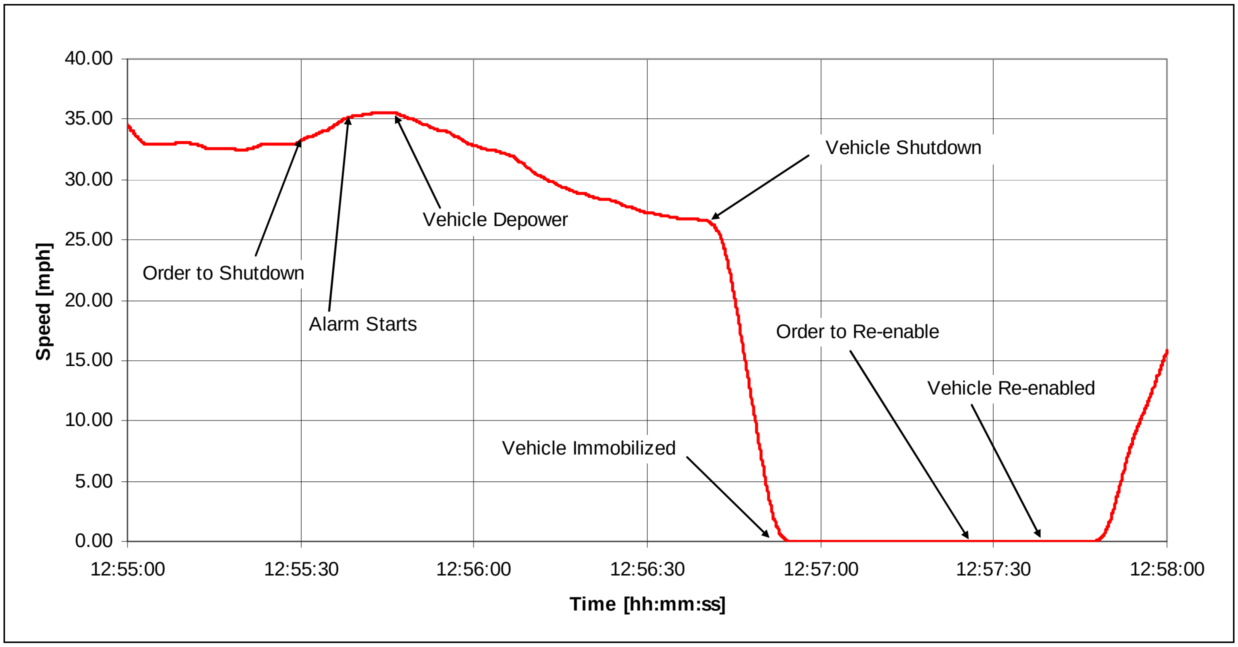


Figure 32. International Truck and Engine VST Demonstration Test at Arterial Speed Run 2 (75% Depower) Speed Profile

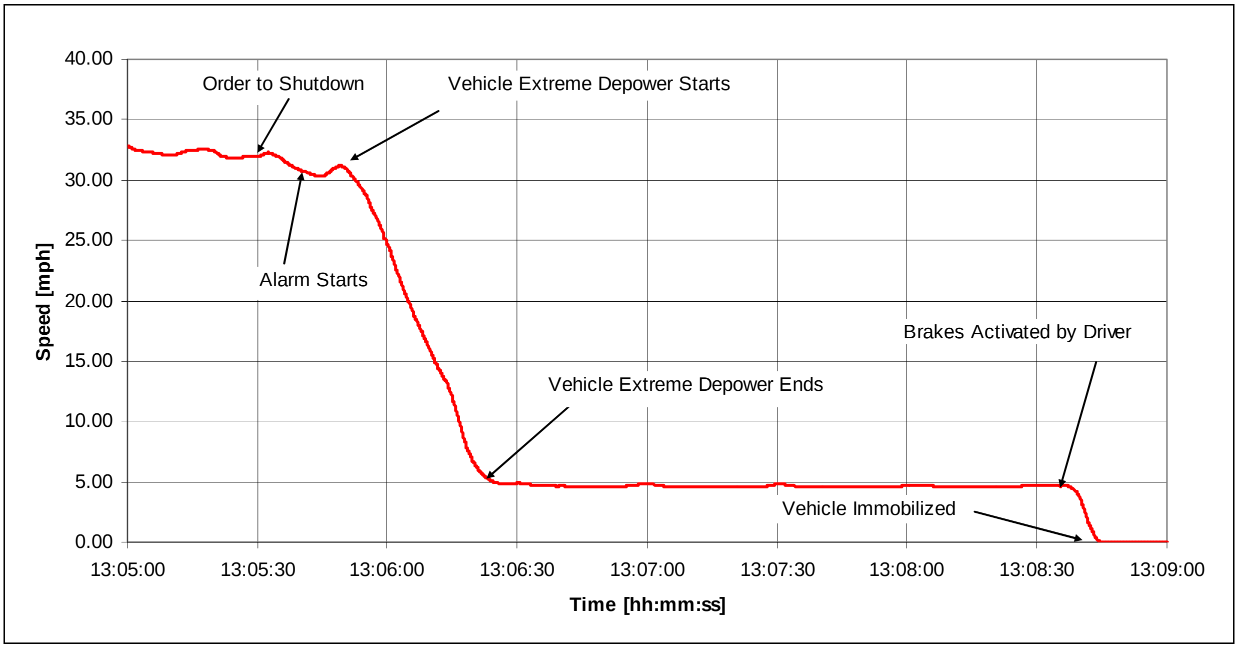


Figure 33. International Truck and Engine VST Demonstration Test at Arterial Speed Run 3 (Extreme Depower) Speed Profile

The results of the International Truck and Engine VST tests show that on average, the company's vehicle immobilization technology required 63 seconds from the instant that the order to shutdown the vehicle was given to the instant at which the vehicle shutdown process started, and for Runs 1 and 2, 83 seconds from when the order to shutdown was given by law enforcement to the instant the vehicle came to a stop. The average deceleration rate after the order to shutdown was given was 1.24 ft/sec^2. Re-enablement required, on average, 110 seconds.

BSM Wireless VST Demonstrations

BSM Wireless (BSM Wireless, 2007) demonstrated their VIT (Figure 34) under two conditions: activation by law enforcement and activation by crossing a geofence. BSM provides a two-stage shutdown process. During the first stage, the engine is set in an idle mode in which pressing the accelerator pedal has no effect on the engine revolutions (i.e., the engine remains idling). This mode causes the speed of the vehicle to decrease at a more dramatic rate than in stage 2. Once the vehicle reaches a speed of 15 mph, the vehicle enters the second stage in which its engine is shut off.

The results of the tests are presented in Table 9 and graphically depicted (i.e., speed profiles) in Figure 35, Figure 36 and Figure 37.

Figure 34. BSM Wireless VST Demonstration Test

The company's VIT uses an engine shutdown technology; therefore, the test events shown in Table 9 are the same as in the case of S3. Also, as described in the last section, the company was required to perform a test at a slow speed (Run 1). The shutdown process started with the issuing of the order by law enforcement (i.e., a researcher traveling in the South Carolina State Highway Patrol vehicle) (Runs 1 to 3) or by crossing the geofence (Run 4); after some time, the alarm indicating that the eVID was activated was heard inside the cabin. This was followed by the initiation of the vehicle engine shutdown process, and after the truck had diminished its speed sufficiently, the driver was asked to apply the brakes until the vehicle came to a full stop.

The results of Runs 1 to 4 indicated that on average, it took 22 seconds to start the engine shut off process from the instant that the order to shutdown the vehicle was issued, and about 30 seconds to re-enable the vehicle. The average deceleration rate from engine shutdown to the instant the brakes were applied was 0.53 ft/sec^2. Because the brakes were applied, the vehicle stop times are, of course, shorter than if the vehicle came to a stop without intervention from the driver. However, the difference is not significant. Consider, for example, Run 2. The 0.67 ft/sec^2 deceleration rate reported Table 9 is an average of a deceleration of 1.1 ft/sec^2 during 31 seconds (from shutdown to about 15.9 mph) and a deceleration of 0.31 ft/sec^2 for 38 seconds (from 15.9 mph until the brakes were applied at 7.7 mph). That is, as can be seen in Figure 35 (and also 36 and 37), this particular vehicle showed two distinct deceleration rates after the shutdown process was initiated. From that moment until the vehicle reached 16 mph, it decelerated at a higher rate than from 16 mph onwards. If the vehicle continued traveling with the second deceleration rate (and the brakes were not applied), it would have come to a stop at approximately 13:58:37; or 2 minutes and 33 seconds after the order to shutdown was issued, instead of the one minute 49 seconds indicated in Table 9 (i.e., a difference of 44 seconds).

Assuming a flat terrain and no application of brakes, the BSM Wireless truck would have traveled 4,220 ft, 4,160 ft, and 1,750 ft for Runs 2, 3, and 4, respectively from the moment the order to shutdown was given to the instant the vehicle came to a complete stop.

Table 9. BSM Wireless VST Tests Results—Slow Speed (Run 1), Arterial Speed (Runs 2 and 3), and Geofence Demo (Run 4)

	Run 1 Clock Time [hh:mm:ss]	Run 1 Elapsed Time [mm:ss]	Run 1 Speed [mph]	Run 2 Clock Time [hh:mm:ss]	Run 2 Elapsed Time [mm:ss]	Run 2 Speed [mph]	Run 3 Clock Time [hh:mm:ss]	Run 3 Elapsed Time [mm:ss]	Run 3 Speed [mph]	Run 4 Clock Time [hh:mm:ss]	Run 4 Elapsed Time [mm:ss]	Run 4 Speed [mph]
Order to SD*	13:51:08	00:00	16.40	13:56:04	00:00	34.20	14:02:32	00:00	36.60	14:08:37	00:00	26.10
Alarm	13:51:14	00:06	16.10	13:56:09	00:05	34.20	14:02:38	00:06	39.50	14:08:38	00:01	26.00
Vehicle SD	13:51:16	**00:08**	15.50	13:56:40	**00:36**	39.10	14:03:08	**00:36**	35.40	14:08:43	**00:06**	25.00
Brakes App.	13:51:52	**00:44**	8.79	13:57:49	**01:45**	7.71	14:03:49	**01:17**	13.50	14:09:47	**01:10**	7.47
Veh. Stop	13:52:01	**00:53**	0.00	13:57:53	**01:49**	0.00	14:03:55	**01:23**	0.00	14:09:54	**01:17**	0.00
Dec. (fps^2)			**0.28**			**0.67**			**0.78**			**0.40**
Order to RE	13:52:10	00:00	0.00	13:57:58	00:00	0.00	14:04:05	00:00	0.00	14:10:36	00:00	0.00
Veh. RE	13:52:39	**00:29**	0.00	13:58:26	**00:28**	0.00	14:04:07	**00:02**	0.00	14:11:03	**00:27**	0.00

*For Run 4, crossing the geofence boundary triggered the device.

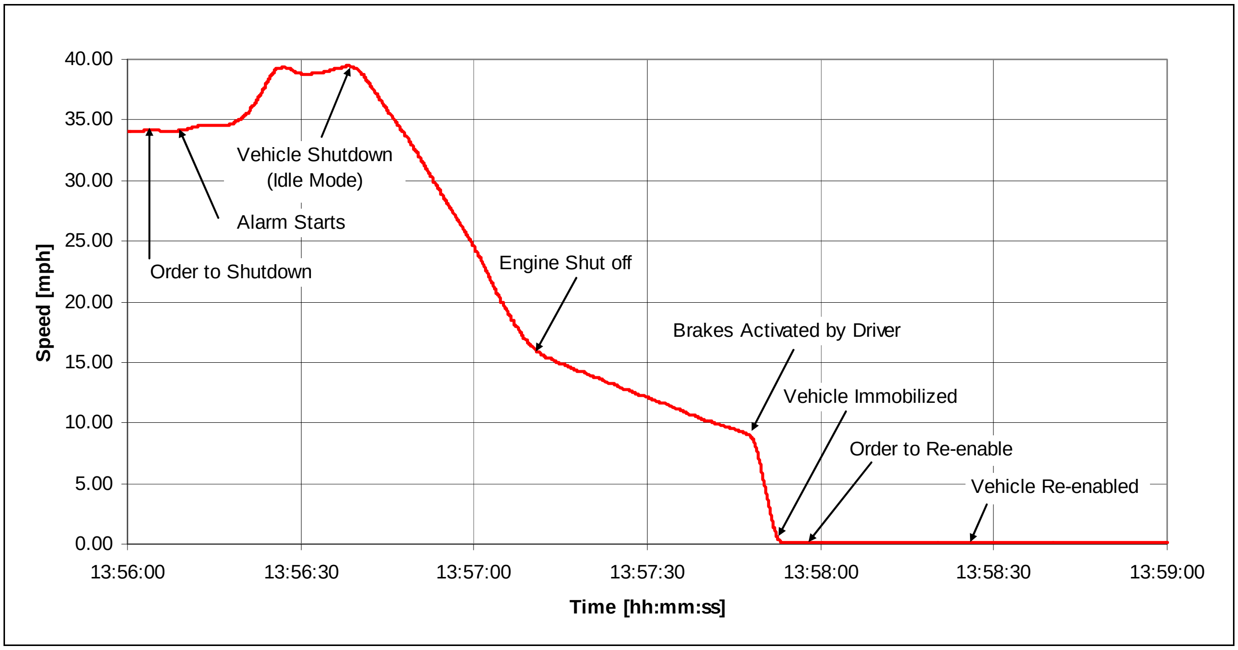


Figure 35. BSM Wireless VST Demonstration Test at Arterial Speed Run 2 Speed Profile

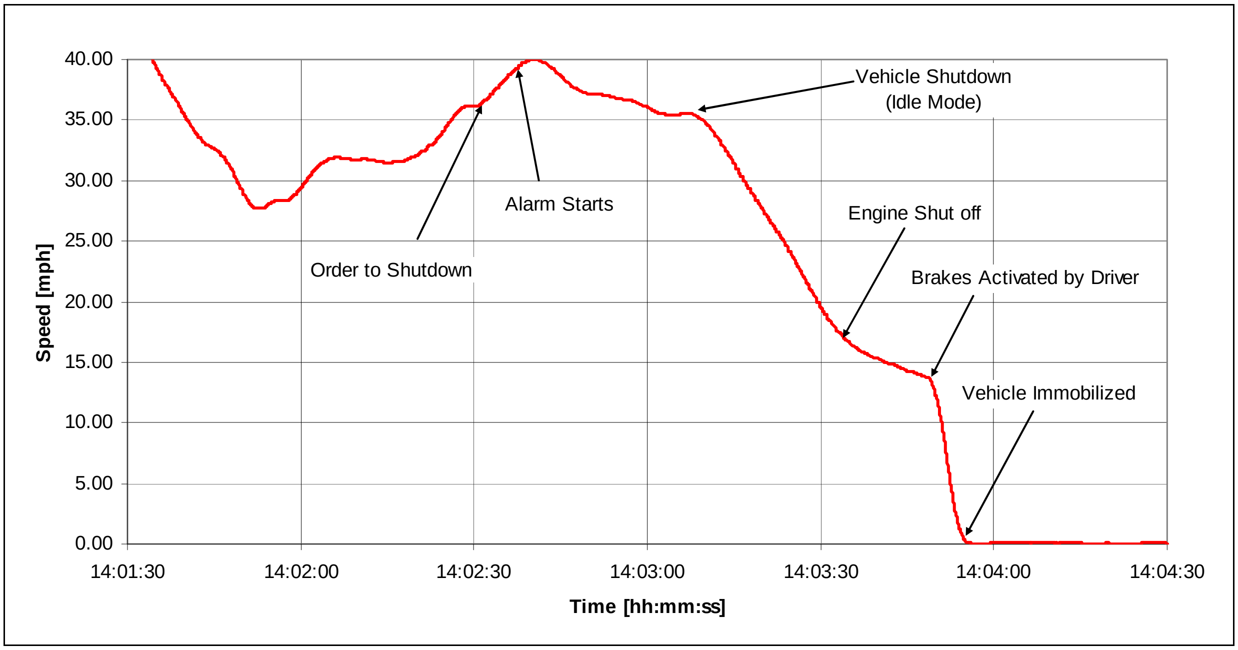


Figure 36. BSM Wireless VST Demonstration Test at Arterial Speed Run 3 Speed Profile

In the last run, Run 4, BSM Wireless demonstrated their VIT Geofence (or geozone) capabilities. In this case the eVID was activated when the vehicle crossed the geofence (see Figure 8). Because the geofence coordinates were resident in the onboard system, it took only one second for the system to sound the alarm (i.e., activate the vehicle immobilization device).

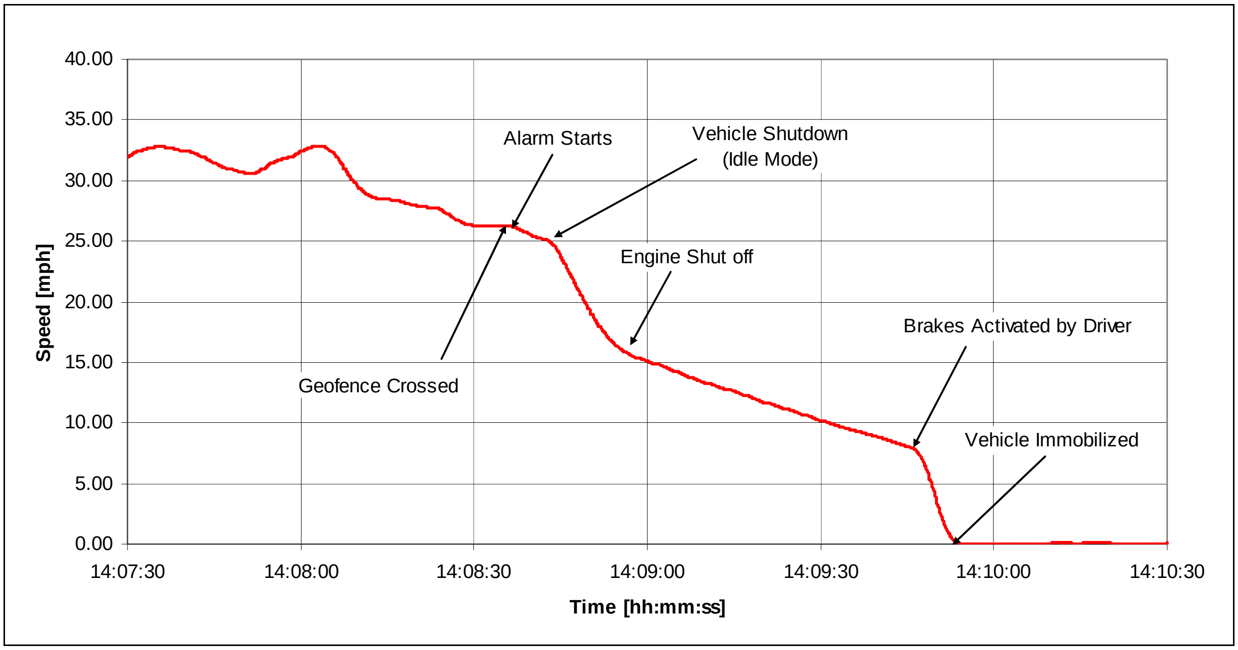


Figure 37. BSM Wireless VST Demonstration Test at Arterial Speed Run 4 (Geofence Demo) Speed Profile

GlenHugh Enterprise (autoWATCH) VST Demonstrations

The last company to demonstrate its VST at LPG in February 2007 was GlenHugh Enterprise (GHE), which used a class-8 truck for the tests (see Figure 38). Because of some minor technical difficulties, it was only possible to demonstrate the autoWATCH technology in two runs: a VIT geofence demonstration test (Run 1) and a vehicle shutdown at arterial speed demonstration (Run 2). The results of these runs are shown in Table 10 and the corresponding speed profiles for the last three minutes before the vehicle came to a stop are illustrated in Figure 39 and Figure 40.

Figure 38. GlenHugh Enterprise VST Demonstration Test

Table 10. GlenHugh Enterprise VST Tests Results—
Geofence Demo (Run 1) and Arterial Speed (Run 2)

	Run 1 Clock Time [hh:mm:ss]	Run 1 Elapsed Time [mm:ss]	Run 1 Speed [mph]	Run 2 Clock Time [hh:mm:ss]	Run 2 Elapsed Time [mm:ss]	Run 2 Speed [mph]
Order to SD*	14:48:38	00:00	34.00	15:55:03	00:00	30.5
Alarm	14:48:43	00:05	34.20	15:55:42	00:39	33.8
Vehicle SD	14:48:50	**00:12**	34.30	15:56:10	**01:07**	33.6
Brakes App.				15:57:28	**02:25**	14.8
Vehicle Stop	14:49:17	**00:39**	0.00	15:57:39	**02:36**	0.00
Dec. (fps^2)			**1.86**			**0.35**
Order to RE	14:49:53	00:00	0.00			
Vehicle RE	14:49:59	**00:06**	0.00			

*For Run 1, crossing the geofence boundary triggered the device.

The VIT geofence run showed that it required only five seconds for the system to determine that the boundary of the protected zone was crossed and to activate the eVID. Seven seconds later, the shutdown process was initiated and brought the vehicle to a stop 39 seconds after the geofence was crossed. The speed profile shown in Figure 39 indicates two clearly distinct deceleration rates after shutdown. However, as opposed to the demonstration vehicles used by S3 and BSM Wireless, the second deceleration rate was larger than the first one. The driver only applied the brakes when the vehicle was traveling at less than one mph, so the total deceleration rate for this run was 1.86 ft/sec^2, second only to that shown by the International Truck and Engine demonstration vehicle in their first run.

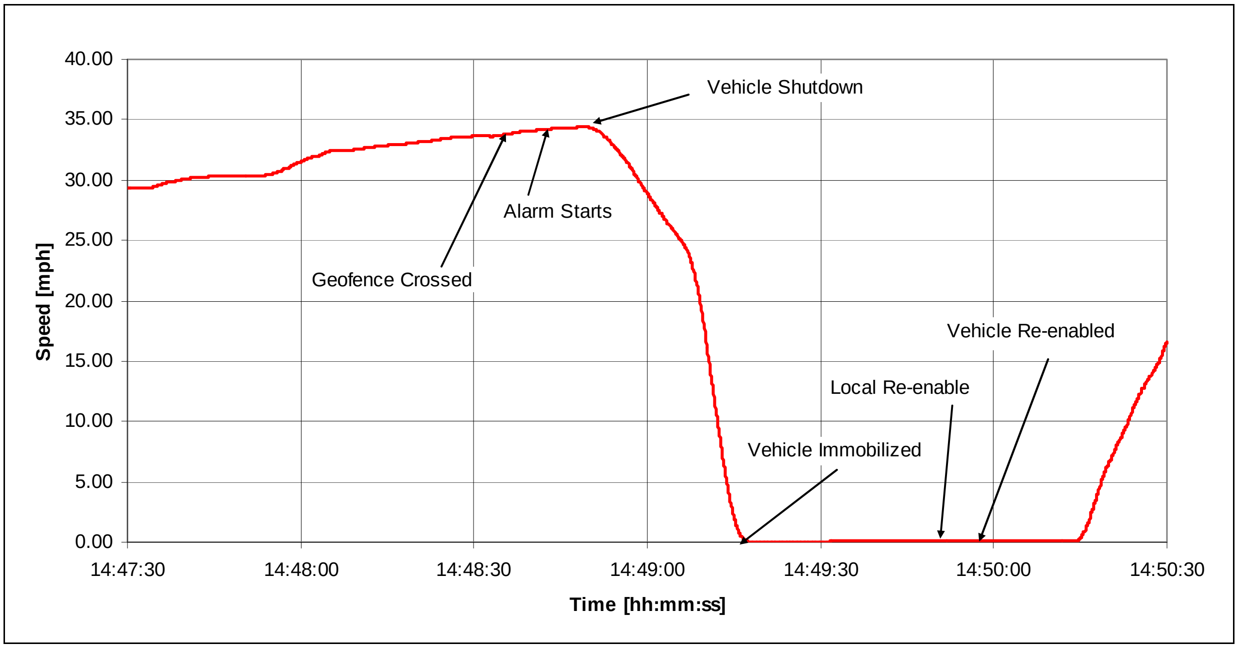


Figure 39. GlenHugh Enterprise Demonstration Test at Arterial Speed Run 1 (Geofence Demo) Speed Profile

Run 2 of GlenHugh Enterprise was a demonstration of remote vehicle shutdown in which law enforcement initiated the shutdown process. The order to shutdown the vehicle was given when the truck was traveling on the southwest curve of the test track, indicated in Figure 41 with a yellow circle. Thirty-nine seconds after that, the eVID was triggered while the truck was on segment E-F (second yellow circle in Figure 41). Although the engine was in a dying mode, it was possible for the driver to negotiate, with no problems, the northeast curve of the track before the vehicle came to a complete stop (in this case the driver applied the brakes when the vehicle was traveling at about 15 mph as shown in Figure 40). Assuming a flat terrain and that the vehicle would have continued decelerating at the same rate that was experienced just before the brakes were applied, the GHE truck would have traveled 7,000 ft (1.33 miles) from the instant that the order to shutdown was issued to the instant the vehicle would have come to a stop.

Only one local vehicle re-enable test was performed (at the end of Run 1), and that required only six seconds for the driver to be able to re-start the vehicle.

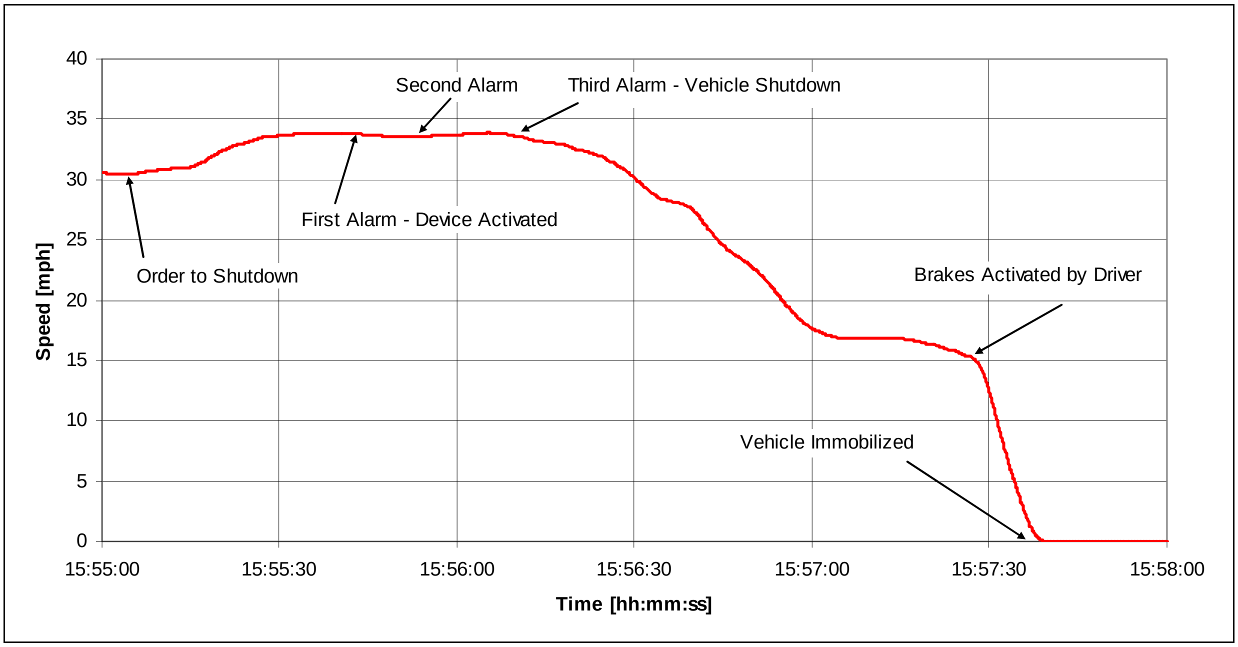


Figure 40. GlenHugh Enterprise VST Demonstration Test at Arterial Speed Run 2 Speed Profile

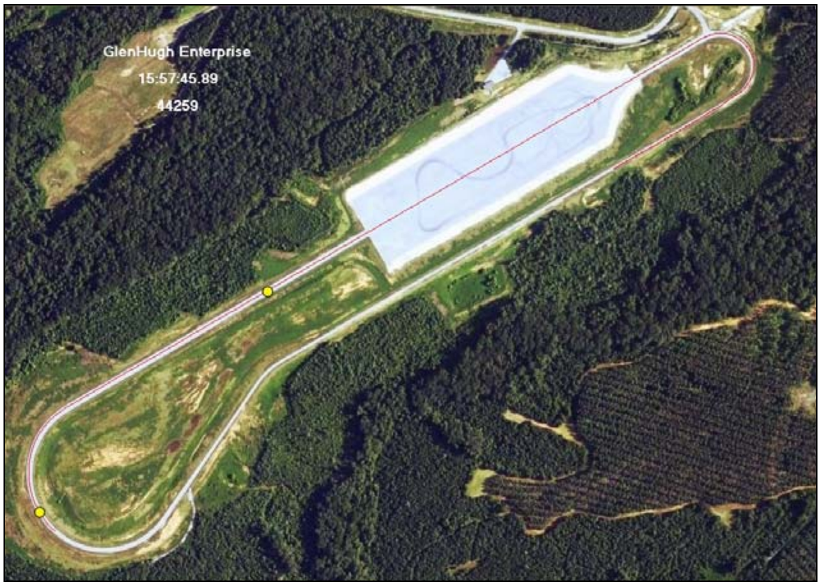


Figure 41. GlenHugh Enterprise VST Demonstration Test at Arterial Speed Vehicle Trajectory Immediately before Stopping (Run 2)

3.3 DEMONSTRATION TESTS CONCLUSIONS

All the participating vendors successfully demonstrated their VDT and VST products, which were documented through videotaping. For FR1, different technologies were demonstrated including swipe cards (S3), proximity cards (BSM Wireless), keypads (MAGTEC, Qualcomm, International Truck and Engine, and BSM Wireless), and transponders (GlenHugh Enterprise). Two companies (MAGTEC and BSM Wireless) demonstrated how their technologies were able to disable the vehicle in response to a loss of signal (FR2) event. No company demonstrated FR2 for a shutdown situation. For FR3, a panic button (S3) and a key fob (BSM Wireless) were demonstrated. Also related to this FR, MAGTEC and BSM Wireless demonstrated their “under-duress” code entry capability, and GlenHugh Enterprise showed a technology that arms itself every time a cabin door is opened.

The vendors also showed a variety of VSTs (FR4 and FR5). Those included engine shutdown technologies (S3, International Truck and Engine, BSM Wireless), engine power degradation technologies (International Truck and Engine, GlenHugh Enterprise), and speed control technology (MAGTEC and Qualcomm). International Truck and Engine demonstrated how different levels of engine power degradation could be implemented by sending different messages to the vehicle to be shutdown. In the same way, although not demonstrated at this event, MAGTEC and Qualcomm can change the parameters governing the total time to shut off the vehicle wirelessly.

The tests provided a first-hand understanding of how these different vehicle immobilization technologies are triggered and activated. The tests were also used to investigate the level of vehicle control by the driver once the shutdown sequence started and until the vehicle reached a complete stop. The most sophisticated technologies allowed for a gradual speed reduction during the shutdown process in which all of the vehicle functions are available to the driver. The only exception is that the driver cannot accelerate the vehicle above a speed threshold, which is constantly decreasing during the shutdown sequence, but otherwise he/she can maintain complete control of the vehicle. Depower technologies work in the same way (i.e., the driver has complete control of all of the mechanical functions of the vehicle during the shutdown process except for the ability to accelerate), but in a shorter spatial and temporal interval.

The simplest VSTs demonstrations consisted of technologies that shutdown the engine completely, with the consequence that the vehicle mechanical functions cease to operate. Nevertheless, because of residual air pressure in the brake system, some of those functions are still available to the driver until the service brake reservoir is depleted. The tests demonstrated that even for these technologies, the vehicles did not experience any significant loss of maneuverability. Although the demonstrated VSTs were tested in a controlled environment, it does not appear that these technologies would have had an impact on the stream of traffic different from what, for example, a vehicle that runs out of gas would have produced. However, steering may present some problems, especially for loaded vehicles facing even moderately sharp curves.

The tests also provided an indication of how long it takes from the instant that the order to shutdown the vehicle was given to the instant that it comes to a stop, as well as the time it takes to re-enable the vehicles. Both measurements strongly depend on the type of technology and communication used. In general, for engine shutdown technologies and cell phone communications, it took, on average, 30 seconds from the time the order to shutdown was issued by law enforcement to the time the shutdown process was initiated. The average was 64 seconds for technologies that degrade the engine performance. For acceleration control technologies, this number depends on the parameters entered in the system. The remote re-enabling of the vehicle took, on average, 52 seconds. All the VST tests used cellular communications (note: Qualcomm used satellite communications, but the demonstrations were limited to driver authentication technologies with a stationary Celadon truck; however, vehicle remote disabling was demonstrated and the elapsed time between the instant that the order was given and the engine shutoff was measured at about 80 seconds, only slightly longer than the elapsed times observed for cellular wireless communication technologies).

Stopping distances depend on many factors, including topography, speed at which the vehicle is traveling when the eVID is activated, the type of VIT, and the way in which the vehicle is driven (e.g., whether the driver maintains the maximum possible speed or not). Because of the dependency of these factors on the particular situation in which a vehicle is to be shutdown, it is not possible to generalize regarding these parameters. Nevertheless, some technologies, specifically those that allow changing parameters wirelessly, offer better control over the maximum expected distance that a vehicle would travel after shutdown.

4. CASE STUDIES

Previous sections of this report presented technical and other VIT issues from the perspective of the technology vendors. Although those vendors are providing products that are market driven and are continuously capturing and incorporating attributes that customers require in their products and services, a more in-depth understanding of the perceived/real benefits and costs that a VIT deployment in the real-world involves is necessary for completeness. For this purpose, three carriers using VITs provided by three of the vendors that participated in this project were interviewed. These transportation companies included: (1) a large high-value carrier, Celadon Trucking, (2) a large hazmat transportation carrier of bulk flammable liquids that, because of security reasons, preferred to keep its name anonymous, and (3) a small hazmat carrier of bulk flammable liquids, Swain Oil Transport. A large commercial insurance brokerage firm, First Horizon Insurance Inc., providing risk management services, insurance, and bonds to commercial clients, including the transportation industry, was also interviewed. The results of these interactions are presented below.

4.1 HIGH-VALUE CARRIER: CELADON TRUCKING

Celadon Group, Inc. is a publicly-traded truckload carrier with a fleet of approximately 2,900 trucks and 7,600 trailers that, through its subsidiaries, provides service across the United States, Canada, and Mexico.

In the United States, Celadon's corporate headquarters, including its dispatch office, are located in Indianapolis, while the subsidiaries are dispatched from their respective countries, Canada and Mexico. The company transports diverse freight. It started with auto parts and has diversified its business to a point where no single customer accounts for more than 5% to 6% of the total volume transported by Celadon.

The information below was the result of discussions with Mr. Bruce Wishart, Celadon's Director of Security.

4.1.1 VIT System at Celadon Trucking

When the decision was made to incorporate VITs into their fleet, Celadon was already a 20-year customer of Qualcomm and was using their location and communication services for their entire fleet.

The main criteria used in the decision for adopting a VIT system were the security of the freight and, more importantly, the safety of the driver (note: Qualcomm uses the MAGTEC VIT system, see Sections 2 and 3 for more information about this VIT device). The driver authentication technology was viewed as a very powerful feature that almost eliminated the need for tracking a vehicle (for security purposes) since the technology makes it very unlikely that someone would be able to steal the vehicle. The company identified the proactive approach offered by the driver authentication component as critical and was the main focus of the decision to adopt VIT. It viewed the (remote) disablement of the vehicle as an added feature that it probably would not have to use except in very rare occasions, such as an internal theft, a disgruntled driver, or in a hijack situation where the driver has no control over the situation. Even though the company only expected to use the vehicle stopping capabilities very rarely, the features of this VIT system that ensures a safe shutdown of a vehicle for both the driver and the public were additional factors in making the decision to adopt this particular technology.

The VIT system at Celadon consists of Qualcomm's Vehicle Command and Control (VCC) coupled with MAGTEC's immobilization technology. It was deployed initially on 100 vehicles for beta testing and has expanded to about 200 trucks as of the end of June 2007. The company policy is to deploy this technology mainly for their high-value cargo (the company only transports a minimal amount of hazmat). It was pointed out that the technology may not be required for every application (e.g., low-value cargo); therefore, the decision should remain a company decision and not be a mandate.

Installation

The installation of the eVIDs was performed by MAGTEC's representatives onsite. Although, as indicated previously, all of the Celadon trucks already had the Qualcomm unit on board (GPS and communications), the installation of the VIT units required an additional 3-4 hours for complete installation. This was primarily due to the fact that this was relatively high-tech equipment, and it was important that it be done carefully to avoid subsequent problems. Once the installation of the unit had been completed, it was integrated into the Qualcomm system. The eVID, which has its own particular NCP (network control protocol) number, will not work with any other Qualcomm unit unless it is re-programmed. After this installation, the truck is ready to be assigned to a driver.

Training

Celadon has a training department that has developed a training protocol and a companion book to instruct Celadon drivers' managers, supervisors, and operation personnel on how to operate and work with the VCC system. Initially, the company was apprehensive about safety issues that may arise when shutting down a vehicle on public roads. However, after Celadon conducted extensive tests in a controlled environment, the company realized that, because of the way in which this particular technology works, safety concerns and endangerment to the public were minimal in terms of consequences.

Regarding the drivers, they receive a short, one-to-two hour training course. In this training, an overview of the system and its capabilities is presented, alongside instructions and demonstrations on how to use the keypad, how to start the truck, how to proceed when the truck has to go into maintenance, how to configure the device when the driver has to stop and take a break, and other situations that may be encountered by the drivers while operating their vehicles.

The reason that the training period is so short is that the system is very driver-accommodating (i.e.; the unit is designed to take the driver out of the equation). As pointed out by Celadon, "other technologies have to be engaged by a person and are only good if the person remembers to operate them; this technology eliminates that requirement." For example, if the driver forgets to input the code when he/she takes a break, then the device arms itself as soon as the parking brake is engaged. The driver can even leave the engine running. If someone touches the brake, then the device will shutdown the engine unless the correct override code is entered. In other words, the driver is not required to perform any dedicated tasks devoted to the system since the default setting of the device is armed.

System Operation

Celadon has an equipment control manager (ECM) that assigns trucks to new drivers. When a new driver is to be assigned to a truck that has the Qualcomm/MAGTEC unit, the ECM accesses the VCC system through its website, enters the driver information (name, code, etc.), and then issues the information to that driver. The actual command and control of that vehicle is then passed to the driver's manager.

If during the day-to-day operations, the driver enters a wrong code several times, the system goes into a tampering mode and several managers get a notification (e.g., an e-mail into a blackberry device). The protocol then calls for these managers to contact the driver to determine the nature of the problem and proceed accordingly. In some cases, and depending on the situation, the triggering of a shutdown procedure may follow. If that were the case, the shutdown procedure can be initiated with just the approval from the Operations Supervisor and/or driver managers (DMs). At the beginning of the VIT deployment, the company's Director of Security and VP of Safety had to be notified and they were the only ones authorized to initiate the shutdown procedure. However, after the tests conducted by Celadon, which underscored the high level of safety with which this technology can achieve a vehicle shutdown, this requirement was relaxed and currently it only requires approval from the Operations Supervisor or DM, who receive training on this particular issue and know when and how to implement the shutdown procedure. The ECM had no operational function with the VCC after the initial entry/removal of new drivers.

In addition, since the system allows changing the code or password over the air, if there is an internal problem (e.g., a problem with a driver), the managers can change the code through the Qualcomm system and block a driver from driving the vehicle.

Celadon had a few instances where the VIT was activated, but these events were due to driver error (i.e., a wrong code was entered). Thus far, the company has not had to shutdown a truck traveling on public roads; however, they have had a real-world instance of shutting down a vehicle in a parking lot and changing the code over the air to impede a driver from moving that vehicle. This was done during a controlled theft simulation of a high-risk load, conducted by the VP of Operations and the Director of Security. The simulation was not disclosed to anyone in the company until it was completed. Operations followed all of the high-risk procedures and initiated the shutdown; the operation was considered to be 100% successful.

As discussed in Sections 2 and 3, this technology has other capabilities such as VIT-based geofencing and vehicle disablement due to loss of signal. Celadon has chosen not to implement the geofencing capabilities on their day-to-day operations (they only use it for inventory control) because sometimes due to accidents or road closures, for example, the driver has to deviate from his/her assigned road, which could trigger an involuntary truck shutdown. Celadon has also not enabled the loss of signal capability. Also, at the present time, the company does not use the system to keep track of hours-of-service and other related information.

4.1.2 VIT System Costs and Benefits

Besides the training costs, which were estimated to be minimal, the VIT system also incurs maintenance and operating costs.

Maintenance

The system is very reliable and requires minimal maintenance. Celadon encountered only one problem with the system, which was related to the keypad in 50 of its units. This was a manufacturer's problem resulting in the keypad having functionality in only one digit. Although it was still possible in this situation to give an access code to the drivers (using just a single digit) in order to start the vehicle, the security of the system was severely reduced. MAGTEC replaced all these keypads and they have not had this or any other widespread problems since.

There were, however, some isolated problems derived mostly from driver errors or misinformation. For example, in one instance, a driver installed a power inverter in the truck to be able to connect some appliances (a refrigerator and other devices). This caused an overload of the electrical system, which in turn caused the device (keypad) to operate incorrectly and impeded the driver from entering his access code to start the truck. Celadon contacted MAGTEC's 24-hour technical support and the problem was solved over the air (i.e., by asking questions to the driver over the phone).

Operating Costs

The VIT system operating costs are minimal since it takes only a few minutes per driver to enter the code and other system relevant information; additionally, the company did not have to add any extra employee to operate the VIT system and support the new capabilities it provides. The additional monthly costs are also minimal (about $5.00/truck), since Celadon already had the Qualcomm GPS/communications system in all of their vehicles. The system also requires some upfront disbursement to buy and install the eVID units. For a generic MAGTEC customer, these amount to about $1,300/unit plus $515/unit for the installation (see Table 2; notice also that most vendors offer quantity discounts and that the prices listed in that table are for just one unit). Celadon investigated the feasibility of leasing the equipment from MAGTEC, however, the company opted to own the equipment.

Benefits

The tangible benefits that the VIT can bring to the company could be substantial. During the interview, it was mentioned that there had been a theft recently of a truck (belonging to another company) carrying $5M in pharmaceuticals in West Memphis, Arkansas. Having VIT deployed in that one truck would have paid for the substantial part of the system for the entire fleet.

Celadon also had an instance in which the VIT system would have helped; unfortunately, this incident involved a truck that did not have the eVID deployed (note that Celadon is just starting to add this system to its fleet). The case involved a driver who disconnected the Qualcomm device in Memphis, TN, and traveled to Baltimore, MD. Just the fuel itself for this 800-mile trip and the salary of the people who were associated with tracking the vehicle (the MD Highway Patrol found the truck) and bringing it back to Indiana would have been enough to pay for the device. A quick calculation of these savings was computed at about $1,330 for the recovery of the vehicle (i.e., 800 miles @ 5.1 mpg X $2.75 per gal of fuel = $ 431.48, plus $300.00 recovery fee and about 20 total man hours @ $30.00 per hour = $600). In this particular circumstance, the intention of the driver was not to steal the cargo; if that were the case, with the cost of the load, the savings would have been over $2 million.

However, from the perspective of Celadon, one thing that outweighs any monetary gain that the system could provide is the peace of mind that it brings to the company managers and customers, especially when transporting high-value cargo. The system also provides a deterrent; that is, a disgruntled driver would think twice before stealing the truck since he knows that the VIT-instrumented truck could easily be stopped.

Risk Reduction

Most, if not all of the large carriers in the United States, including Celadon, are self-insured. The use of VITs significantly reduces the risks of theft or hijacking and, in consequence, reduces the expected losses that thefts could impose on the company. In addition, this reduction in risk increases customer confidence that Celadon can haul their freight securely and not have it stolen. Moreover, although Celadon does not specialize in high-risk freight, because of the confidence that the technology brings to the company, they are not averse to taking on this type of cargo.

4.2 LARGE HAZMAT TRANSPORTATION COMPANY

This case study involves a large hazmat transportation company that covers the entire United States, but involves mostly local operations. The company has its own fleet and also works with independent contractors to increase coverage. Both the company's trucks and the subcontracted vehicles have the VIT deployed.

Due to security concerns, the company preferred to remain anonymous in this report (the company will be referred as LHMT hereafter). The information below was provided by two managers, the company's national fleet manager, and a manager in the United States logistics department.

4.2.1 VIT System at the LHMT

Both of these managers were part of the original decision-making group that some years earlier was in charge of evaluating and making recommendations regarding the adoption of a VIT system for the LHMT. The main needs that the group addressed were: (1) driver security and protection, (2) product security and protection, and (3) the ability to remotely locate and shutdown a truck. These were the system requirements that the company used to identify the VIT system and its vendor (which was one of the vendors interviewed in this report). The entire fleet was then equipped with the technology.

At the present, the national fleet mangers are in charge of the LHMT VIT system, overseeing its operation and making sure that all of the system components, including all the eVID units, are functional and in perfect working order. The fleet manager is also tasked with keeping the technology up-to-date.

Installation

The adopted system is similar to the one shown in Figure 1 of this report (note: prior to the adoption of the VIT system, the LHMT did not have any vehicle tracking technology deployed in its fleet). The installation of the system, specifically the eVIDs, was performed by the LHMT after the appropriate personnel were trained by the vendor/developer of the technology. Installation took around two hours per vehicle.

Training

All of the company's drivers, fleet managers, area managers, and personnel at the dispatch center receive a training course, which can vary from between four and eight hours, depending on the trainee function and the different and relevant aspects of the VIT system for the respective functions.

The drivers go through eight hours of training that instructs them on how every component that is relevant to their mission works, what to expect under different situations, and the different ways to use the system. The main objectives in designing this extended training for the drivers was that the LHMT wanted to make sure that their drivers were very familiar with the system in order to enhance their comfort in using it, and also to minimize, or completely avoid subsequent and associated downtime. The training is a one-time event. Everyday use of the system maintains high levels of familiarity and experience.

The managers of the system (i.e., fleet managers, area managers, and dispatchers) take a shorter, four-hour training session to learn how to use the system, get trained on the web-based application that is used to access and change related information such as the type of data requirements, learn how and when to make changes, and other relevant tasks. This is also a one-time training event, but everyday use of the system maintains high levels of familiarity and experience.

Besides these managers, the company also has other employees that act as administrators of the system. Those administrators, who also receive a four-hour training course, have as their main mission, the task of overseeing the entire system database in order to ensure its correctness—they deal with tasks such as certifying that the pin numbers are assigned correctly and that driver authentication information is up-to-date. These administrators are the company's personnel who interact with the system the most.

System Operation

After deploying the VIT system, the company noted that they did not have the need to add anyone to their staff to manage it; the new tasks that resulted from the deployment were absorbed by existing personnel. It did require, however, that the LHMT give the responsibility for specific parts of the system to different managers that oversee the fleet. For example, after the VIT system was deployed, when assigning a driver to a truck, more information than what was previously required needed to be entered into the system (e.g., authentication codes). Overall, the experience of the LHMT is that a day-to-day management of the system is not required; only when there is a need to assign or re-assign a driver to a truck would it necessitate providing or updating new information to the system. This is done through a web-based application.

In the LHMT VIT system, each driver has a personal PIN and is assigned to a specific truck. If it becomes necessary for a driver to operate a different truck, then he/she is assigned to that truck by the manager through the VIT system web-based application. If the managers have any problems, then they contact the system administrators. Those system administrators are also responsible for initiating any VIT-based shutdown procedures.

The company has conducted (and conducts) tests with moving vehicles. Those tests, which are conducted at the company's vehicle maintenance facilities, have shown that the adopted VIT produces a controlled shutdown of the truck with the driver never losing control of the vehicle. These tests are also used to corroborate that the vehicles are in fact disabled and cannot be driven away. The onboard system is tested every time the truck has scheduled maintenance (e.g., about three times a year). There have been some accidental activations of the system, but those occurred in the early deployment stages, and after small changes were introduced, the system became very stable.

The driver authentication part of the system is, of course, used everyday so that the vehicles can be started and driven. To disable a vehicle, the drivers have three different options: (1) through the onboard keypad, (2) using the remote system (i.e., key fob), or (3) by sending an alert.

The LHMT has also had the opportunity to use the remote shutdown capabilities of the VIT system in a real-world situation. This is the only corroborated real-world shutdown of a moving vehicle that has occurred in the United States. The incident was a hijack case wherein the driver was abducted and placed in the trunk of one of the hijacker's cars. However, before that happened and as soon as he realized that his truck was being hijacked, the driver activated the alert system, indicating that there was something wrong. The company's managers proceeded with the established protocol that requires them to contact the driver. Because they were not able to do so, the company went to the next step, that is, the initiation of the vehicle shutdown procedure. Law enforcement was involved in this event and the LHMT shutdown the vehicle when it was determined that the driver was not in danger. The vehicle was successfully stopped; however, the hijacker was not apprehended because he abandoned the truck as soon as he realized it could not be accelerated. Using the system, the vehicle's location was identified, which aided the police in quickly locating the truck and recovering it with the cargo intact. The apparent main motivation for the hijack of this vehicle was a monetary one (the truck and cargo were valued at $250K). However, the path of the vehicle would have taken it by a public facility (a hospital); it is not known if that was coincidental to where the thief was trying to take the truck. For the company, the main benefits were the ability to track the unit and have police dispatched immediately, as well as impeding the vehicle from traveling any distance by shutting it down remotely.

The LHMT does not use the technology for fleet management purposes. The system also has the ability to implement geofences, but the company is not using this capability at the present time. However, in the future the company expects to implement this capability so that if the vehicle strays off course more than an established number of feet/miles from its prescribed route, then the dispatcher and fleet managers will get notified and, if required by the particular circumstances, could react immediately.

4.2.2 VIT System Costs and Benefits

Three main cost items are part of the LHMT VIT system: the cost of the training the drivers, managers, and system administrators have to take; system maintenance costs; and system operating costs. Training costs are a one-time expenditure, and although higher than those incurred by Celadon on a per capita basis (i.e., eight hours versus two hours for the drivers), they can still be considered minimal.

Maintenance

The LHMT has found that the devices are very reliable and the company only had to replace some of the key fob devices because of malfunction problems. On a regular basis, the only maintenance requirement is the replacement of the key fob batteries; however, the system is also tested every time a truck goes for its scheduled vehicle maintenance. Overall, maintenance costs are minimal.

Operating Costs

Regarding labor costs, the system requires only a minimal amount of time for the managers and administrators to update the information when a new driver is added, an existing driver is re-assigned, or an existing driver leaves the company and is deleted from the database. Overall, the labor costs associated to the VIT system are minimal. Other operating costs include the monthly fees that the company pays to the VIT technology provider. The system also requires an upfront one-time disbursement to buy and install the eVID units, which, for a generic customer like that of the LHMT technology vendor, is in the $1,000-$1,500/unit range, including installation. The company bought 450 units.

Benefits

One of the main benefits identified by the LHMT is the increased security that the VIT system brings. The ability to track their vehicles and shut them down if necessary gives management “peace of mind” as indicated by both interviewees. The VIT system is very important for the drivers as well, who feel not only very secure, but also that the company is proactively taking care of their personal safety and well being. Besides these intangibles, the company had a real-world case in which, because it had the VIT system deployed, was able to recover a truck with its cargo intact with a benefit of $250K.

Risk Reduction

Because the LHMT is a large company, it is self-insured. The benefit that the VIT system brings manifests itself in risk reduction.

4.3 SMALL HAZMAT TRANSPORTATION COMPANY: SWAIN OIL TRANSPORT

Swain Oil Transport is a small San Diego, California-based petroleum hauler that started business in 1994 with a single tractor-tanker combination. At the time of this interview, the company had a fleet of nine tankers and 18 drivers, and had recently announced plans to expand operations into Arizona and Nevada. The company's drivers handle, on average, six and four loads during the day and night shifts, respectively. The business strategy of Swain is on building strong relationships with its customers by providing personalized and flexible service.

The information below was provided by Doug Kenner, Swain Oil Transport Operations Manager.[9]

4.3.1 VIT System at Swain Oil Transport

Because of its customer-oriented and flexible service business philosophy, Swain Oil relies strongly on technology to accomplish its mission. This, together with the fact that after 9/11, the company's operating costs, particularly insurance premium costs, increased substantially, were the main triggers for Swain to investigate the utilization of VIT in its fleet.

The main criteria used in the decision of adopting a VIT system were to increase driver safety and cargo security, the need for a communication and vehicle tracking capability, and to increase the company's productivity through a system that could provide added capabilities such as, for example, tracking drivers' hours-of-service.

The company selected Satellite Security Systems as the VIT technology provider because it offered an easy-to-use, web-based, vehicle tracking capability, improved security through their vehicle disabling/shutdown technology, and was cost competitive (a very important factor for a small company such as Swain Oil).

Installation

The installation of the eVIDs was performed by Satellite Security Systems and it took about 45 minutes per vehicle.

Training

The system is very easy to use and requires very little training of the drivers since its authentication system consists of a swipe card (see Sections 2 and 3 for more details about S3's VIT). The managers of the VIT system required little training as well since they only needed to get familiar with the web-based application for tracking and information entering purposes and because their intervention in the shutdown process is minimal (i.e., the VIT provider used a vendor-based control system and a large part of the vehicle shutdown protocol was handled directly by S3).

System Operation

The driver authentication component consists of a swipe card system. The truck cannot be started without the driver swiping his/her driver's license (or any card with a magnetic strip that has been programmed to do this) to allow the system to check whether that person has been authorized to drive the vehicle. (Note: in future versions of the system, it is expected that this

[9] As of April 30, 2007 Swain Oil Transport was sold and changed management personnel; Mr. Keener is no longer with the company.

identification procedure will be conducted using biometric technology.) The carrier, through the system web-based interface, can add or delete particular drivers.

If the driver is not identified, then the S3 center (called the Monitoring and Support Center or MSC) is notified and the vehicle is disabled. To re-enable the vehicle, a call by an authorized person at Swain Oil has to be made to the MSC to reactivate the eVID. In the case of a shutdown event, as soon as the problem is identified and it is determined that a such procedure is warranted, the protocol at the MSC calls for activating the vehicle tracking process, contacting law enforcement, and after the vehicle has been identified and surrounded, triggering the vehicle's shutdown as soon as law enforcement personnel in the field give the order to do so. No disablement is made directly by Swain Oil.

Besides the described capabilities, the system also offers geofencing (which is available with a remote truck shutdown option; a similar procedure as the one described above for vehicle shutdown would be used if the vehicle equipped with the device passes through a virtual boundary), as well as serving as the driver's timecard to track work hours. Swain Oil uses the latter feature of the system for improved fleet management. However, the company decided not to implement the geofencing capabilities since they did not want involuntary shutdowns in case a truck had to divert from its prespecified route due to an incident or road construction.

4.3.2 VIT System Costs and Benefits

Similarly to the two previous cases, the training costs attributed to the system are negligible, and maintenance and operating costs are minimal. Those costs, as well as perceived and real benefits are described below.

Maintenance

The system is very reliable and requires minimal maintenance, if any. Once the unit is installed and operational, its performance is monitored by the vendor on a daily/weekly basis to ensure it is connected to the network and is fully operational. If any anomalies occur, the S3 staff can perform over-the-air diagnostics to determine what the problem may be.

Operating Costs

The VIT system operating costs are minimal. The additional labor required by the system amounts to a few minutes per month per truck. The system, however, has a monthly fee that, in the case of S3, is in the range of $25 to $45 per month, per vehicle. The system also requires some upfront expenditure to buy and install the eVID units (about $445/unit for a generic S3 customer).

Benefits

Tangible benefits for Swain Oil Transport that are derived from its VIT system include a reduction in insurance premiums (Swain Oil, being a small company cannot self-insure as in the other two cases) and an improvement in productivity by using the system to aid in the tasks of accounting and personnel management. Increased driver safety and equipment/cargo security are also benefits derived from the VIT system.

4.4 INSURANCE BROKERAGE COMPANY: FIRST HORIZON INSURANCE, INC.

First Horizon Insurance, Inc., a subsidiary of First Horizon National Corp., is among the 50 largest commercial insurance brokerages in the United States with over $350 million in premiums. The company provides risk management services, insurance, bonds and employee benefits to commercial clients, including the transportation industry, in 40 states.

The information below was provided Mr. Ed Bass from First Horizon Insurance, Inc.

4.4.1 Insurance Considerations Regarding VIT Systems

Insurance for the commercial sector is different from that of individual households, and in that sense, it is not appropriate to talk about "discounts" (such as those obtained by a household with an honor student, for example) when discussing the benefits of VIT deployments by a trucking company. Instead, underwriters from insurance companies look at how a trucking company is being managed and how the drivers are hired, trained, and managed. The commercial risk management side of insurance companies is a very involved process by which the underwriters analyze the financial situation of the trucking company, its previous five-year loss history (i.e., actuarial assessments of the company’s crash trends in relationship with frequency and severity of crashes), and the safety management culture of the company.

The latter information is essential for the insurance carriers, and the analysis focuses on determining the company’s safety management procedures, its driver hiring practices, how the company trains these drivers, the type of driver management and control, how they communicate with their drivers, the type of disciplinary procedures that are in place, and the type of safety bonuses/incentives that are provided to the drivers, among other safety-related factors. The mechanics of the process involve the trucking company filling out a three-to-five page insurance application, which is followed by a site visit by the insurance company's safety engineers to determine how safety is being considered by the carrier. Adoption of technologies that can help positively affect a company’s safety and security practices is crucial. VITs provide a proactive technology for protecting and managing drivers, while also being very important for truck and cargo security.

VITs have characteristics that are appealing to the insurance companies. Those include: (1) provision of cargo security that would keep the truck from being stolen without driver intervention (e.g., it is possible to leave the truck unattended at a truck stop), (2) protection of the driver, and (3) enhanced driver management tools. The adoption of VITs by a trucking company provides inferences to insurers on where that company is with regard to their commitment to safety management and the culture of the organization (i.e., it shows a strong commitment towards safety since a deployment of a VIT system involves initial investments by the carrier).

All the different aspects involved in the safety management procedures of a given company are important per se, but they also interplay. For example, a trucking company may have a very good driver hiring and managing processes, but if something goes wrong while that driver is on the road (e.g., he/she is driving erratically), a deployed VIT system can allow the trucking company to take some action (e.g., stop the vehicle) that could not be possible if the system were not in place. In the pre-VIT era, there was only information about location of the vehicle, but it was not possible to take any action (other than contacting law enforcement) if a vehicle strayed off course. For example, VIT allows companies to act proactively when dealing with driver-related issues that if left unchecked could result in a serious crash, or if the results of a drug test indicate that a driver has tested positive, the company can immediately initiate an action plan to safely impede him/her from continuing to drive their vehicles. Also, the carrier can now be proactive when receiving and dealing with qualified 'How's my driving' complaints. VITs are also important for the cargo side as well. Many carriers are required to have team drivers because the load cannot be left unattended; however, with a VIT system, the situation can be managed with just one driver, saving the company a great deal of money.

All of this has a value in reducing risks and, therefore, are pondered by insurers at the time of assessing a trucking company. In other words, if the trucking company has appropriate VITs, then the underwriter can take an aggressive approach rather than a conservative one in estimating the risks of that company. A carrier that has very little safety management processes underway will be underwritten very differently from one with a more comprehensive safety culture and that has specific technologies in place (not only VITs but other technologies such as warning devices for lane changes).

Regarding the specific type of VIT, insurance carriers prefer a controlled vehicle shutdown process because it minimizes the likelihood of potential liabilities. Technologies that slow down the truck in a controlled process while permitting the driver to control the vehicle are the ones that are valued the most by the insurance companies. However, the underwriters also analyze how the trucking company uses the technology, how the vehicle deceleration process is designed, and the policies that are implemented around the technology.

In summary, trucking companies that deploy VITs with the characteristics described above show a strong commitment to safety practices, which is decisively taken into consideration by insurance underwriters when assessing the risks of those carriers.

5. VIT BEST PRACTICES

The previous two chapters focused on the description of the current status and characteristics of VITs in North America. The experience and information collected from the direct interactions with different stakeholders (i.e., vendors, users, and law enforcement) permitted a preliminary compilation of best practices, both from a technological and a deployment point of view.

A VIT "best practice" is defined here as any procedure, approach, method or technique, technology application, or other type of activity that improves the overall performance of a vehicle immobilization system. As defined in Section 2, a VIT system involves a number of technologies, companies, and agencies. Therefore, the best practices described below have three main purposes: (1) to assess the current state of the practice of VITs for feedback to the industry, (2) to provide input to hazmat and other carriers regarding the functionality and characteristics of VITs in order to support better decision making regarding the utilization of VITs in the industry, and (3) to provide input to government decision makers regarding the functionalities that can be expected from VITs in order to assess their value in providing security and safety.

5.1 STAKEHOLDERS WORKSHOP, WEBINARS, AND DISCUSSIONS

The direct interactions described in Sections 2, 3, and 4, although comprehensive, by their very nature only covered a limited number of stakeholders. In order to reach a larger audience to discuss the preliminarily compiled “best practices,” as well as to identify other VIT issues, a Stakeholder Workshop was organized and conducted in conjunction with the Commercial Vehicle Safety Alliance (CVSA) Annual Conference and FMCSA MCSAP Leadership Conference that was held in Atlanta, GA, on March 24-30, 2007. Many stakeholders with potential interests in the deployment of VITs (i.e., law-enforcement and hazmat carriers, among others) attended the Stakeholder Workshop, which was organized in conjunction with the CVSA Transportation Security and Hazardous Materials Committees. The Stakeholder Workshop was followed by a series of webinars that focused on industry and law enforcement stakeholders (see Appendix E for a complete list of all the stakeholders with which the research team interacted for this project). The discussions resulted in a list of VIT best practices that is presented in the next section.

5.2 IDENTIFIED BEST PRACTICES

The approach taken in the determination of VIT “best practices” was descriptive rather than prescriptive. That is, the interactions with the different stakeholders permitted the identification of the types of VITs, procedures, and methodologies that are “best” at the current time—as assessed by these stakeholders and the research team—compared to all of the surveyed technologies. For example, there are VIT vendors that currently have the capability to switch between different type of communication systems (e.g., satellite and cellular), while others offer just one or the other. The ability to dynamically switch between communication networks, which enhances the reliability of the entire VIT system, was identified as a “best practice,” as compared to having to select that communication system up front.

In some cases, however, the stakeholders provided suggestions on how these technologies should operate or be deployed, such as, for example, VITs that can be easily integrated with existing systems or technologies that allow for the rapid identification of the distressed vehicle in the stream of traffic. These suggestions are also included below.

Due to the diversity in the organizations that provided input to this project, the interactions with the stakeholders focused mainly on the identification of VIT "best practices" and only secondarily on their prioritization. Because of the different concerns of the participating stakeholders, it would have been very difficult to arrive at an absolute group consensus on how these identified "best practices" should be prioritized. The lists presented below, for both technology- and law enforcement-related "best practices," are organized based on the chronology of events that occur in the usage of VITs. Following this, Subsection 5.5 presents a prioritization of these different "best practices" according to their impacts on four main criteria: security, safety, reliability, and deployability.

5.3 VIT TECHNOLOGY-RELATED BEST PRACTICES

The following identified VIT best practices focus primarily on the different technological aspects of the system.

5.3.1 VITs that Can Be Easily Integrated with Existing Systems

The proliferation of technologies that can improve the operations of trucking companies, while being a welcome development by the industry, also brings concerns about how these different technologies can be integrated such that there are no redundant subsystems. An example of this is the need for multiple communication antennas. A VIT that can be easily incorporated into existing systems (new or legacy systems) without unnecessary duplication of components would expedite its adoption.

At the present, some vendors are seamlessly incorporating VITs into their already existing communications/AVL systems; this integration is even tighter for OEMs who choose to provide VIT capabilities with the vehicles they manufacture.

5.3.2 Enhanced Security, Reliability, and Safety

The VIT system should have a high level of security built in to prevent spoofing and other forms of attack, as well as the necessary precautions to avoid circumventing or tampering with the system. The security of the system should address attempts to meddle with the system originating outside and inside of the system.

The system should also be robust enough to minimize the number of false alarms, inadvertent disablements, and, particularly, inadvertent shutdowns. The safety of the driver is also critical, and the system should provide all the necessary measures so it is as safe as possible, particularly in hijack cases.

All the technologies surveyed in this project had as main objectives the security of the system and the safety of the driver. For enhanced security, many vendors offered tampering protection of their systems, as well as self-diagnosis to detect any potential problems. Some vendors also require background checks on their installers, thus reducing the chances of their technology being defeated. Regarding reliability, no case of inadvertent disablements or shutdowns were reported by any of the vendors surveyed (the few cases of vehicle disablement shutdowns were triggered by a dispatcher or a call center).

5.3.3 Robust Driver Authentication System

The first line of defense in any VIT deployment is its driver authentication system. If an unauthorized driver cannot drive the vehicle, then the chances of needing a remote vehicle shutdown are greatly reduced. Therefore, a robust driver authentication capability and subsequent, periodic re-authentication should be the first element of a vehicle immobilization system. The system should have the necessary provisions to reduce the possibility of non-authorized persons being able to drive the vehicle, such as, for example, requiring a form of identification that cannot be easily duplicated or unlawfully appropriated. The system should also be able to give indications to the driver that the VIT system is working properly.

Some of the vendors surveyed in this project require not only a form of ID (such as a driver’s license) but also an entering of an authentication code. This combination of IDs results in a reasonably robust driver authentication system.

5.3.4 Driver Authentication Technologies that Can Be Used under Different Operational Environments

There are cases in which the vehicle has to be accessed and driven under conditions that are outside of the day-to-day operations. The VIT system should be flexible enough to accommodate these situations without decreasing the security level. For example, it should be possible for the authorized driver to enter an “under-duress” code to indicate a distress situation or for the dispatcher to supply a one-time access code for vehicle maintenance purposes. In the latter case, a combination with a VIT geofence capability could completely secure the vehicle inside a defined area. (Note: VIT geofencing, although demonstrated in this project by several vendors, is not one of the five FRs identified by FMCSA. For systems providing this capability, it is suggested that the geofence boundaries reside in the onboard computer since, in this case, the eVID can be triggered faster, thus reducing the potential distance that the vehicle can travel inside the protected area.)

5.3.5 Technologies that Arm Themselves with no Human Intervention

The disabling/shutdown system should be armed when the door is opened in order to protect the driver and the vehicle/cargo, particularly in a hijack scenario. Similar to other authentication technologies, this technology requires an action by the driver to disarm the system every time the vehicle is to be driven. However, in a hijack case, the driver does not have to do anything to arm the system, not even enter a distress code (e.g., a distress message can be automatically and silently sent to the control/dispatch center after a certain interval of time has elapsed since the last time a door was opened without a subsequent system disarm action issued).

5.3.6 Redundancy in Communications

One of the key components of any remote VIT is its communications system. A disruption in the communication links between the call center/dispatch center and the equipped vehicle would render any remote control of the eVID impossible, thus precluding a vehicle shutdown. These disruptions, many times, happen because of a lack of cell-tower coverage (for these technologies that use cell phone communications) and because of interference with the infrastructure (e.g., bridges, tunnels, urban canyons) and environment (e.g., tree canopies) for satellite communications. While some VIT vendors offer the choice between one and the other (paging communications is also offered in some cases), there are a few companies that can provide automatic switching between communications systems. This capability of choosing among different communication modes based on availability greatly enhances communication redundancy (although it also increases operation costs).

5.3.7 Capability to Override Loss of Signal Disablement

As indicated in the previous chapter, FR2 is not implemented by any vendor at the present time for moving vehicles (i.e., vehicle shutdown due to loss of signal). However, this feature is implemented for stationary vehicles which, as was demonstrated, may become disabled if there is tampering with the communication system (including GPS). A local override, to allow the lawful driver of the vehicle to re-enable it even under conditions in which the communications is lost, diminishes the consequences (e.g., down-time) of false alarms. This feature, however, has to be implemented in such a way that it is required by the driver to contact the dispatcher (e.g., by calling in) in order to obtain the override code. Otherwise, disgruntled drivers could easily defeat the system.

5.3.8 Backup Power Supply for VIT

The VIT system should have an internal battery so that if the power is lost, the unit can still send and receive messages from the central computer (dispatcher). If, for example, the loss of power is due to tampering, the dispatcher or control center would be notified and would be able to send a message to disable the vehicle.

5.3.9 Control Center Awareness

Unintentional loss of power or inadvertent loss of all communication links should not prevent a call center to be notified of such an occurrence. Some existing systems provide the capability of labeling vehicles by the elapsed time since they have reported their location. This capability can be extended to flag certain types of vehicles that have not reported in a predefined interval of time; those vehicles, in turn, could implement some VIT action if they have not received a handshake from the central system during that interval of time. This, however, would require human confirmation (i.e., checking with driver on the status of the vehicle).

5.3.10 Technologies that Acknowledge Task Accomplishment

It is important that when any action is taken to disable or (especially) shutdown a vehicle, that the onboard device notifies the call center/dispatch center when the immobilization process starts and ends. In general, all the technologies tested in this project provided this capability. However, for its implementation, the vehicle has to have a communication system.

5.3.11 Alarm Queuing Prioritization

Alarms at a call center should be prioritized so that the most urgent alarms (e.g., hazmat, high-value) go to the top of the queue. Prioritization was identified by law enforcement as being critical since they consider that it is not necessary that law enforcement be involved in all cases of vehicle immobilization, particularly those involving non dangerous/low-value goods carried by vehicles with VITs that gradually degrade the vehicle performance to a stop. For the other cases, it is important that the call center personnel have the required training to handle different situations and keep an effective contact list.

5.3.12 Technologies that Degrade the Vehicle Performance Rather than Implementing a Complete Power Cutoff

When a vehicle has to be shutdown, the safety of the drivers traveling alongside that vehicle is very important. Therefore, the VIT should utilize an approach involving vehicle degraded performance while maintaining power so that vehicle can be maneuvered in the stream of traffic. The demonstration tests conducted in this project showed that approaches that completely shut off the engine were still safe to maneuver. However, this was done in a very controlled environment and under a non stressful situation for the driver.

Technologies that provide a degradation of the vehicle performance together with an over-the-air control of the settings to achieve a gradual vehicle shutdown also have the advantage that they could allow for the cancellation of the shutdown process once it was initiated simply by changing system parameters. Some of these technologies can also provide a better estimate of the distance that it would take to stop the vehicle once the process has started (see previous chapter). For example, engine depower technologies that are able to wirelessly change the level of engine degradation (i.e., the deceleration of the vehicle) for the shutdown procedure can better control the vehicle stopping distance by selecting the appropriate engine degradation level (notice that for vehicles equipped with GPS or for technologies that are able to read information from the vehicle's data bus, the speed of the truck around the time of shutdown can be determined, which is the other parameter needed to estimate stopping distance).

5.3.13 Adaptive VITs

Vehicle shutdown may occur anywhere under different traffic conditions and roadway geometric configurations. Particularly regarding the latter, rigid (i.e., non-adaptive) VITs could impair the maneuverability of the vehicle, thus increasing the risk of crashes and, therefore, decreasing the safety of the surrounding traveling vehicles. It is, therefore, important that the vehicle shutdown technologies are responsive to changing road conditions, including downward slopes and roadway curvature. Some of the technologies surveyed in this project achieve this by returning full control of the vehicle in distress to the driver if the technology senses that, for example, the vehicle is traveling in a down grade and return to the shutdown process once the geometry of the road has changed.

5.3.14 Variable Spatial Data Polling Frequency

As described below (see Law Enforcement-Related Best Practices), in general, the shutdown of a vehicle should be done with visual contact from the law enforcement agency with jurisdiction in the area. In some cases, however, this will not be feasible. For instance, it was pointed out that in some remote areas (e.g., Oregon), law enforcement may not be able to have visual contact with a vehicle to be immobilized. That is, it may take as much as 1.5 hours before officers can interact visually with that vehicle. It is therefore important to track the vehicle accurately in order to determine the area in which it is traveling when the shutdown process is initiated. Usually, and because under normal circumstances there is no need to determine the spatial location of a vehicle with a high accuracy, their locations are pinged at a lower frequency than would be necessary in cases involving a vehicle shutdown. A spatial data polling frequency that can be changed depending on the circumstances for a given VIT equipped vehicle would provide a means to make better determinations of when to start the shutdown process, especially if law enforcement is not readily able to be in visual contact with the vehicle.

5.4 LAW ENFORCEMENT-RELATED BEST PRACTICES FOR VITS

The following identified VIT best practices focus primarily on issues concerning the deployment and activation of these technologies.

5.4.1 Law Enforcement Involvement in Remote Vehicle Shutdown Incidents

The general consensus of the stakeholders was that a moving vehicle shutdown should be accomplished with visual contact by law enforcement personnel (although with some caveats), and that the activation of the system should be done through the control center (if one exists) in conjunction with the carrier, as opposed of being accomplished directly by law enforcement.

Safety and security were identified as the critical elements in deciding whether the vehicle shutdown requires the involvement of law enforcement. Public safety is a major concern and is the reason why many police departments no longer chase stolen vehicles. However, law enforcement should be involved if there is a security concern, such as if the vehicle is transporting a high-value or high-risk load or the driver is in a hijack situation. Under other situations and depending on the type of VIT and the reaction sequence of the vehicle after activation, the carrier should be allowed to shutdown the vehicle. Stakeholders also determined that vehicle disablements, in general, do not necessarily warrant the involvement of law enforcement personnel.

Legal concerns were also identified as an area to be taken into account for law enforcement involvement in vehicle shutdown events. In particular, there should be a mechanism that permits determination and verification that a crime has occurred before law enforcement is involved. Some of these events may be civil in nature, not criminal, and do not necessarily require law enforcement participation; except if safety and/or security are at stake. The other legal concern identified, and one that requires further discussion, is how easy would it be to trigger these devices, given that certain legal-based procedures were required to be followed; that is, although the VITs can shutdown a vehicle quickly, they may be delayed because certain legal procedures may need to be followed before the order is issued. This is an area that remains to be researched.

5.4.2 VIT Systems that Permit Identifying Law Enforcement Jurisdictions

For those cases deemed to require the involvement of law enforcement in a vehicle shutdown event, it is necessary that the identification of the corresponding jurisdiction on where that event would be facilitated be done via a national call center with appropriate, up-to-date, nationwide contact information for all law enforcement agencies. Some of the vendors surveyed offer this capability to their customers, either through their own or third-party managed call centers.

5.4.3 Technologies that Permit Easy Identification of Distressed Vehicle

In order for law enforcement to identify a particular vehicle that is to be shutdown, or has been shutdown, a capability to distinguish the vehicle from others in a traffic flow needs to be deployed. However, this capability should be designed in such a way that it does not further endanger the safety of the authorized driver involved, for example, in a hijack situation.

Some of the vendors surveyed in this study flash the trailer and tractor lights when the truck is in distress. In many cases, this is not done if the driver has entered the under-duress code (indicating a hijack situation) so that the driver's life is not further endangered. In these cases, other ways of identifying a distressed vehicle should be used, including an increase in the spatial data polling frequency (see 5.3.14) to enhance the truck location accuracy.

5.4.4 Technologies that Are Easy to Use by Law Enforcement

The VITs should be easy to use by law enforcement, including the determination of the time that it would require to shutdown the vehicle and the likely distance that it would traverse before coming to a stop.

Although, there are VITs that are completely activated and controlled by law enforcement (see Section 2 for two examples), the result of the interactions with different law enforcement stakeholders has determined that law enforcement does not need to activate the devices directly. This simplifies the usage of the technology since the activation is reduced to an order given wirelessly as described in Section 3 of this report. This also eliminates issues related to technology obsolescence and legacy systems for law enforcement agencies since under the model described here, the technology would reside outside of these agencies.

Regarding the time it takes to stop a vehicle from the time the order to shutdown is given and the distance traversed, those parameters can be assessed and predicted by the VIT systems in the same way as was described in Section 3, and passed along to the law enforcement personnel at the scene so informed decisions can be made on when to start the shutdown process.

5.4.5 Technologies that Permit Quick Recovery after Shutdown

A swift recovery from immobilization—that is, the ability to quickly restart the vehicle—is a necessary capability to minimize the effects (e.g., congestion increase or disablement on critical infrastructure) that any vehicle shutdown would cause. In general, the technologies surveyed in this study provide rapid re-enablement of vehicles (see Section 3).

5.5 PRIORITIZATION OF BEST PRACTICES

As explained previously, the diversity in the organizations that participated in this project, while fundamental to obtain the widest spectrum in VIT best practices, was not conducive to their prioritization since it would have been very difficult to arrive at an absolute group consensus. The “best practices” identified in this section, however, were prioritized by the research team following four main criteria: security, safety, reliability, and deployability. The results are presented in Table 11 below (notice that some of the “best practices” are relevant to more than one criteria and, therefore, may appear more than once in the table).

Table 11. Prioritized List of Best Practices by Four Criteria

Criterion and Priority	Best Practice
Security 1	5.3.2 Enhanced Security, Reliability, and Safety
Security 2	5.3.3 Robust Driver Authentication System
Security 3	5.3.5 Technologies that Arm Themselves with no Human Intervention
Security 4	5.4.1 Law Enforcement Involvement in Remote Vehicle Shutdown Incidents
Security 5	5.3.6 Redundancy in Communications
Security 6	5.3.11 Alarm Queuing Prioritization
Security 7	5.4.2 VIT Systems that Permit Identifying Law Enforcement Jurisdictions
Security 8	5.3.9 Control Center Awareness
Security 9	5.3.10 Technologies that Acknowledge Task Accomplishment
Security 10	5.3.4 DATs that Can Be Used under Different Operation Environments
Security 11	5.4.3 Technologies that Permit Easy Identification of Distressed Vehicle
Security 12	5.3.8 Backup Power Supply for VIT
Security 13	5.4.4 Technologies that Are Easy to Use by Law Enforcement
Security 14	5.3.14 Variable Spatial Data Polling Frequency
Safety 1	5.3.2 Enhanced Security, Reliability, and Safety
Safety 2	5.3.13 Adaptive VITs
Safety 3	5.3.6 Redundancy in Communications
Safety 4	5.3.9 Control Center Awareness
Safety 5	5.3.12 Technologies that Degrade the Vehicle Performance
Safety 6	5.4.5 Technologies that Permit Quick Recovery after Shutdown
Safety 7	5.3.5 Technologies that Arm Themselves with no Human Intervention
Safety 8	5.4.1 Law Enforcement Involvement in Remote Vehicle Shutdown Incidents
Safety 9	5.4.2 VIT Systems that Permit Identifying Law Enforcement Jurisdictions
Safety 10	5.3.14 Variable Spatial Data Polling Frequency
Safety 11	5.4.3 Technologies that Permit Easy Identification of Distressed Vehicle
Safety 12	5.4.4 Technologies that Are Easy to Use by Law Enforcement
Reliability 1	5.3.2 Enhanced Security, Reliability, and Safety
Reliability 2	5.3.6 Redundancy in Communications
Reliability 3	5.3.7 Capability to Override Loss of Signal Disablement
Reliability 4	5.3.8 Backup Power Supply for VIT
Reliability 5	5.3.10 Technologies that Acknowledge Task Accomplishment
Deployability 1	5.3.1 VITs that Can Be Easily Integrated with Existing Systems

6. VST CONCEPT OF OPERATIONS FOR LAW ENFORCEMENT

The concept of operations (COO) for stopping moving vehicles using VSTs provides the appropriate protocol to avoid inadvertent activation, a list of steps and procedures to be followed before activation, and a checklist of organizations that should be coordinated with to ensure safe utilization. The target application of the COO is hazmat safety and security in Tennessee. The COO includes the steps and procedures from the identification of the need for stopping a moving vehicle through the shutdown and securing of the vehicle.

6.1 OVERVIEW OF PROCESS

The security of vehicles is accomplished in many ways. This COO focuses ONLY on the potential stopping of a moving vehicle with the assistance of law enforcement. There are several steps in the proposed protocol for a law enforcement-supported remote stopping of a vehicle equipped with a VST:

- Initiation of a VST protocol
- Threat/risk assessment
- Vehicle interdiction

Each of these steps will be discussed in the subsequent sections.

If adopted by TDOS, it would be expected that this protocol would be implemented as a General Order similar to General Order 412 on the use of tire deflation devices. A General Order would establish the policy basis for the use of VSTs.

6.1.1 Initiation of VST Protocol

A law enforcement-assisted VST implementation would only be considered when the requesting party has been determined to meet minimum best practices as defined above. It is also possible for a vehicle owner (VO) or owner representative (OR) to be certified as prescribing to minimum best practices. The OR would typically be a fleet management service that has vehicle tracking and remote stopping capabilities.

The most likely first notice of an incident is from the vehicle owner or owner’s representative. The most likely first point of law enforcement contact would be law enforcement dispatch. Dispatch should acquire the following information from the VO or OR:

- Company name
- DOT number
- Vehicle license plate number
- VIN (optional)
- Driver’s name
- Driver’s license number

- Cargo
- Current or last known position of vehicle

The dispatcher will verify the credentials through the Commercial Vehicle Information Exchange Window (CVIEW) and National Crime Information Center (NCIC). Verification of credentials will provide a presumption of a valid incident and initiation of the remaining steps of the protocol. (Failure to verify credentials requires additional intervention by higher levels of authority.)

6.1.2 Threat Assessment and Risk

The second step is an assessment of the threat and risk. The assessment is primarily of the vehicle and its cargo. The three levels of threat are: low, moderate, and high.

Low

The primary damage potential is that which can be caused by the size and weight of a large vehicle impacting another object. The vehicle is essentially a stolen vehicle and should be handled using normal procedures, that is, which would not require the initiation of the VST protocol.

Under low risk, law enforcement should encourage restraint by the VO or OR to not create a larger risk by potential intervention. The initial response should be to perform a normal traffic stop. If the vehicle complies, the officer should call for activation of VDT as soon as the vehicle is off the roadway. If the vehicle being pursued does not comply, the primary response vehicle will not chase the vehicle.

Moderate

The vehicle contains material that if released following an impact with an object has moderate environmental impact. Such an incident would be a moderate priority and intervention would be considered only when interdiction was likely to be capable of reducing the risk. A moderate level of risk would endorse a more limited use of VSTs; that is, a moderate risk situation could escalate to be more serious if a VST protocol were enacted. A stolen vehicle would be less likely to suggest the need for an immediate VST implementation. A terrorist-related event would suggest a more immediate implementation of VST.

A moderate risk event, such as a stolen gasoline truck, suggests the need for a graduated response, unless it is known that there is a hostage or that it is a terrorist situation. The dispatcher should immediately contact a supervisor to assist in assessing the response options in the event that the incident escalates. The initial response should be to perform a normal traffic stop. If the vehicle complies, the officer should call for activation of VDT as soon as the vehicle is off the roadway, as this technology only activates when the vehicle is stopped.

If the vehicle being pursued does not comply, the probability increases that it is a terrorist-driven action. The supervisor will determine if the incident requires escalation to the VST moving vehicle protocol described below.

High

A potential impact has long-term health and safety impacts that are significantly greater than that caused by a traffic accident. The incident would receive high priority, and interdiction would be actively considered due to the potential to reduce risk.

A high-risk incident exists when the subject vehicle has an extremely dangerous cargo and is believed to be in the control of terrorists. The goal is still to shut the vehicle down at the safest possible location. However, if the vehicle is near a known or suspected target, a more aggressive approach may be undertaken. A supervisor should be involved prior to implementation of a VST unless circumstances are so time-sensitive as to preclude such involvement. Otherwise, the moving vehicle protocol described below should be followed.

6.2 VEHICLE INTERDICTION

The moving vehicle interdiction is the most complex portion of the protocol and dictates that the response always be tempered by the ongoing assessment of the threat and risk. The goal is to implement VST only when it is likely to reduce the risk of an undesirable outcome. Unless the threat is so severe that immediate action is the only logical course of action, the goal is to select a point of interdiction that maximizes the likelihood of a safe and orderly VST activation using this moving vehicle protocol.

6.2.1 Issues

Vehicle interdiction requires that the VST be activated by some form of communication. This communication may or may not be timely or continuous. Communications may be lost in remote areas or tunnels. If a VST is activated and a vehicle is shut down in a tunnel, it may require some form of manual intervention by the VR to move the disabled vehicle.

VSTs will NOT be considered when the VSTs do not allow for maintaining the steering and braking functions, unless the threat is high. Even in a high-threat event, the risk of an out-of-control vehicle should be assessed before implementing a VST that allows for the loss of braking and steering.

The ideal shutdown location is a straight, level road in a rural area. However, an ideal location seldom exists in practice. Therefore, an understanding of how a vehicle shutdown would occur is necessary to make an informed decision on when to implement a VST. Critical issues include:

- How quickly does the VST begin to impact the vehicle?
- How will the vehicle function after a VST has been activated?
- How quickly after activation of the VST does the vehicle come to a stop?

The answers to the above questions indicate the length of roadway potentially impacted by VST activation and the potential need to avoid curves and grades. (Note: For the technologies demonstrated in this project, this information can be found in Section 3 of this report.)

An additional consideration in a hostage scenario is the factor of not alerting the perpetrator to the impending VST activation. The presence of alerting technology (horns, lights, etc.) on particular vehicles should be ascertained by the VO or OR.

6.2.2 Moving Vehicle Protocol

The moving vehicle protocol requires a minimum of two vehicles, with three vehicles being desirable. The roles of these vehicles are more fully discussed below. The following items need to be determined prior to initiation:

- Expected time and length of roadway to implement VST
- Roadway, traffic, and weather conditions along the roadway
- Locations to avoid VST activation (hills, curves, tunnels)
- Communications dead spots

The law enforcement role is to aid in maintaining the health, safety, and welfare of the general public. Law enforcement's role is continually being shaped by risk assessment. The following steps should only be undertaken when the roadway ahead is safe to engage in a traffic stop and the deployment of a VST, or the threat is so great that immediate action is likely to be less severe than waiting.

Initiation

The activation of VST requires consideration of a number of important issues. The checklist shown in

Table 12 has been put together to guide the dispatcher in considering a number of factors associated with initiation of VST. Therefore, a critical requirement in moving forward with assisting in a VST event is a determination by the dispatcher that the checklist criteria in Table 12 have been met. The only immediate VST implementation would be when a higher authority has determined that failure to immediately implement VST is a greater threat than the worst case outcome of an immediate VST event.

A critical aspect of activation of a VST is the necessity of having the moving vehicle in sight of the primary law enforcement vehicle. This is necessary to ensure that all requirements of the shutdown protocol listed above are in fact being met, including acceptable traffic and roadway conditions.

Initiation should not begin unless there are two, and preferably three, law enforcement vehicles in close proximity to the shutdown.

The primary (first) unit is responsible for continual visual contact with the vehicle and communication with the dispatcher concerning activation of the VST.

The responsibility of the backup (second) unit is to provide traffic control. It is also the first unit to respond to a traffic accident. If requested by the primary unit, it could replace the primary unit.

The responsibility of the support (third) unit is to assist with arrests or to replace the backup unit in case of a traffic accident. This unit can replace the primary or backup unit should one of those units not be able to continue.

When the primary unit makes an assessment that roadway and traffic conditions are favorable for activating the VST, he/she notifies the dispatcher. The dispatcher is responsible for ensuring that all checklist items in Table 12 have been addressed. The dispatcher then notifies the VO or OR of the location, conditions, and presence of law enforcement. The VO/OR makes the determination that all technical requirements are met and that the VO/OR wants to activate the VST. The VO/OR then initiates the VST activation and notifies law enforcement dispatch.

Post-Initiation

Law enforcement has two principal roles following activation of a VST: maintaining traffic safety and apprehending the stopped vehicle’s driver. Following completion of the VST event, a debriefing should be undertaken to determine any lessons learned from the VST event.

Table 12. VST Activation Checklist

Check Here	Issue	Result/Action
	Company Name	
	DOT Number	
	Vehicle License Plate Number	
	VIN (optional)	
	Driver’s Name	
	Driver’s License Number	
	Cargo	
	Current/Last Known Position	
	Credentials Validated	(Yes/No) If no, refer to supervisor.
	Risk Assessment	If low; no action. If medium; proceed if the threat is higher than the risk. If high; proceed with VST activation.
	Does VST disable brakes and steering?	If yes, proceed only if high-level risk.
	How quickly (minutes) before the effect of VST activation is realized?	
	How long (minutes) does VST activation take to stop the vehicle?	
	Speed of Vehicle (mph)	
	What is the expected distance (miles) traveled by the vehicle with an activated VST? Multiply total minutes times speed and divide by 60 (e.g., 2 minutes to implement plus 2 minutes to shut down is 4 minutes times 60 mph divided by 60 is four miles to shut down).	
	Is the road ahead safe enough to begin VST activation? Consider roadway, traffic, and weather conditions along the roadway. Locations to avoid: (hills, curves, tunnels, bridges and known communications dead spots).	
	Check criteria met	
	Advise VO or OR that VST can be activated.	
	Notify field units when VO or OR initiates VST activation.	

7. CONCLUSIONS

Building on previous FMCSA studies, field operational tests, and evaluations of security technologies for the motor carrier industry, this VIT Evaluation Project focused on demonstration testing and assessment of VITs for eventual application to Hazardous Materials and other transportation applications. Within that framework, the main goal of this high-level study was to determine how these technologies are being deployed and used by the motor carrier industry. The results showed that the industry, as a whole, favors an approach that focuses on theft prevention before a vehicle is underway (i.e., technologies that ensure verification of authorized personnel as well as prevent hijack situations) and that vehicle shutdown technologies are viewed as a last resort. This is not a surprise since the Major Theft Unit at the FBI's Criminal Investigative Division identifies cargo theft as their number-one priority (FBI, 2006).

Specifically, the study conducted under this project determined that VITs are being developed in various VDT and VST forms, and have been implemented primarily as a security technology by early adopters, especially those involved with high-value cargo. In the last several years, VIT deployment has moved from the theoretical domain to reality, and its adoption continues to be on the rise.

From a technological stand point, this study found that there are several approaches being currently used for driver authentication which, as pointed out above, is identified by the industry as one of the first and most important lines of defense to improve security. Currently available driver authentication technologies for CVO include swipe cards, proximity cards, and keypads; no biometrics technology is being used by the VIT vendors identified in this study. Keypads or combinations of swipe/proximity cards with keypads are the most secure driver authentication technology types.

VSTs can be divided into two main types: (1) complete engine shutdown technologies and (2) engine performance degradation technologies. Engine performance degradation technologies are safer because the vehicle never loses power during the process and can be controlled by the driver at all times. Some of these technologies use a multiple step approach that implements decreasing speed thresholds triggered at constant intervals during the vehicle shutdown process, with a longer interval once the vehicle has reached a very low speed (usually 10 mph). Other engine degradation technologies use just a single or a two-step process by which the vehicle is rapidly decelerated while maintaining all the mechanical functions available to the driver.

The demonstration tests conducted in this project allowed for the measurement of some parameters associated with VSTs, which play an important role in the potential use of these technologies by law enforcement. The tests showed that, on the average, it took 30 and 64 seconds for engine shutdown and engine performance degradation technologies, respectively, using cellular communications to shutdown the vehicle. For acceleration control technologies, this number depends on the parameters entered in the system to define the speed decrement intervals. In general, several speed decrement intervals are implemented, each with lengths of about one minute (although these are user defined), and, therefore, the longer latency in satellite communications, as compared to that of wireless cellular communications, does not have a significant impact in the length of the entire shutdown process. Regarding remote vehicle re-enable, it took 52 seconds on the average when cellular communications was used and slightly longer, 80 seconds, when it was performed using satellite communications.

Another important parameter for the law-enforcement COO is the distance that the vehicle would travel during the shutdown process. Stopping distances depend on many factors, including the type of VST, the vehicle speed at the moment the eVID is activated, the topography and geometric characteristics of the roadway, and the behavior of the driver (e.g., whether the driver maintains the maximum possible speed or not). Because of the dependency of these factors on the particular situation in which a vehicle is to be shutdown, it is not possible to generalize regarding these parameters. Nevertheless, some VSTs, specifically those that allow changing parameters wirelessly, offer better control over the maximum expected distance that a vehicle would travel after shutdown.

The research also showed that at the present time, it is possible to achieve four out of the five FRs identified by FMCSA. Functional Requirements 1 (vehicle disablement if the vehicle senses an unauthorized driver), 3 (remote vehicle disablement/shutdown by the driver), and 4 (remote vehicle shutdown by the dispatcher) were fully demonstrated in this project. Loss of signal disablement (FR2) is only being implemented for VDTs (e.g., wire cutting), but not for VSTs. The latter, although technically feasible, may cause undesired vehicle shutdowns and, therefore, is not implemented by the vendors or the users of the technology. Regarding FR5, at the present time, law enforcement cannot independently trigger a remote vehicle shutdown and has to accomplish shutdown through the carrier or the VIT vendor. The lack of this capability was viewed as an advantage since there was a strong consensus among stakeholders that FR5 should always work in conjunction with FR4 (remote vehicle disabling by the dispatcher). That is, discussions with law enforcement personnel have indicated that it would be very difficult and impractical for law enforcement to remotely shutdown a vehicle without coordination with the dispatcher or some other party in possession of all the necessary information and control capabilities to trigger such an event.

Regarding VIT's fixed and periodic costs, the research demonstrated that there is a wide variation of VIT capabilities and, in consequence, prices among the vendors. The price of the unit varies between $100 and $1,700, with an average of $535. The monthly fees are in the $25-to-$85 range, with an average of $45. Identified benefits by companies using VITs include risk exposure reduction, theft avoidance, insurance premium reduction, and increased driver and cargo safety. Other spillover benefits resulting from the deployment of a VIT system include better fleet management by using its driver and vehicle tracking capabilities.

VIT "best practices" and issues were identified in this project and further discussed in different forums (e.g., the 2007 Commercial Vehicle Safety Alliance Conference, several industry and law enforcement-focused webinars, and discussions with both large and small trucking companies) in an attempt to capture the perspectives of the main VIT stakeholders. Among those VIT "best practices," it was determined that law enforcement should be involved in vehicle shutdown events in which a crime has been committed. Furthermore, the technology should be easy to use by law enforcement and allow for easy identification of the vehicle under distress in the stream of traffic. Other "best practices" included robust driver authentication systems, adaptive VITs, technologies that degrade the vehicle performance, technologies that permit quick recovery after shutdown, technologies that arm themselves with no human intervention, alarm queuing prioritization at the control center, and redundancy in communications, among others. The "best practices" also played a critical role in the development of the concept of operation for law enforcement application of VITs, which is included in this report.

While VITs can greatly increase the security of any trucking operations and would certainly decrease the number of cargo thefts, the technology is not infallible. The communication component of VIT systems is its weakest link. As pointed out before, one of the findings of this project is that vehicle shutdown due to loss of signal cannot be implemented because it would create too many undesired shutdown events. Therefore, anyone with knowledge of the system can cut the communication link (with the vehicle moving) and continue driving the truck. There are, however, anti-hijack technologies that trigger the eVID locally if someone opens the door to the cab and the device is not deactivated. If the driver is abducted and kept in the cab, this could also be defeated by forcing the driver to re-enable the truck.

The fact that the study shows that the technology is not infallible has repercussions on findings of past studies, specifically the "Hazardous Materials Safety and Security Technology Field Operational Test" (FMCSA, 2004b; 2004c). Although the costs of deploying VIT systems were found to be in range with those of that study, the security benefits that this technology may provide would probably need to be revised. That is, in calculating the benefits that can be accrued from the deployment of the technology, it was (correctly) assumed in the 2004 FOT that partial deployments might not necessarily result in a directly proportional security benefit (e.g., x percent deployment may not yield x percent of achievable security benefits). The conclusion then was that it was necessary to have a full deployment of the technologies. The study shows that, with the current state of the art in terms of VIT systems, even in a full deployment case, there is no warranty that 100% of the security benefits that this technology can provide would be achievable.

Future research, therefore, should focus on how to make these VIT systems more robust if they are to be used to enhance national security. In the meantime, and to both assist law enforcement in the application of the COO and to minimize the impacts that vehicle shutdowns could cause in the stream of traffic, it is important that stopping distances for different VSTs be further studied.

8. REFERENCES

Authentify. 2007. Authentify Voice Biometric Applications. Available at: http://www.authentify.com/solutions/voice_biometrics.html.

AutoCab. n.d. In the Cab: Driver Flexibility. Available at: http://www.autocab.com/en-au/system/cab/flexibility.shtml.

Automotive Wireless. 2007. Automotive Wireless Web Homepage. Available at: http://www.automotivewireless.com. Accessed July 24, 2007.

BiometricWatch. n.d. News Weekly Web Homepage. Available at: www.biometricwatch.com/Technologies/Iris_recognition/iris.htm

Blackburn, Duane, M., and U.S. Federal Bureau of Investigation. 2004. Biometrics 101, Version 3.1.

Bromba, Manfred. 2007. Bioidentification: Frequently Asked Questions. Available at: http://www.bromba.com/faq/biofaqe.htm#Vorteile.

BSM Wireless. 2007. BSM Wireless Web Homepage. Available at: http://www.bsmwireless.com. Accessed July 24, 2007.

Bundesamt fur Sicherheit in der Informationstechnik (BSI). 2004. Study: Evaluation of Fingerprint Recognition Technologies-BioFinger. Available at: http://www.bsi.bund.de/english/publications/studies/BioFinger.pdf.

Das, Ravi. n.d. Business and Technical Factors to Be Taken into Consideration before Implementing a Biometric System at Your Place of Business. Available at: http://www.findbiometrics.com/Pages/feature%20articles/business-technical-factors.html

Eureka Aerospace. 2007. HPEMS Technology: Technology Description. Available at: http://www.eurekaaerospace.com/hpems.php. Accessed July 24, 2007.

Federal Bureau of Investigation (FBI). 2006. Cargo Thefts High Cost. Available at: http://www.fbi.gov/page2/july06/cargo_theft072106.htm. Accessed July 24, 2007.

Federal Highway Administration (FHWA). 1996. Smart Cards in Commercial Vehicle Operations (December). FHWA/MC-97/022 Final Report.

Federal Motor Carrier Safety Administration (FMCSA), U.S. Department of Transportation. 2004a. *Hazmat Safety and Security Field Operational Test, Final Report* (August). Available at: www.fmcsa.dot.gov/documents/hazmat/fot/HMFOT-Final-Report.pdf. Accessed July 24, 2007.

———. 2004b. *Hazardous Materials Safety and Security Technology Field Operational Test, Volume I: Evaluation Final Report Executive Summary* (November). Available at: www.fmcsa.dot.gov/documents/hazmat/fot/FINAL-Volume-I-Executive-Summary-11-10-04.pdf. Accessed July 24, 2007.

———. 2004c. *Hazardous Materials Safety and Security Technology Field Operational Test, Volume II: Evaluation Final Report Synthesis* (November). Available at: www.fmcsa.dot.gov/documents/hazmat/fot/FINAL-Volume-II-HAZMAT-Synthesis-11-12-04.pdf. Accessed July 24, 2007.

———. 2006. *Expanded Satellite Tracking* (March. Available at: www.fmcsa.dot.gov/facts-research/research-technology/report/Mobile-Communications/mobile-communications-tracking-system-requirements.pdf. Accessed July 24, 2007.

———. 2005. *Untethered Trailer Tracking and Control System* (December). Available at: www.fmcsa.dot.gov/facts-research/research-technology/report/untethered-dec05/untethered-dec05.pdf. Accessed July 24, 2007.

Findbiometrics. n.d. Understanding Voice Recognition. Available at: http://findbiometrics.com/Pages/voice%20articles/voice_1.html

Gaits. 2007. Face Recognition. Available at: www.gaits.com/biometrics_face.asp

Gifford, J. L; Marwah, S., and Morstein, J. H. 1996. Smart Cards in Commercial Vehicle Operations: Prototype Applications and Institutional Issues. Presented at the 1996 ITS America Meeting, Houston, Texas.

GlenHugh Enterprise. 2007. Vehicle Security. Available at: http://www.autowatchamerica.com/invehi.asp. Accessed July 24, 2007.

Global Security. 2007. Homeland Security: Biometrics. Available at: http://www.globalsecurity.org/security/systems/biometrics.htm

Global Security. n.d. Available at: http://www.globalsecurity.org/security/systems/hand.htm

Haase, Michelle Speir. 2005. Face-off: Face recognition is emerging as a viable tool for verifying identities. Available at: http://www.fcw.com/article88535-04-11-05-Print

Human Recognition Systems. n.d. Available at: http://www.hrsltd.com/products/hand_geometry/handkey_id3d.htm

Information Technology Standards Committee. 2004. Available at: http://www.itsc.org.sg/synthesis/2004/2_Voice.pdf

International Biometric Group. 2006. Which is the Best Biometric Technology? Available at: www.biometricgroup.com.

International Biometric Industry Association. n.d. Smart Cards. http://www.ibia.org/biometrics/technologies_view.asp?id=14

International Truck and Engine/NAVISTAR. n.d. AWARE Vehicle Intelligence. Available at: http://www.internationaldelivers.com/site_layout/aware/section.aspx?code=avi. Accessed July 24, 2007.

Iridian Technologies. 2003. Proof Positive Technologies. Available at: www.iridiantech.com/products.php?page=5.

Kalyanaraman, Sriram. 2006. Biometric Authentication Systems: A Report. Madras: India Institute of Technology.

Knight, Will. 2005. Finger-vein reader to foil car thieves. Available at: http://www.newscientist.com/article.ns?id=dn8249&feedId=online-news_rss091.

L-l Identity Solutions. n.d. L-1 Identity Solutions Web Homepage. Available at: www.identix.com/trends/face.html

Lawrence Livermore National Laboratory.2004. Science and Technology Review. Available at: http://www.llnl.gov/str/JulAug07/PatJulAug07.html; Bill Wattenburg's Truck-Stopping Device for Hijacked Trucks. Available at: http://www.pushback.com/terror/TSD/index.html. Accessed July 24, 2007.

LG Electronics. n.d. LG IrisAccess. Available at: http://www.lgiris.com/iris/compares.html.

Lumidigim. 2004. The Science behind Lumiguard. Available at: http://www.lumidigm.com/.

MAGTEC. 2005. M5K in Action: MAGTEC Introduces Unparalleled Breakthrough in Driver/Truck Management. Available at: http://www.magtecproducts.com/mk5-in-action.asp. Accessed July 24, 2007.

MAGTEC. n.d. M5K. Available at: http://www.magtecproducts.com/mk5.asp.

National Center for State Courts. n.d. Available at: http://ctl.ncsc.dni.us/biomet%20web/BMHand.html

National Institute for Standards and Technology (NIST). 2006. Face Recognition Vendor Test. Available at: www.frvt.org

Qualcomm. 2007. Vehicle Command and Control. Available at: http://www.qualcomm.com/technology/assetmanagement/services/vcc.html. Accessed July 24, 2007.

Rosenzweig, Paul, Kochems, Alane, and Schwartz, Ari. 2004. Biometric Technologies: Security, Legal, and Policy Implications. Available at: http://www.heritage.org/Research/HomelandDefense/lm12.cfm

Ross, Arun, and Jain, Anil. n.d. Hand Geometry. Available at: http://biometrics.cse.msu.edu/hand_geometry.html

Safefreight Technology. 2007. Security and Fleet Management. Available at: http://www.safefreight.com. Accessed July 24, 2007.

Smart Card Alliance. 2002. Smart Cards and Biometrics Report. Available at: http://www.smartcardalliance.org/pages/publications-smart-card-biometric-report

Spectrotec. 2005. Biometric Fingerprint Immobilizer. Available at: http://www.spetrotec.com.

Trackn/Aircept. n.d. About eTrailerTrack. Available at: http://www.etrailertrack.com/etrailertrack/about.asp. Accessed July 24, 2007.

Turk, M., and Pentland, A. 1991. Face recognition using eigenfaces. Proc. IEEE Conference on Computer Vision and Pattern Recognition.

U.S. Department of Transportation (DOT). 2000. Electronic Intermodal Supply Chain Manifest ITS Field Operational Test Evaluation Plan (September). Available at: www.itsdocs.fhwa.dot.gov/JPODOCS/REPTS_TE/13474.pdf. Accessed July 24, 2007.

U.S. House of Representatives. 2004. *Making Appropriations for Foreign Operations, Export Financing, and Related Programs for the Fiscal Year Ending September 30, 2005, and for Other Purposes.* 108th Cong., 2d sess. H. Rept. 108–792. Available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_reports&docid=f:hr792.108.pdf. Accessed July 24, 2007.

Watanabe, Masaki, Endoh, Toshio, Shiohara, Morito, Sasaki, Shigeru, and Fujitsu Laboratories Ltd. 2005. Palm vein authentication technology and its applications. Available at: www.fujitsu.com.

Wireless Matrix. 2006. Fleet Outlook: Increase Productivity and Reduce Costs. Available at: http://www.wirelessmatrixcorp.com/products/fleetoutlook.html. Accessed July 24, 2007.

APPENDIX A:
DRIVER AUTHENTICATION TECHNOLOGIES

A.1 INTRODUCTION

This appendix summarizes the results from a technology scanning study of Driver Authentication Technologies (DAT), which was undertaken as part of this FMCSA's VIT Project. The study presented here pays particular attention to devices that fall in the realm of log-in devices and biometrics. The basic science behind biometric technologies is also presented. Application of many of these technologies to commercial vehicle operations (CVO) and carrier safety and security is a growing area, but still very limited. Because of this limitation, the spectrum of devices considered in this scanning study includes those devices that may not currently be implemented in the industry, but show considerable promise for being deployed.

The study presented in this appendix will first discuss log-in devices, particularly those with global log-in (GL) capabilities, and their relationship, or potential relationship, to CVO. The science of biometrics will be discussed and various biometric technologies will be introduced. Benefits and concerns for each of these technologies will be presented. Best practices for the integration of these devices into CVO will be recommended as well. The report will conclude with a discussion on the potential use of smart cards in CVO; a combination of log-in and biometric devices.

A.2 BACKGROUND

Driver Authentication Technologies, which are a subgroup of Vehicle Disabling Technologies (VDTs), require users to prove their identity before operating a vehicle (see Figure 42 and Section 2 for further definitions and a taxonomy of Vehicle Immobilization Technologies, VITs). This can be accomplished in several ways: through a password, token (e.g., a swipe card), a biometric device, or a combination of the two. In any case, unless the driver is authenticated, the vehicle will remain disabled and will not start. Vehicle Shutdown Technologies (VSTs), on the other hand, are typically electronic technologies capable of stopping a moving vehicle or disabling a stopped vehicle. Immobilization can be achieved by any number of methods, including impeding fuel to the engine or using the onboard computer to limit the vehicle's speed. DATs and VSTs are related technologies. VSTs tend to be a last line of defense in vehicle security, while DATs are viewed as one of the first technological interventions. With proper installation and implementation of a DAT, a VST system may never have to be used. Since usage of VSTs have the potential to be dangerous, may be complex to implement, and may cause collateral damage in a high-risk/high-consequences event, they should be used only in a last resort situation. DATs, on the other hand, are relatively easy to implement, are cost-effective, and tend to be relatively safe to use. Preventing a potential hijacker or thief from ever starting a vehicle significantly improves overall safety and security.

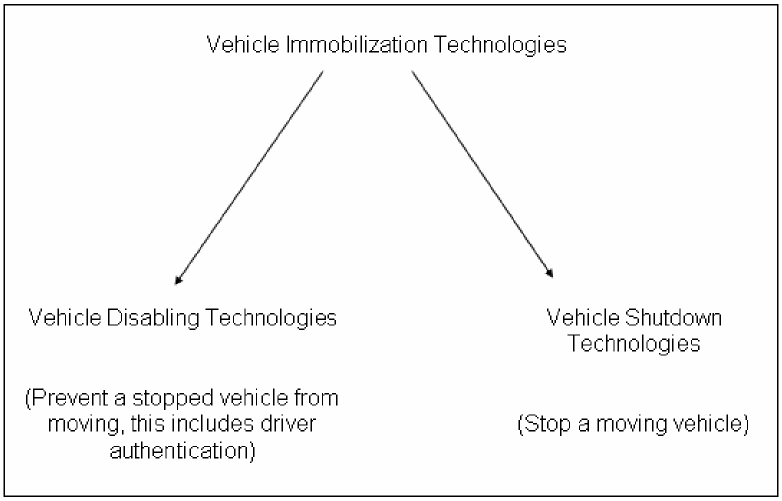

Vehicle Immobilization Technologies
Vehicle Disabling Technologies
(Prevent a stopped vehicle from moving, this includes driver authentication)
Vehicle Shutdown Technologies
(Stop a moving vehicle)

Figure 42. VIT Definitions

A.2.1 Driver Authentication Technology Attributes

Some of the technologies discussed in this appendix have not yet been implemented in CVO, mostly due to their unsuitability for that environment. To bridge the shortcomings of these technologies for their potential future use in this industry, they should be designed according to the following paradigm.

Ability to Verify or Identify a Driver

When dealing with authentication, it is important to recognize the difference between the two modes of authentication: verification and identification. In a verification situation, a user makes a claim as to his/her identity and the system determines if the claim is correct. When using a DAT, a user enters his/her identity into a system using a scan card or keypad, and then the system verifies that this claim is correct. The user’s ID signature is only compared to one reference; the claim must be the same as the reference in order to gain access. A visual example is provided in Figure 43.

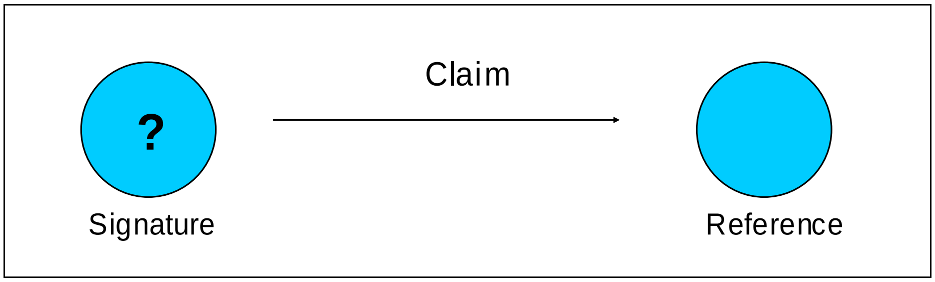


Figure 43. Visual Representation of Verification

In this example; consider the blue circle on the left as a user’s ID signature, the circle is compared only to one reference image (blue circle on the right). If the reference image were not a blue circle, verification would not be made. Since the reference is also a blue circle, in this case the system would make verification. A log-in device is an example of a verification system. A good way to think about how verification works is to pose the question, “Am I who I claim to be?” This is the fundamental idea behind verification.

In an identification situation, a user’s input is compared to all other users’ unique inputs in the system, information that, in general, is contained in a database. The system views the user and identifies his ID signature in the system’s database. A visual example is provided in Figure 44. In this example, the blue circle is again a user’s ID signature. This time it is compared to all other users’ ID signatures in the database. Since the database contains a blue circle, identification would be made. A good way to think about how identification works is to pose the question, “Who am I?” This is the fundamental idea behind identification (Bromba, 2007).

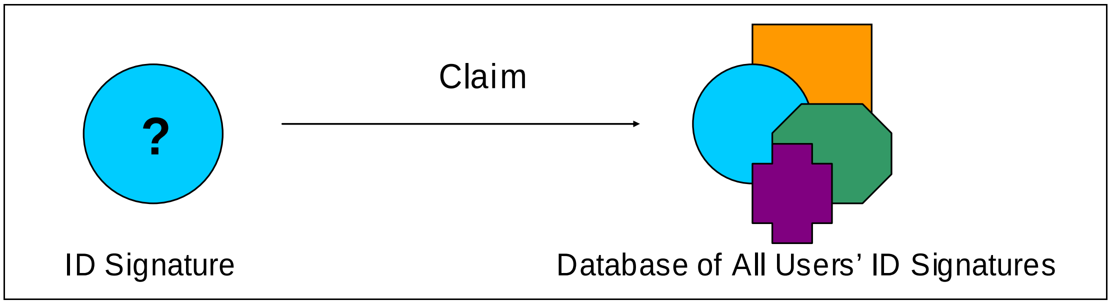


Figure 44. Visual Representation of Identification

Verification is a faster method, while identification is more secure. Both have their benefits in DAT. High-security operations may need to use a combination of identification and verification. For small groups of people, identification may not be very time consuming. For a large group of users, where a database may be large, identification may take a large amount of time. DATs in this report should be capable of either verification or identification or use both. Some of the DAT technologies demonstrated in this project (see Section 3) offered both verification and identification procedures. For example, BSM Wireless uses a proximity card as identification (i.e., the person in possession of that card shows that he/she is a valid driver for the particular vehicle) and a keypad for verification purposes (i.e., once the driver has been identified as a valid driver for the vehicle, he/she gets authenticated by providing a unique code number that belongs to that person).

The Technology Should Be Non-Intrusive

A DAT technology must not interfere with daily CVO. It must perform its tasks without greatly impeding a driver’s ability to perform his/her daily duties. Also, the DAT must be easy enough to use so that it will not be a nuisance to the driver. For this reason, the majority of current DAT technologies that require the analysis of behavioral traits will not be discussed in this report. For example, a walking gait sensor would require the driver to walk in front of a camera in a specific way. This would be an annoyance to a driver and is not easily or normally performed in daily vehicle operation. Additionally, the technology should not involve excessive examination of the driver. For example, technologies such as retinal scanning will not be discussed in-depth because they require an unacceptable amount of time/intrusion on behalf of the driver.

The Technology Should Have Potential Application in CVO

The technologies discussed in this appendix may not be in current use in CVO or may not yet be commercially available. They all, however, have the potential to be used in CVO in the future. Many biometric technologies currently available exist only in location security applications, like a door access guard. However, if current trends continue, many of these technologies may see utilization in CVO. Other technologies, such as signature or keystroke verification, will not be discussed here because their associated sensors would not easily integrate into a vehicle. Technologies still in early development, such as ear shape identification/matching and body odor sensors, will be discussed, however, not in depth. Table 13 shows the technologies, including their level of detail, mentioned in this appendix (Kalyanaraman, 2006).

Table 13. Driver Authentication Technology List

Technology	Level of Detail Discussed in this Report
Log-in Devices	Full
Finger Print Scanner	Full
Iris Scanner	Full
Vein Recognition	Full
Voice Authentication	Full
Voice Recognition	Full
Hand Geometry Authentication	Full
DNA Sampling	Brief
Ear Shape Scanner	Brief
Body Odor Sensor	Brief
Retina Scanner	None
Walking Gait Sensor	None
Keystroke Recognition	None
Signature Recognition	None

A.3 LOG-IN DEVICES

A log-in device prevents access or movement of a vehicle without proper credentials (i.e., an ID card, prox card, or a password). A user makes a claim to the validity of his or her identity and the system, locally or remotely (i.e., by accessing a centralized database), recognizes or rejects that claim. If the user is recognized, a particular action is allowed, such as unlocking a door or starting a vehicle.

A.3.1 Token Devices Overview

The use of a card and accompanying reader to gain access to a vehicle or initiate start up provides a secure way to authenticate the identity of a driver. Without possession of the card, use of the vehicle is disallowed. A typical system can be seen in Figure 45 (see also Section 3 where different “flavors” of this technology, demonstrated by Satellite Security Systems, BSM Wireless, and GlenHugh Enterprise, are discussed). Often times, as an added measure of safety, the card (or token device) must remain in the reader during operation of the vehicle. Of course, if the card is lost or stolen, access to the vehicle by an unauthorized user would be possible.

Typically, these devices are paired with a biometric device to become a “Smart Card” (discussed later in this appendix in more depth).

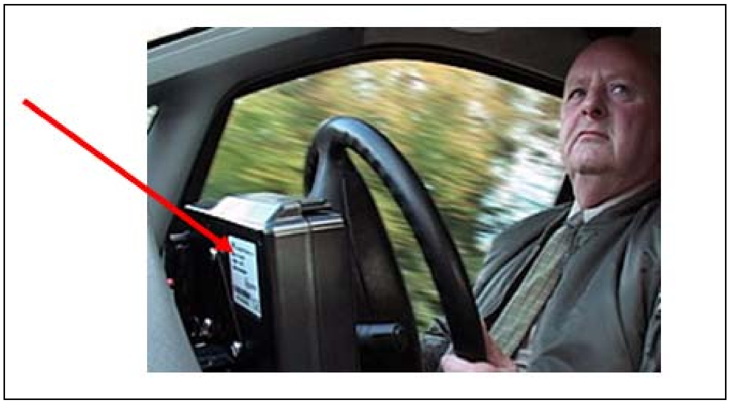


Figure 45. Truck Cab Outfitted With Swipe Card System.

Source: AutoCab, n.d.

A.3.2 Keypad Devices Overview

A common use of verification devices in CVO is the use of a keypad in order to prevent unauthorized access to a vehicle. The keypad, in a sense, acts as a door lock, preventing access into a vehicle without entering the correct code. This is a well-developed technology and seen quite regularly on both commercial and personal vehicles.

In more recent applications, the use of a keypad has been shifted from preventing access into the vehicle to preventing startup without proper input. Figure 46 provides an example of such a device. The use of a keypad in this way, while allowing unauthorized access into a vehicle, will prevent unauthorized startup and also hotwiring. When coupled with communication capabilities, keypads not only prevent unauthorized actions, but also provide the vehicle’s dispatch office with notice of all actions, such as repeated failed attempts at log-in (MAGTEC, n.d.). This feature makes it ideal for use in VIT concepts, that is, after notification of multiple failed attempts at entering the correct code, a dispatcher (i.e., remote vehicle control) or the onboard system itself (i.e., local vehicle control) could initiate a vehicle immobilization protocol and prevent any movement of the vehicle.

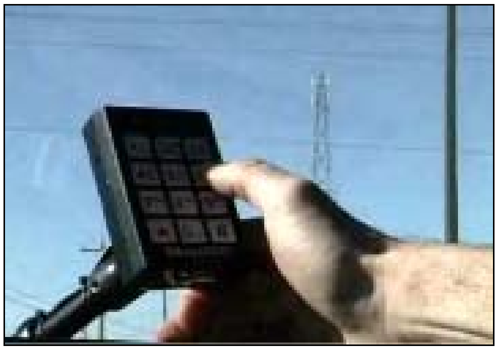


Figure 46. Global Log-in Device

A downside of keypad devices is that they require the knowledge of a password in order to operate; anyone with this knowledge is, therefore, capable of access. Passwords can also be lost, stolen, forgotten, or observed. However, when this password is protected and not compromised, there is little possibility of error in the device. Individual CVO companies determine the length and complexity of a log-in. Additionally, they determine how often log-ins are updated; frequent updates protect vehicles from being accessed by former employees.

Four out of the six companies that demonstrated their vehicle immobilization technologies for this project at Laurens Proving Grounds (LPG) in February 2007 used keypad technology for driver authentication (see Section 3), with one of them combining keypads and a token device (a proximity card).

A.3.3 Log-in Devices and CVO

During the VIT and DAT demonstration and evaluation event at LPG, examples of several keypad and log-in device technologies that were currently integrated on working commercial vehicles were presented (see Section 3). Log-in devices, swipe cards, and proximity cards were all demonstrated. Without proper authentication from the driver, these DAT devices prevented vehicle startup.

The major benefit of using a simple log-in device is that without knowledge of a password or the possession of token, false positives or imitation attempts are nearly impossible. Devices can easily be implemented into the locks or ignition system of a vehicle. GL devices provide an added level of security and communication. Compared to more robust systems, these verification devices are relatively inexpensive. A GL system can be purchased for approximately $1,500 and typically involves a yearly licensing fee (see Section 2 of this report for more details; if there is a communication system already in place, the upfront cost for the device does not change significantly, but the added monthly fee is minimal as discussed in Section 4 of this report). Another benefit is that compared to biometric devices, the time necessary to enroll and become familiar with the device is much shorter. Once the password or token is acquired, the user can operate the system.

The drawback to these systems is that if compromised, a device provides little or no protection against unauthorized access. The only remaining protection in this case is being that the unauthorized user may not be familiar with the system. While an unauthorized user may have knowledge of a log-in, he/she may not know the correct log-in protocol, thereby, providing added security. Clearly, in some applications, simple authentication devices provide more than adequate security. Nevertheless, in high-risk or high-value shipment situations, something more robust may be necessary.

A.4. BIOMETRIC SYSTEMS

Biometric systems use automated methods to recognize unique features of a user. These features can be physiological or behavioral traits. Physiological traits, such as a thumbprint, tend to be stable and unlikely to change during one’s lifetime. Behavioral traits reflect a user’s individual psychological makeup; one’s upbringing and gender also have affects. Examples would include a user's walking gait or typing dynamics. Biometric systems generally identify users in the following way:

1. A sensor takes an observation.
2. The sensor data is used by the biometric system to describe an observation mathematically and creates a biometric signature.
3. The biometric system compares this signature with signatures in a database.

The majority of biometric systems complete their recognition through identification, though some use a combination of verification and identification (Blackburn and FBI, 2004). Biometric systems require users to enroll into a database and have their information captured, extracted, and encoded into a biometric signature so that it can be compared during authentication. A system is only as strong as its enrollment program. A weak program will lead to high levels of false rejection or acceptance (Rosenzweig, et al., 2004).

When comparing different biometric technologies, it is important to use common nomenclature and standards. This way, technologies that may work in different ways can still be compared fairly. It is common in the industry to use different equations and rates in order to present the accuracy of their product. A large concern in the industry revolves around False Rejection Rates (FRR) and False Acceptance Rates (FAR) associated with a particular product. The FAR and FRR are described by equations (1) and (2):

$$\text{FAR}(\lambda) = \text{Number of False Attempts} / \text{Number of Imposter Accesses} \quad \text{(Eq. 1)}$$

$$\text{FRR}(\lambda) = \text{Number of False Rejects} / \text{Number of Client Accesses} \quad \text{(Eq. 2)}$$

where λ = Security Level

The FAR and FRR are dependent on the security level of the system and are opposing parameters. That is, as the security level goes up, the number of false rejections will increase, but the number of false acceptances will decrease and vice versa (Kalyanaraman, 2006). This is apparent in Figure 47. Statistically, they are Type-1 (false positive, or the error of identifying something as true when it is actually false) and Type-2 (false negative, or the error of identifying something as false when it is actually true) errors.

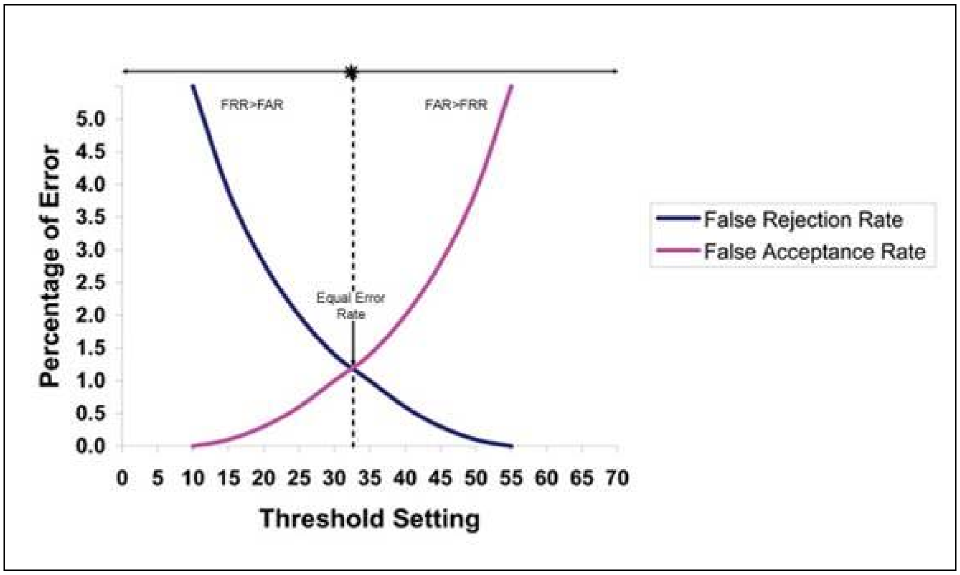


Figure 47. FAR and FRR Graphical Representation

Source: Das, n.d.

The point where the FAR = FRR is called the Equal Error Rate (EER) and is often reported on product information sheets, since it is independent of security level. When available, the FAR, FRR, and EER are used to compare biometric systems in this report.

A.4.1 Biometric Technologies

When evaluating and comparing different biometric technologies, the following criteria should be considered by individual end users of each technology:

Universality: Unlike log-in devices, it is possible that a person may not be able to use a biometric system. For example, someone without an iris could not use an iris scanner.

Uniqueness: In most situations, two people will not have the same biometric signatures; however, some systems may have a difficult time distinguishing between very similar signatures.

Permanence: A person's biometric signature should not change over time; it should remain nearly constant over their lifetime.

Acceptability: A technology can not be so intrusive that users will have little acceptance of the system.

Circumvention: The technology should be difficult to deceive or spoof (Global Security, 2007).

Finger Print Scanning Technology

Fingerprint biometrics is one of the oldest and most tested biometric technologies. Mathematical algorithms are used to create a biometric signature of the print. A print is matched to a stored signature in the database using the minutia, or unique features, of a user's fingerprint. Examples of these unique features can be seen in Figure 48 (Kalyanaraman, 2006).

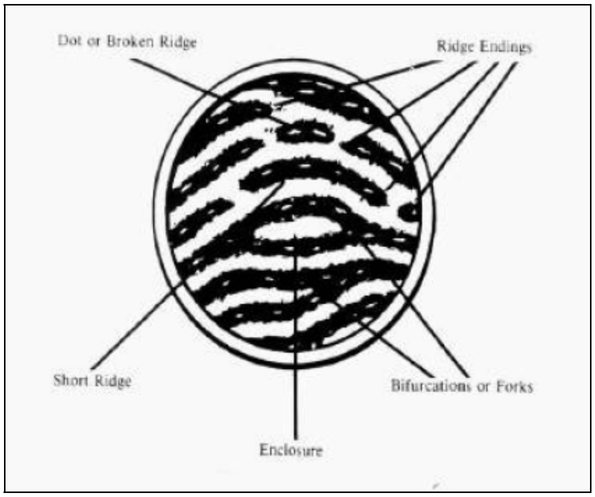


Figure 48. Fingerprint Minutia

Source: Kalyanaraman, 2006

There are several different types of sensors used in the attainment of the fingerprint. Optical sensors use light to make the biometric signature. Electric field sensors measure small local variations in an electric field due to fingerprint ridges. The electric field is created when the sensor releases a small electric signal onto the finger. Finally, a capacitive sensor works by creating a capacitor when the finger comes in contact with its surface. The capacitance changes locally due to the differing shapes and depths of ridges in a fingerprint. Optical technology is the most frequently used. Many manufacturers claim EERs for their product to be less than 1% (BSI, 2004).

It should be noted that some people cannot be enrolled into a fingerprint scanning system. Fingerprints can become worn or damaged due to age, dryness, or work with corrosive chemicals. Additionally, it is not uncommon for some people to be wary of using a fingerprint scanner as fingerprints are often associated with law enforcement and criminal offense (Rosenzweig, et al., 2004).

Fingerprint scanning systems have often been criticized for being easy to spoof. Often, the simple use of a fake finger could fool a scanner. A new technology uses multi-spectral imaging that not only looks at the fingerprint, but also beneath the surface at the finger's deep tissue. It also eliminates the need for a high-quality fingerprint. The manufacturer can enroll 2%-5% of the population that conventional scanners cannot (Lumidigim, 2004). A scanner with this system is presented in Figure 49. Another problem with scanners is that if they become dirty, they may give false readings. If oils from a fingerprint remain on the scanner after use, there may be the possibility that an imposter may gain access due to a false reading. Care must be taken to keep the scanners clean of residual prints.

Fingerprint scanning technology is already being used on vehicles, particularly as a device that prevents vehicle mobilization without authentication. The device in Figure 50 is an after-market device for personal vehicles, but could possibly be used in CVO as well.

Fingerprint scanning technology shows great potential for use in CVO and, if the system is well maintained, it may provide adequate security in many situations. The technology is quick and easy to use, noninvasive, and new technologies are difficult to deceive. Compared to other systems, such as iris or hand scanners, it is also inexpensive. Moreover, it appears that this new generation of scanners have solved some of the problems identified in the 2004 FMCSA FOT (FMCSA, 2004a), such as errors derived by skin temperature variations, or the need to introduce very consistent fingerprints in the biometric reader. Other problems, such ergonomics in a truck and the unwillingness of people to get "fingerprinted," are inherent to this technology and may remain a barrier for its deployment in CVO.

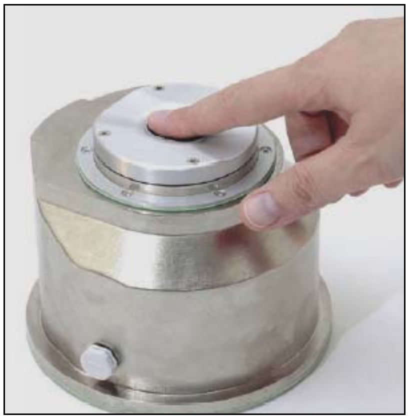


Figure 49. Fingerprint Scanner.

Source: Lumidigim, 2004.

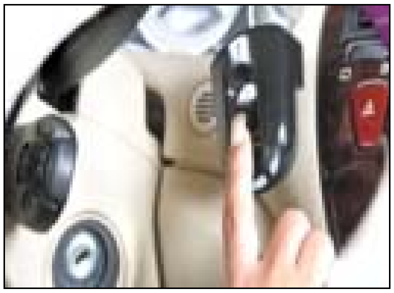


Figure 50. Vehicle Fingerprint Scanner

Source: Spectrotec, 2005.

Iris Scanning Technology

Unlike the more well-known retinal scanning technology, iris scanning is much less invasive to the user. While retinal scanning requires infra-red light to illuminate the retina, which is not clearly visible otherwise, the human iris is plainly visible and is a highly unique attribute. Figure 51 shows a picture of an iris. The probability of two people having the same iris pattern is 1 in 1078 (LG Electronics, n.d.). Even monozygotic twins have different iris patterns.

Iris scanning works by using a black and white camera to take an image of the iris and subsequently turning the image into a digital template to use as a biometric signature. It then identifies the signature by comparing it to the contents of its user database. Iris recognition devices can recognize up to 240 unique features about the iris (high-end fingerprint systems can only recognize 40-60 unique features); even an angled glance at the camera often provides enough information to make an identification. Contrary to popular belief, a living eyeball must be used for identification (i.e., the system checks for pupil adjustment as part of its algorithm).

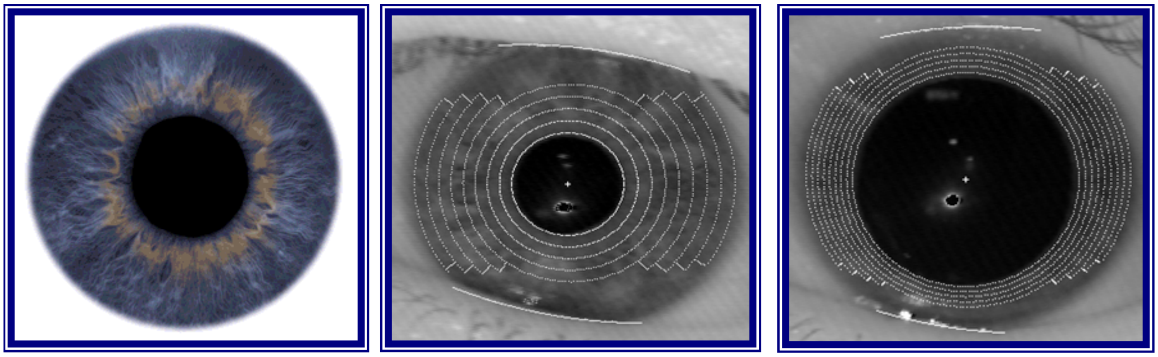


Figure 51. Iris Patterns Used for Identification.

Source: Biometric Watch, n.d.

A benefit of iris scanning technology is that standards have been created to ensure that quality products are released on the market. Iridian Technologies created the ProofPositive™ program to ensure quality products. Proof Positive™ certification is based on the following criteria, quoted from Iridian's website (Iridian Technologies, 2003):

Performance: Certification ensures that iris cameras meet stringent requirements for FARs, FRRs, Failure to Enroll Rates (FTEs), Failure to Acquire Rates (FTAs), and response time.

Interoperability: Proof Positive™ guarantees PrivateID application program interface (API) and KnoWho API compliance and interoperability across all Proof Positive certified cameras and software solutions.

Safety: Proof Positive iris cameras have met stringent government and industry standards for eye safety.

Security: Proof Positive certification ensures compliance with Iridian and industry standards for cryptographic and physical security, as well as countermeasure protection. The protection and integrity of the biometric data is maintained throughout the solution.

Scalability: Proof Positive solutions built on Iridian's PrivateID and KnoWho architecture are scalable to millions of records.

Usability: Proof Positive ensures compliance with Iridian and industry usability standards. Iris cameras and software solutions meet requirements for user feedback, non-intrusiveness, simplicity, consistency, and use for the disabled.

Reliability: Certification ensures that iris cameras and software solutions have met Iridian's minimum system robustness requirements.

Statistically, iris recognition technology has an EER of 1 in 1.2 million, or 0.0008% (LG Electronics, n.d.). Clearly it is a highly accurate technology and is well-equipped to handle high security situations. Adding to this accuracy is the fact that the human iris remains stable over a user's lifetime. Although many people wear glasses or contacts, the technology still works in most cases because the iris is still visible. However, anti-glare and color changing contacts may lead to errors. Price is another concern. The cameras used in the technology can cost a few thousand dollars (no official prices were available), though in a high-risk security situation, this cost may be relatively minimal compared to other concerns.

Vein Recognition Technology

Vein authentication technology consists of a scanner that uses near-infra-red light to create an image of the veins in the hand or finger. The light is absorbed by the de-oxygenized hemoglobin in the vein vessels, and the device traces out these lines to create a signature. This process is shown pictorially in Figure 52. As with the iris, even twins have different vein patterns, making this another extremely unique biometric signature. The difficulty required to forge the veins in the hand make this technology highly secure.

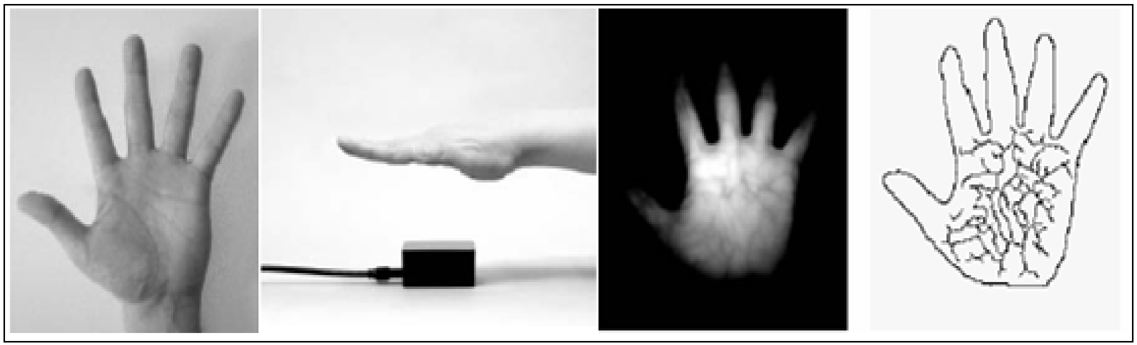


Figure 52. Vein Recognition Process

Source: Watanabe, et al., 2005.

The product shown in Figure 52 is contactless. The hand does not have to touch the sensor itself in order to work; though other products do require contact. The intensity of the light that this product emits is controlled by measuring the surrounding ambient light. The sensor is capable of capturing an image regardless of hand position, but the position with the highest possibility for an accurate result is having the hand perpendicular to the sensor. Internal testing from the manufacturer claims a FRR of 0.01%, and a FAR of 0.00008% or lower, based on 140,000 palms (Watanabe, et al., 2005).

Vein recognition technology has seen some development for application in the transportation industry. The system in Figure 53 fits onto the handle of a vehicle door. The development of a products specific to vehicle access shows promise that more authentication technologies will be created for use in CVO (Knight, 2005).

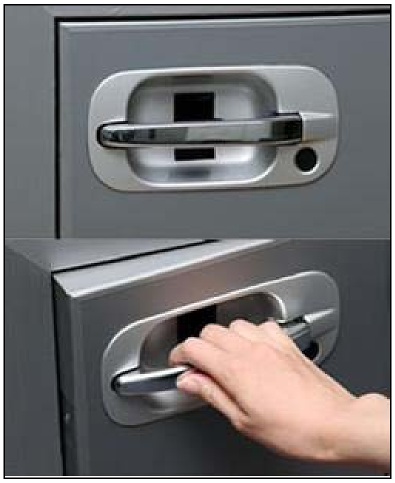


Figure 53. Finger Vein Authentication Technology.

Source: Knight, 2005.

Vein authentication technology's accuracy, small size, and ease of use make it a good candidate for use in CVO. A scanner could easily fit within the cab of a vehicle. It is also a very robust technology, having the potential to work in early-morning/late-night conditions where little ambient light is available. The system is also not affected by unclean hands. If the system is verifying a user, a keypad is also required. Additionally, changes in temperature may affect a user's blood flow which in turn may affect the reader. However, this non-invasive technology may be more comfortable for drivers to use as many may feel wary using technologies that require cameras (Watanabe, 2005).

Voice Authentication Technology

Voice authentication technology, while measuring a behavioral biometric, has potential for use in CVO. Voice authentication is a simple technology: a user speaks into a microphone and the accompanying software creates a biometric signature using the sound, pattern, and rhythm of the user's voice. Algorithms used for verification are able to classify impersonations and detect distortions created by using a recorded voice. A sample user input can be seen in Figure 54 (Authentify, 2007).

In another security mechanism, verification is performed by using a randomly generated string of words. The user must repeat this random phase into the microphone. This prevents the use of a previously recorded message (Authentify, 2007). Some other devices use a neural network to "learn" a user's speech patterns. The use of statistical tools allows the program to predict inflections and accents in a user's speech pattern. This may alleviate concerns that a change in a user's voice because of illness or age may cause a false rejection (Findbiometrics, n.d.).

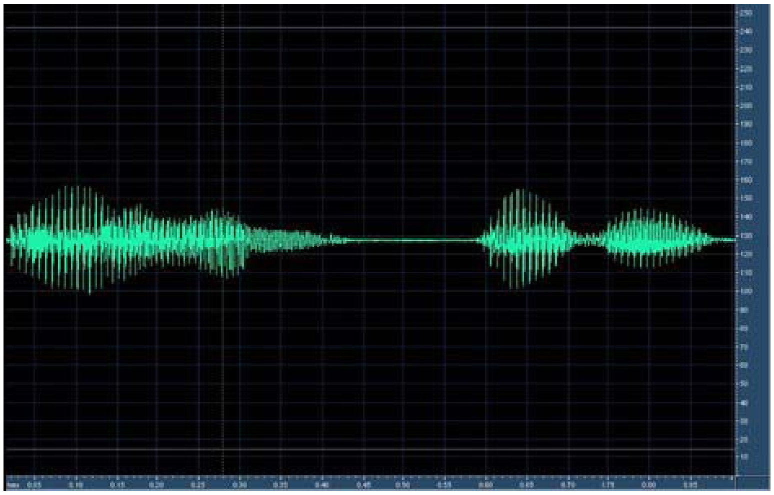


Figure 54. Voice Authentication User Input

Source: Kalyanaraman, 2006

A voice authentication system could easily be implemented into CVO and be relatively autonomous to a driver. The driver would simply be asked to repeat a phrase, and then the vehicle would be mobilized. Situations in which there are large amounts of background noise may, however, not be ideal for this technology. Compared to technologies like iris scanning, voice authentication is much less expensive; the only sensor required is a microphone (Information Technology Standards Committee, 2004).

Facial Recognition Technology

Facial recognition technology is a well-tested method of biometric identification. Using the face to create a biometric signature is a very natural and non-invasive method. Facial recognition can work by comparing geometric attributes of a user to a database. A sample of facial geometric measurement points can be seen in Figure 55 (Kalyanaraman, 2006).

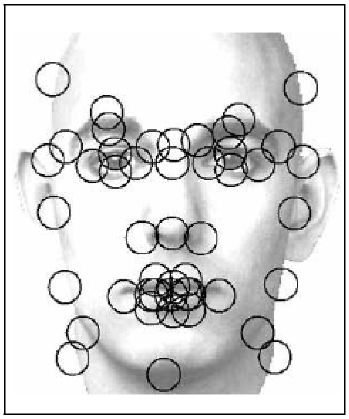


Figure 55. Geometric Measurement Points

One of the more advanced approaches is the Eigenface approach. The Eigenface approach describes images in terms of linear combinations of base images. A set of eigenvectors, or standardized facial ingredients, can be combined to reconstruct a reference image (Turk and Pentland, 1991). Different facial features are singled out and scored individually. Each individual feature is an Eigenface. Sample Eigenfaces are shown in Figure 56. There are many other algorithms for facial recognition: some use neural networks to “learn” the user’s facial attributes (Kalyanaraman, 2006).

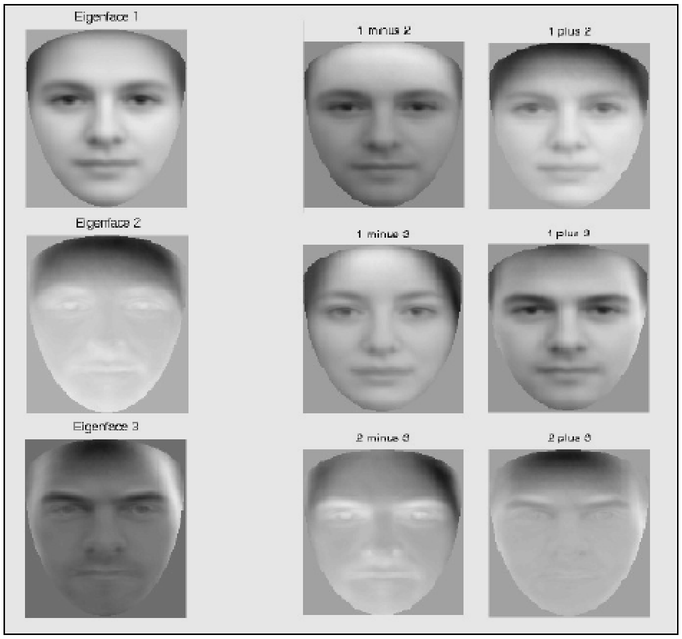


Figure 56. Eigenfaces.

Source: Kalyanaraman, 2006.

Facial recognition can also be implemented using skin recognition technology. Identix, a company that takes such an approach, reports an increase in program accuracy (L-1 Identity Solutions, n.d.). Accuracy data is compiled by the Face Recognition Vendor Test, the last for which results are available was in 2002. There was another scheduled for January 30, 2006, but the data is not yet available. The latest information can be found at: www.identix.com/trends/face.html and www.frvt.org (NIST, 2006). In 2002, under optimal lighting and pose conditions, accuracy was only 90%, at a 1% FAR for verification, and only 73% for identification in a database of 37,437 individuals (NIST, 2006).

The cameras used in facial recognition need not be the quality of those required by some other technologies; a simple surveillance camera may be adequate (Gaits, 2007). The systems are capable of very fast searches. A manufacturer claims to be able to search through 2.7 million eight-image templates per second on a standard 2 GHz PC expanded with 2 GB of RAM. The cameras used, however, require a proper amount of lighting to work (Haase, 2005). This may be a concern for CVO, since users may need to gain access in the dark. Items such as glasses and earrings may also cause problems, as well as changes in facial features due to age. In some situations, where low-cost may outweigh decreased accuracy, facial recognition may be a good fit for a CVO application. However, this would require mounting a camera in the CV cabin, which is viewed by most drivers as an invasion of privacy. Nevertheless, cameras have already been deployed inside truck cabins for security and safety purposes. One such example was given by Wireless Matrix (see Appendix C) in which a large hazmat transportation customer of the company deployed in-cabin cameras to collect data via a 15-minute loop. The collected information is only used in the event of a hard-braking incident or a severe turn that causes a crash (e.g., similarly to airplane black boxes). The "invasion of privacy" concerns were addressed in this case by only storing the "last" 15 minutes of information and by pointing the camera towards the direction of travel instead of the inside the cabin.

Hand Geometry Recognition Technology

Hand geometry technology measures a user's finger length, thickness, and curvature using a camera or infra-red light. Since the signature created using this technology is not as unique as other technologies, it is not descriptive enough to identify a user, but provides a very robust verification system (Ross and Jain, n.d.).

The camera captures two orthogonal, two-dimensional images of the palm and sides of the hand, and measures as many as 90 different points. Finger width, height, and length; distances between joints; and knuckle shapes are all possible measurements. Since the technology measures geometry, finger or palm prints are not necessary for verification (Global Security, n.d.). A typical sensor, with measurement lines, is shown in Figure 57. The rods in the figure are simply used for finger placement; they take no part in measurements. Generally, the verification process can be done in less than five seconds.

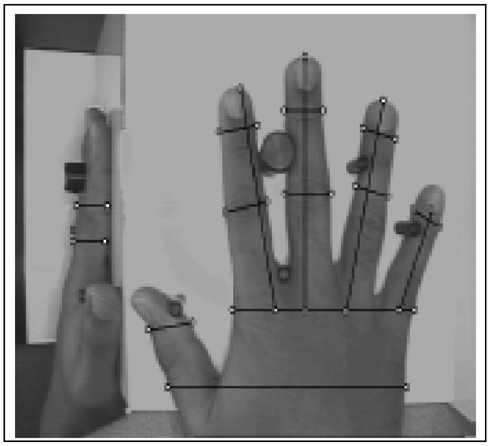


Figure 57. Hand Geometry Measurement System.

Source: Kalyanaraman, 2006.

Currently, systems do not have the ability to detect if a hand is living or not, though the time necessary to create a model that would be able to spoof the system would likely be excessive. The system also tends to be rather large; currently, its overall footprint may be too cumbersome for CVO use. An access system can be seen in Figure 58 (National Center for State Courts, n.d.).

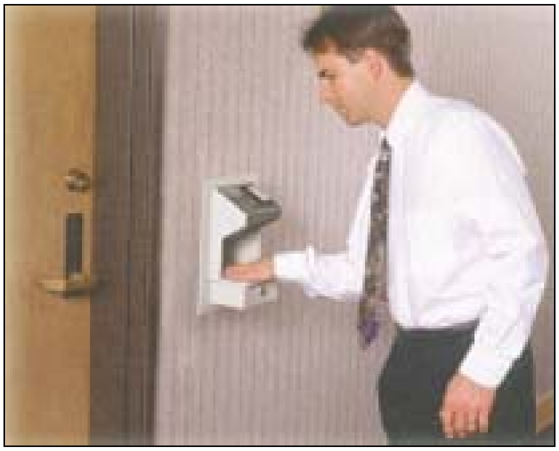


Figure 58. Hand Geometry Measurement System in Use.

Source: Human Recognition Systems, n.d.

If there is space to fit the system, it provides a quick way to verify identity. However, the possibility for spoofing and the inability to identify a user may pose the need for a different technology in high-risk situations.

A.4.2 Future Biometric Technologies

Biometric technologies continue to be developed on a regular basis. This bodes well for CVO, for as technologies continue to be developed they will become faster, less expensive, and more accurate. Some interesting up-and-coming technologies include:

DNA Sampling

DNA sampling requires the user to present some form of tissue, blood, or bodily fluid for authentication. This is a rather intrusive method and quite slow, taking as much as ten minutes to perform. The method used to obtain DNA still needs to be refined. However, such a technology would be very difficult to deceive (Kalyanaraman, 2006).

Ear Shape Sensor

The ear is another biometric feature that does not change over time or with facial expression. It remains fixed in the same location for life. These sensors look like a telephone headset, where a camera takes a picture of the ear. An artistic rendering of the signature is presented in Figure 59 (Kalyanaraman, 2006).

Figure 59. Ear Shape Biometric Signature.

Source: Kalyanaraman, 2006.

Body Odor Sensor

Virtually everyone's smell is unique. Sensors are used to measure the odor from a non-intrusive part of the body, such as the back of a user's hand. Volatiles from the odor are used to create a biometric signature (Kalyanaraman, 2006).

A.4.3 Biometrics Summary

Biometric technologies provide an extra layer of security that log-in devices do not. The requirement of a highly unique feature makes unauthorized use of a commercial vehicle much more difficult. It is clear that different biometric technologies provide different strengths and weaknesses. A report by the International Biometric Group presents a comparison of biometric technologies; a summary of their results are shown in Figure 60 (International Biometric Group, 2006).

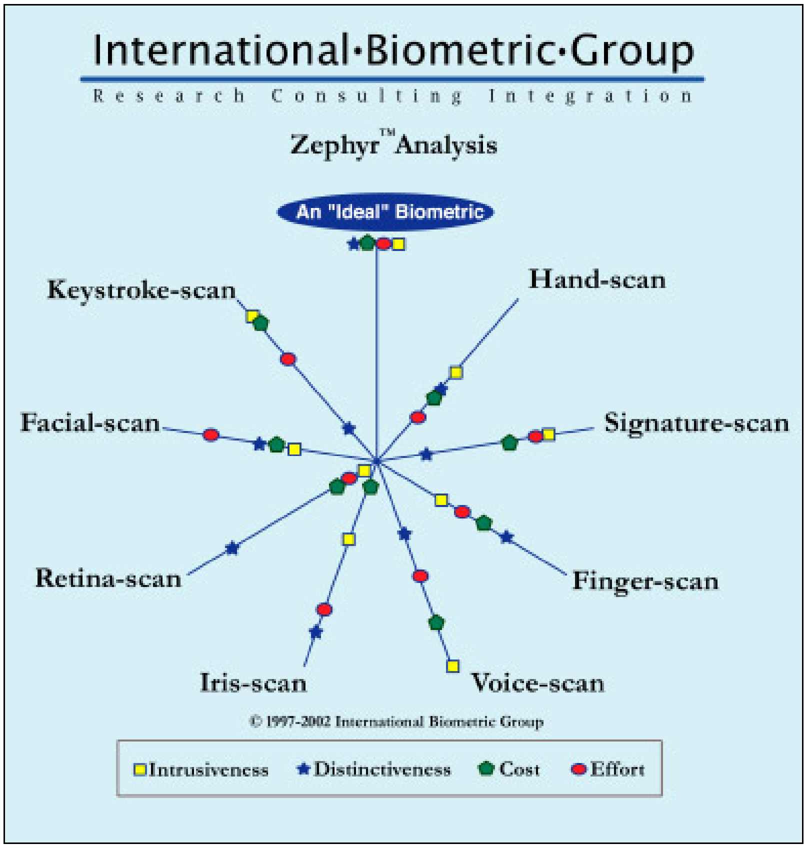


Figure 60. Biometric Technology Comparison.

Poor measures of performance (MOPS) fall towards the center of the chart, while excellent MOPS fall towards the edges. It is clear that there is no single technology that represents the "ideal" biometric. It is up to the end user to weigh the pros and cons of each technology and choose the device best suited for a particular operation.

Biometrics show great promise for future use in CVO. If sensor prices continue to become affordable and accuracy increases, they will become a staple of the transportation industry. However, the need still exists for unified standards across technologies. While the industry is beginning to address this need, it will likely not mature significantly until this concern is fully addressed. Currently, the need for standards exists for the following areas:

- System communications
- Biometric signature extraction
- Signature comparison methods
- Encryption methods
- Signature storage and retrieval methods (Kalyanaraman, 2006)

The creation of these standards may encourage more risk-averse companies to invest in biometric systems.

A.5 SMART CARDS

Smart cards are credit card-sized tokens with embedded integrated circuit chips and memory capacity. They have the ability to store both biographical and biometric information. Often, they are capable of performing biometric matching entirely within the card itself. Smart cards store biometric information without the need for a central computer system. When coupled with a biometric sensor, a smart card provides the ability to both verify and identify a user. Smart cards combined with biometrics provide a multimodal method of authentication. When a user possesses a smart card, both “who you are” and “what you have” are satisfied (International Biometric Industry Association, n.d.).

According to the Smart Card Alliance (quoted directly), smart cards combined with biometrics provide the following benefits:

- Enhanced privacy, securing information on the card, allowing the individual to control access to that information and removing the need for central database access during identity verification.
- Improved security, protecting information and processes within the ID system and actively authenticating the trust level of the environment before releasing information.
- Improved ID system performance and availability through local information processing and contactless ID card and reader implementations.
- Improved system return on investment through the flexibility and upgradeability that smart cards provide, allowing support of different authentication methods and multiple, evolving applications (Smart Card Alliance, 2002).

Smart cards combine the benefits of token devices and biometric technologies. A user must not only possess the card, but must also provide a biometric signature. Smart cards provide the added benefit of being capable of being combined with Radio Frequency Identification (RFID) technology so that the card does not have to come into contact with the biometric sensor used. This “contactless” smart card would not require the user to present the card. Simply having possession would be sufficient. This adds a level of security as well as a level of transparency for the user. When coupled with a high-security biometric device, the smart card provides an extremely robust method for authentication for CVO applications (note: numerous projects have been conducted to study smart cards in a commercial vehicle environment; see, for example, FMCSA, 2004a; DOT, 2000; Gifford, et al., 1996; and FHWA, 1996).

A.6 CONCLUSIONS

Driver authentication technologies clearly have a place in CVO. The security that these technologies add could prevent possible hijackings and terrorist plots involving any type of commercial vehicle. Driver authentication technologies have a place in the heavy vehicle industry, vehicles carrying high-cost cargo, and vehicles carrying hazardous materials. Log-in devices, biometrics, and smart cards provide various strengths and weakness, but all have some form of benefit for CVO applications. The device chosen for a particular operation must be decided upon based on ease of use, amount of invasiveness, and the amount of security provided. As these technologies continue to develop, they will become smaller, faster, and less expensive. It is important that these technologies be understood fully now so that when they begin to become more fully implemented in CVO, their benefits and limitations are well-defined and documented. Questionnaires developed within this project and sent to VIT vendors revealed that several claim to have thousands of DAT devices in use today. It is a fair estimate that over 100,000 are in use in United States CVO market today.

Field Operational Testing (FOT) of these technologies on a small fleet of vehicles and regularly interviewing those involved would provide data on real-world experiences. This data may help to create technologies better suited for use in CVO with a better ability to integrate into VIT. Additionally, bench-top testing could be completed on biometric technologies to obtain better accuracy and error information.

APPENDIX B:
VIT VENDOR/DEVELOPER QUESTIONNAIRE

B.1 OVERVIEW

The materials presented in the subsequent sections were part of a questionnaire package that was distributed in May 2006. Some of the material was developed early in the project, at which time a much more aggressive multi-faceted testing and evaluation effort was envisioned. However, because of project funding constraints, only some components of the envisioned multi-faceted testing were pursued.

B.2 BACKGROUND

Since September 11, 2001, FMCSA has been actively investigating methods to improve safety, security, and efficiency through the Hazardous Materials Safety and Security Technology Operational Test. The purpose of that Operational Test was to quantify the security costs and benefits of an operational concept that applies technology and improved enforcement procedures to hazmat transportation. Subsequently, the FMCSA undertook the Expanded Satellite Tracking and the Untethered Trailer Tracking and Control Security projects. In 2005, the U.S. House of Representatives Conference Report 108-792 stated that further testing of technologies, including vehicle disabling would be necessary.

This VIT Testing and Evaluation Project is being conducted to support the Congressional need called out in the aforementioned report, and it builds on the experience and lessons learned from previous field operational tests in order to generate Best Practices and a COO. The Best Practices and COO will be based on data and information gathered from identified vendors (like yourselves) via various media, interaction with organizations involved with previous VIT testing and evaluation efforts, as possible, from experience with vendor demonstration vehicles and vendor laboratories, and possibly independent testing and evaluation by a VIT Project Team.

The purpose of this initiative is to test and evaluate various commercially available VITs for assessment of Best Practices and for input into COO development. It is intended to cover multiple technologies from simple to sophisticated. This questionnaire will assist the project team in determining which of the available technologies would be appropriate to test as part of the project. Although not all technologies will be tested, information on all technologies will be included in our analyses. It is NOT the purpose of this project to compare one vendor's products with that of another. Rather, information related to the functionalities and operability of VITs and their associated protocols for utilization will be sought. Positive examples for applying VITs for enhanced safety and security of Hazmat shipments will be examined for their applicability as national guidelines for VIT implementation in Hazmat shipment safety and security.

Your participation in this project, as a vendor for VITs or vehicle immobilization systems/networks, is extremely important for meeting the Congressional goals of this project. It is your expertise and experience with VITs that will provide the basis for the development of industry Best Practices and Concepts of Operation. In the longer term, such guidelines will contribute to the safety and security of Hazmat shipments by leading to technologies and systems that are more robust, more easily understood and applied, and capable of being adapted to new safety and security situations or circumstances.

This project will involve demonstration testing and evaluation of VITs for five functional requirements (FRs):

FR1: Vehicle disablement if the vehicle senses an unauthorized driver
FR2: Vehicle disablement/shutdown in the event of a loss of signal
FR3: Remote vehicle disablement/shutdown by the driver
FR4: Remote vehicle shutdown by a dispatcher
FR5: Remote vehicle shutdown by law enforcement

Testing and evaluation will be conduced within a multi-faceted approach. For the technologies selected for testing, approaches may include one or more of the following test methods. A description of each of these approaches is provided in the next section.

- Vendor-Owned Vehicle Demonstrations
- Vendor-Owned Laboratory Demonstrations
- Independent Laboratory Testing and Evaluation
- Independent On-Vehicle Testing and Evaluation
- Observation Testing and Evaluation of a Commercial Fleet

In preparation for determining which VITs will be selected for testing and evaluation, ORNL has prepared a questionnaire (see below) to assist with the necessary data collection. Information gathered via this questionnaire will be utilized by ORNL and FMCSA to determine a series of vendor visits to be conducted in the third quarter of 2006 to gather additional information.

B.3 POTENTIAL TESTING AND EVALUATION APPROACHES

Vendor-Owned Vehicle Demonstrations: Some vendors have their VITs operating on various vendor-owned vehicle platforms. ORNL will work with vendors that have such platforms to identify an opportunity to assess, first-hand, the functionality of the VITs within an operational vehicle environment. Special scenarios related to the FRs and COO may be requested to be performed to allow for an evaluation of the VIT that has greater face validity. ORNL may request that some instrumentation may be added to the vendor's vehicle platforms to gather selected quantitative information during the demonstrations—such instrumentation will not be added without the concurrence of the vendor. Staff from ORNL, TN-DOS, and possibly FMCSA may be present for these demonstrations.

Vendor-Owned Laboratory Demonstrations: Several of the vendors have indicated that they have their technologies functioning within a vendor-owned laboratory environment in addition to, or in lieu of, a demonstration vehicle. These laboratory environments provide a demonstration potential that although it does not have the face validity of a vehicle-based demonstration, can demonstrate the controlled functionality of a vendor's product. Special scenarios as described in the previous testing and evaluation approach may not be as likely; however, emulated scenarios may be possible. The compilation of some quantitative information may be easier, and testing in difficult or challenging environments may be emulated more easily in a laboratory setting.

Independent Laboratory Testing and Evaluation: There may be instances where a closer look at selected VITs might be desirable. For these technologies, ORNL will request that vendors loan or donate the VITs to ORNL for independent laboratory testing. Such testing will likely be done in the instrumentation labs at ORNL or at the National Transportation Research Center (NTRC—see http://www.ntrc.gov/visit.shtml) located near ORNL, in Knoxville, Tennessee. Such testing will allow the VIT team to gain greater familiarity with the technology, will allow more depth in testing and evaluation as compared to testing and evaluation in vendor-owned laboratories, and will allow for testing and evaluation that may not be able to be carried out in vendor-based laboratories.

Independent On-Vehicle Testing and Evaluation: For several of the VITs, it may be beneficial to conduct independent, on-vehicle testing and evaluation. For these tests, a test vehicle (a class-8 tractor-trailer or possibly another vehicle platform) will be available at a closed test site that can accommodate vehicle-based testing and evaluation. ORNL will request that vendors loan or donate the VITs to ORNL for independent on-vehicle testing. ORNL will integrate the VITs into the test vehicle (either at the test site, if relatively easy, or at the NTRC if installation is more complex). Vendor participation in these efforts may also be requested. Testing will involve specific scenarios or COO-based scenarios developed by ORNL and TN-DOS. A professional driver will operate the test vehicle. Such testing will allow the VIT team to gain greater familiarity with the technology, and will allow more depth in testing and evaluation as compared to testing and evaluation on vendor-owned vehicle platforms.

Observation Testing and Evaluation on a Commercial Fleet: Several of the vendors have already deployed versions of their VITs for use by carriers and shippers in North America. ORNL would like to talk with users to see how VITs have been deployed, identify good protocols associated with VIT usage, and hear about instances wherein the VITs have been utilized to thwart a theft or hijacking. Working with the end-user over the time period of this test will be desirable. That is, ORNL would meet periodically with user carriers or fleets to review recent usage histories of their VITs. Compiled information would be reviewed by the user and maintained anonymously by ORNL. Such real-world opportunities will provide data related to protocols, ease of use, etc., that will be useful for generating Best Practices and input for the COO.

B.4 VEHICLE IMMOBILIZATION TECHNOLOGY (VIT) QUESTIONNAIRE

Please complete one questionnaire for each VIT that your company produces.

1. Please provide the information below on a VIT that your company produces (or is involved with) that can provide one or more of the vehicle disabling functions listed below (i.e., FR1 through FR5) (if your company has more than one VIT product, please complete this form for each VIT produced by your company). The Functional Requirements (FRs) are:

FR1: Vehicle disablement if the vehicle senses an unauthorized driver
FR2: Vehicle disablement/shutdown in the event of a loss of signal
FR3: Remote vehicle disablement/shutdown by the driver
FR4: Remote vehicle shutdown by a dispatcher
FR5: Remote vehicle shutdown by law enforcement

a. Name of the product:____

b. Briefly describe the purpose of the product:________________________________

____

____

____

____

c. Please circle all of the functional requirements that can be provided by the product.

FR1 FR2 FR3 FR4 FR5

d. For those functions <u>not</u> circled in question 1c, does your company intend on providing these functions with this product in the future (Please circle a response)?

YES NO

If so, please circle which FRs will be provided.

FR1 FR2 FR3 FR4 FR5

(Page 1 of 11)

Question 1 continued:

e. Does your company currently provide, or intend on providing any of the functional requirements not addressed by the product identified in item 1a via another product (Please circle a response)? If so, please name the product.

YES NO Name: ______________________________

Which functional requirements will this product provide?

FR1 FR2 FR3 FR4 FR5

f. Please describe <u>how</u> your product provides each of the FRs circled in question 1c (please continue on a separate sheet of paper if necessary).

____

____

____

____

____

2. Please provide the technical specifications (e.g., power requirements, range, data exchange rate, speed of execution, etc.) for the product named in question 1a (or please provide a technical specification list) (please continue on a separate sheet of paper if necessary).

____

____

____

____

____

____

Question 2 continued:

a. What precautions and safeguards are available to discourage hacking into your product or disabling your product once it is deployed?

____

____

____

____

____

____

____

b. Is your product susceptible to electronic interference (Please circle a response)? Please elaborate.

YES NO

____

____

____

____

____

____

3. What volume of this product has been sold or is in-use in the industry?

Number sold or in-use: ______________________________

4. Please generally describe installation of the product. Is it vendor-installed only? How long does it take (per vehicle)? What qualifications are required for someone to install the product? Is any special equipment needed for installation? How invasive into the vehicle is the installation (air/electrical lines cut?)?

____

____

____

____

____

5. Please describe any periodic maintenance or calibration requirements for this VIT.

____

____

____

____

6. Is the installation of your VIT restricted to certain vehicle types, or to vehicles with certain features (please circle a response)? If yes, please describe the restrictions and the types of vehicles that can accept this VIT.

YES NO

____

____

____

____

____

7. Please describe any special training that the users of your VITs must take in order to fully utilize your product. …the length of the training. ….where the training is provided.

____

____

____

____

____

____

8. Please describe how your product is utilized by a fleet or carriers? That is, does it require driver intervention? ….Does it require GPS? ….Who gets notified, and by what means are they notified when your product senses a violation? Please continue on a separate sheet of paper if necessary.

____

____

____

____

9. Please describe what happens when your product senses a violation. Please describe any protocols (rules) for response that you or your customers advocate for the use of your product. Please continue on a separate sheet of paper if necessary.

____

____

____

____

10. Are there situations or circumstances that would be problematic for the performance of your VIT? For example, does it perform less reliably during poor weather? Do city "canyons" cause problems? Do you ever find your product "cutting out," and if so, why? Please elaborate.

____

____

____

____

____

11. What aspect of your VIT do you feel could be improved? What can be done to make it even better?

____

____

____

____

____

12. Please describe any instances where your VIT has worked exceptionally well. Please provide a detailed description of the circumstances, and the events surrounding the circumstance. Please continue on a separate sheet of paper if necessary.

____

____

____

____

____

Please share the direction of the evolution of this VIT? How do you see your product changing over time? Will the customer base be the same? What features or functionalities do you think might be added? Please elaborate.

____

____

____

____

____

13. Has your product ever been used in conjunction with law enforcement? If so, please elaborate.

____

____

____

____

14. What are the costs associated with this VIT?

a. Cost of the product: ________________

b. Does the cost vary with volume purchased (Please circle a response)?

YES NO

If so, please describe:____

____

____

____

____

Question 14 continued:

c. Is the equipment cost associated in any way with a service contract?

YES NO

If so, please describe: ____

____

____

d. annual maintenance costs:: _______________

e. monthly fees: __________________________

f. periodic licensing fees: ________________ period of license: ____________

g. other costs (please elaborate): ______________________________________

____

____

____

15. Does your company own a vehicle-based demonstration platform that has (or could have) your VIT product mounted on it for demonstration or test purposes?

YES NO

If yes, please describe the vehicle.______________________________________

____

____

____

____

____

(Page 8 of 11)

Question 15 continued:

a. Would your company be willing to demonstrate your products on this vehicle for the VIT research team (please circle a response)?

YES NO

16. Does your company own or have access to a development or testing laboratory (please circle a response)?

YES NO

a. If yes, would your company be willing to demonstrate your VIT in this laboratory for the VIT research team (please circle a response)?

YES NO

17. Would your company be willing to loan or donate your VIT to the VIT research team for independent testing (please circle a response)?

YES YES (with conditions – please elaborate below) NO

Please describe conditions: ____

____

____

____

____

18. Would your company be willing to introduce the VIT team to some of your customers to discuss with them how they have used your VIT and their experiences with the use of your product (please circle a response)?

YES YES (with conditions – please elaborate below) NO

Please describe conditions: ____

____

____

19. Please provide the following contact information, and information related to your company and VITs.

a. Primary contact with your company for the VIT team:

Company Name: ____

Contact Person: ____

Contact Person's Office phone(s): ______________________________

Contact Person's E-mail address: _______________________________

Business Address: ____

____

Company website: ____

Product website: ____

b. Does your company have literature, brochures, videos, or other information about this VIT that you can share publicly (please circle a response)?

YES NO

If yes, would you please forward this material to:

Bill Knee or Oscar Franzese
Center for Transportation Analysis
Oak Ridge National Laboratory
2360 Cherahala Blvd.
Knoxville, Tennessee 37932

Office Phone: (865) 946-1300
E-mail address: kneehe@ornl.gov / franzeseo@ornl.gov

(Page 10 of 11)

20. Is there any other information about your VIT that you would like to share with the VIT research team? If so, please elaborate.

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

APPENDIX C:
DEMONSTRATION TESTS PROGRAM

C.1 BACKGROUND

Prior to the VIT demonstration, the participating vendors were given a set of guidelines describing the proposed tests, specifically what type of capabilities they had to demonstrate. Since there was a limited time allocated to each company for the VST (Phase I) and VDT (Phase II) demonstrations, it was left to the vendors to decide the order in which different capabilities were to be demonstrated within each phase. The general schedule of events (supplied by the project researchers to the vendors) and the demonstration tests program (proposed and described by the vendors to the project researchers) are included below.

C.2 SCHEDULE OF EVENTS

Start Time	End Time	Location	Description of Events
7:30	8:30	Test Track	Videotaping Equipment Setup and Testing.
7:30	8:00	Test Track	Vendors report to testing area with their vehicles.
8:00	8:15	Biltmore Bldg*	Safety and track usage discussion (LPG personnel).
8:15	8:25	Biltmore Bldg	Discussion of project objectives and goals.
8:25	8:45	Biltmore Bldg	Summary of test objectives and procedures. Q&A for participating drivers.
8:45	9:00	Test Tack	Positioning of test participants on the test track. This includes bringing the first demonstration vehicle to the test area and the deployment of test assistance personnel at key points alongside the test track.
9:00		**Test Track**	**Start of Demonstration Tests**
9:00	9:45	Test Track	Satellite Security Systems/Blue Bird – FRs 3, 4 and 5 Demos (+ Geofencing Test)
9:45	10:00	Asphalt Lake	Satellite Security Systems/Blue Bird – Driver Authentication Demonstration
10:00	10:15	Asphalt Lake	Satellite Security Systems/Blue Bird – Other VITs
10:00	10:20	Test Track	Qualcomm/Celadon/Magtec Set up
10:20	11:05	Test Track	Qualcomm/Celadon/Magtec – FRs 3, 4 and 5 Demos (+ Geofencing Test)
11:05	11:20	Asphalt Lake	Qualcomm/Celadon/Magtec – Driver Authentication Demonstration
11:20	11:35	Asphalt Lake	Qualcomm/Celadon/Magtec – Other VITs
11:20	11:35	Test Track	International Truck and Engine Corp Set up
11:35	**12:30**	**Biltmore Bldg**	**Lunch**
12:30		**Test Track**	**Demonstration Tests Continue**
12:30	1:15	Test Track	International Truck and Engine Corp – FRs 3, 4 and 5 Demos
1:15	1:30	Asphalt Lake	International Truck and Engine Corp – Driver Authentication Demonstration
1:30	1:45	Asphalt Lake	International Truck and Engine Corp – Other VITs
1:30	1:45	Test Track	BSM Wireless Set up
1:50	2:35	Test Track	BSM Wireless – FRs 3, 4 and 5 Demos (+ Geofencing Test)
2:35	2:50	Asphalt Lake	BSM Wireless – Driver Authentication Demonstration
2:50	3:05	Asphalt Lake	BSM Wireless – Other VITs
2:50	3:05	Test Track	GlenHugh Enterprise Set up
3:10	3:55	Test Track	GlenHugh Enterprise – FRs 3, 4 and 5 Demos (+ Geofencing Test)
3:55	4:10	Asphalt Lake	GlenHugh Enterprise – Driver Authentication Demonstration
4:10	4:25	Asphalt Lake	GlenHugh Enterprise – Other VITs
4:30	**5:00**	**Biltmore Bldg**	**Adjourn - End of Demonstration Tests**

*Facility attached to LPG Test Track 8.

C.3 DEMONSTRATION TESTS PROGRAM

09:00 – 10:15 Satellite Security Systems/Blue Bird

VST Demonstration Tests

1. Test Track Test 1: motion test at lower speed; engine shutdown via phone call to 7/24 Monitoring and Support Center (MSC).
2. Test Track Test 2: motion test at higher speed; engine shutdown via phone call to 7/24 MSC.

VDT Demonstration Tests

1. Demonstrate the ability to enable/disable starter via valid/invalid card swipes.
2. Demonstrate remote engine shutdown by depressing panic button.
3. Demonstrate remote engine shutdown via phone call to 7/24 MSC (simulate law enforcement protocol).
4. View the Global Guard Enterprise Solution (GGES) software and Virtual Parameters (geofencing) reports and additional reporting and mapping features.

10:20 – 11:35 MAGTEC/Qualcomm/Celadon

VST Demonstration Tests

1. VST 35-40 MPH – Qualcomm/Celadon Demo Standard Road Configuration
    a. Qualcomm/Celadon will demonstrate the default working configuration of the MAGTEC M5K with a step down to 10 MPH (5 min), but not to shutdown.
    b. The vehicle will then park at the Asphalt Lake for Driver Authentication Demonstrations (second part; see below).
2. VST 35-40 MPH – MAGTEC Demo Short Stepping Configuration to full shutdown.
3. VST 35-40 MPH – MAGTEC Demo Geofencing and Speed Threshold of 40 MPH without a MAGTEC ACS.
4. VST Hijack - MAGTEC Demo Time Delayed Shutdown for Hijack. Based on a Hijack Scenario, MAGTEC will demonstrate the hijack notification system and the automatic time delayed shutdown of a vehicle.

VDT Demonstration Tests

1. Driver Authentication - Celadon
2. Driver Tamper - MAGTEC
3. Driver Alarm Demonstration - MAGTEC
4. Idle Protection Demonstration – MAGTEC
5. Reconfigure for COM and Signal Protection - MAGTEC
6. Communication Signal Loss Protection – MAGTEC/Celadon
7. Communication Tamper Protection - MAGTEC

11:35 – 12:30 Lunch

12:30 – 01:45 International Truck and Engine Corporation

VST Demonstration Tests

Two different modes will be demonstrated: remote shutdown mode and vehicle depower mode. While in remote shutdown mode, vehicle operation will cease. The normal anti-theft mode will not re-enable normal vehicle operation. When the depower mode is active, there will be audible and visible alarms inside the cab, as well as performance impact to the vehicle. The vehicle will remain operational during this mode.

1. Shutdown at Speed with Remote Re-enable: This demonstration consists of entering the shutdown mode when the vehicle is operational and traveling at normal highway speeds. There will be audible and visual alarms in the cab, but vehicle operational will not cease until the vehicle reaches speeds lower than ~5 mph. Once that speed is reached, vehicle operation will cease. The vehicle will not be operational until it is re-enabled. The demonstration will end with the vehicle being re-enabled remotely. Concepts: Shutdown while at speed, Remote re-enable, automatic engagement of Park Brake if vehicle is stationary, automatic engagement of Hazard lights and Brake lights if vehicle is in motion (provides warning to surrounding traffic).
2. Severe Depower with Remote re-enable: This demonstration consists of placing the vehicle in a severe depower state and demonstrating the performance impact to the vehicle. The demonstration will end with the vehicle being re-enabled remotely. Concepts: Severe depower (provides limited capability to operate vehicle), Remote re-enable, Automatic engagement of Hazard lights and Brake lights (provides warning to surrounding traffic).
3. Extreme Depower with Local re-enable: This demonstration, like the previous one, consists of disabling the vehicle by depower at an extreme level. The vehicle will be operating, but will only be able to move at a slow rate of speed. The demonstration will end with the vehicle re-enabled locally (via the in-cab keypad). Concepts: Extreme depower (provides only enough capability to move vehicle at a slow rate of speed), Local re-enable (provides method to re-enable vehicle if out-of-coverage), Automatic engagement of Hazard lights and Brake lights (provides warning to surrounding traffic).

VDT Demonstration Tests

1. Theft-deterrent. This section will demonstrate theft-deterrent technology. The vehicle will automatically disable when operated by an unauthorized driver.
   a. Theft Case: This demonstration consists of automatic disablement when an idling vehicle is driven by an unauthorized driver. Concepts: Automatic vehicle disablement without authentication, latching capability to survive power loss.
   b. Driver Authentication Technology: This demonstration consists of driver authentication when the vehicle is idling without which, the vehicle will automatically disable. Concepts: Driver Authentication.
2. Hijack Case: This section will demonstrate driver alert to Control Center
   a. Driver Alert Notification: This demonstration consists of a driver notification sent to a Control Center regardless of ignition state. Vehicle can be “on” or “off” for the alert to be sent. Concepts: Driver alert notification regardless of ignition state

b. Shutdown while stationary with Local re-enable: This demonstration consists of a Control Center command to disable the vehicle based on a driver alert notification. Immediate shutdown will result if the vehicle is stationary, regardless of ignition state. Concepts: Immediate vehicle disable with local re-enable.

01:50 – 03:05 BSM Wireless

VST Demonstration Tests

1. Authorized administrator shutdown.
2. Geofence crossed shutdown.

VDT Demonstration Tests

1. Driver authentication including,
   a. key fob entry
   b. voice commands
   c. proximity card authorization
   d. keypad authorization
   e. silent alarm triggered by keypad entry (hijack scenario)
2. Key fob shutdown.
3. GPS tamper shutdown.
4. Box tamper shutdown.

03:10 – 04:25 GlenHugh Enterprise

VST Demonstration Tests

1. Geofence test.
2. VST tests at normal speed.
3. Hi-jack from stationary position.

VDT Demonstration Tests

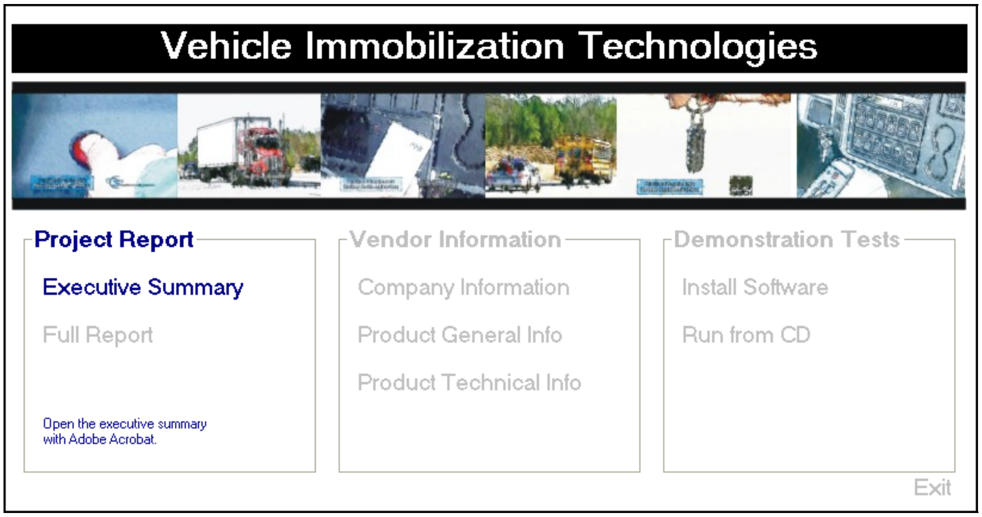
1. VDT test (immobilizer VDT all circuits disabled, driver authentication).
2. VDT test (safe stop idle, driver authentication).
3. VDT test (remote engine starter disable).

04:30 – 05:00 Adjourn – End of Demonstration Tests

APPENDIX D:
VENDOR INFORMATION AND DEMONSTRATION TESTS VISUALIZATION SOFTWARE

D.1 BACKGROUND

The information collected in this project—vendors' questionnaires and data trajectory and speed information from the demonstration tests—can be accessed and visualized using the software provided with the companion CD. To run the software, simply insert the CD in the CD/DVD drive and close the drawer; the software should run automatically showing an access window as show in Figure 61 (note: if the software fails to start automatically, use the Windows Explorer feature to access the information on the CD and double-click on the file named "VITDTCD.exe").



Open the executive summary with Adobe Acrobat.

Figure 61. VIT Information Visualization Interface

Three different frames are presented to the user to access the report in pdf format (left-hand side frame), vendor information (central frame), and the demonstration tests (right–hand side frame). As the mouse cursor is moved over the provided window, different options are highlighted and can be accessed by clicking the left-mouse button on that option. Figure 61 shows the Project Report - Executive Summary highlighted; by clicking on that highlighted label, Adobe Acrobat will be launched and the executive summary of the project loaded (note: users have to have Adobe Acrobat reader installed in their computer for this option to work).

D.2 VENDOR INFORMATION SOFTWARE INTERFACE DESCRIPTION

Three different options are offered to the user to access the information collected through the questionnaire package that was distributed to VIT providers. Moving the mouse cursor to the "Vendor Information" frame highlights it, permitting access to company information, as well as general and technical information about the different VIT products offered by the different vendors. By double-clicking on the "Company Information" option (Figure 62), a screen with contact information about the VIT vendors that completed the questionnaire is shown (see Figure 63). The controls located on the lower left corner of this dialog box allow the user to navigate the database.

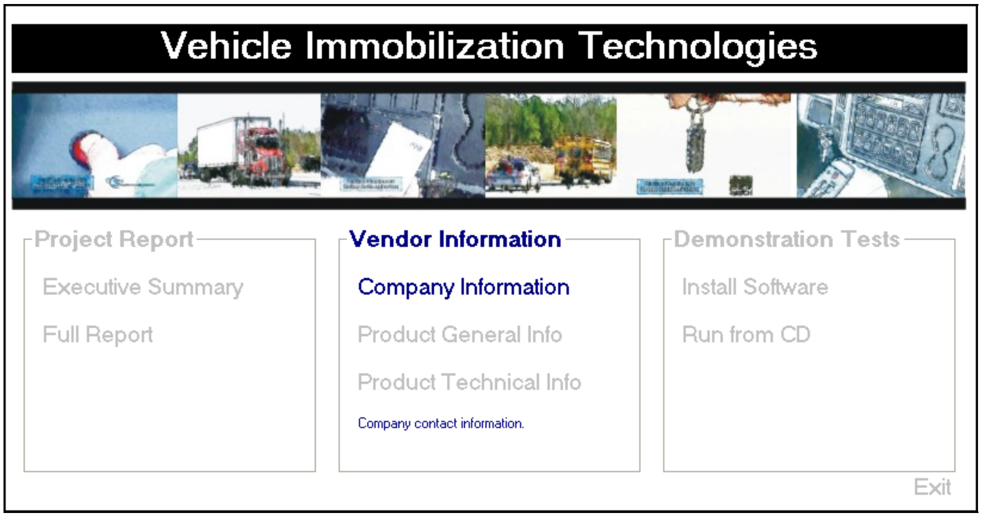
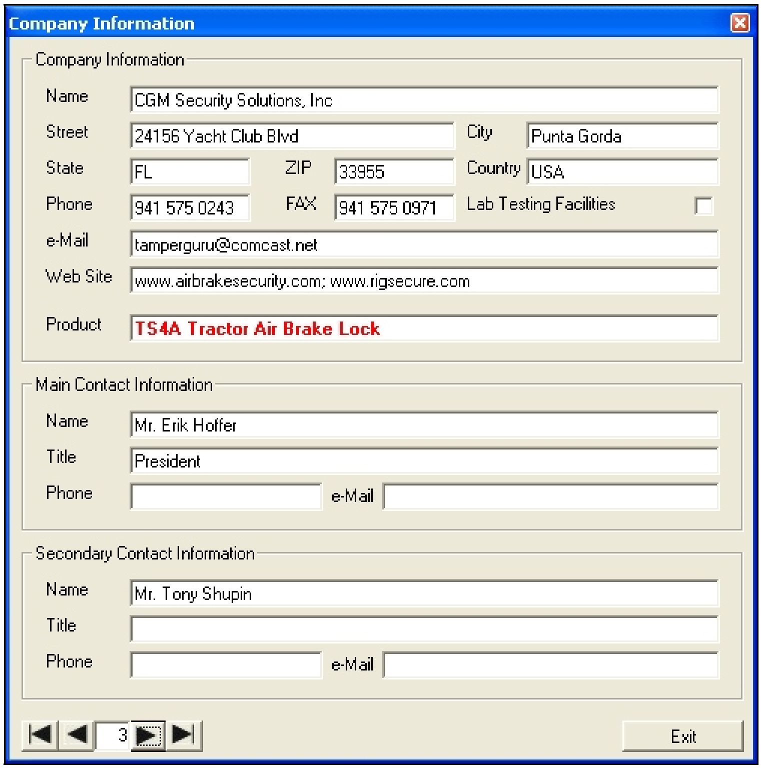


Figure 62. Interface Background



Company Information

Name: CGM Security Solutions, Inc
Street: 24156 Yacht Club Blvd
City: Punta Gorda
State: FL
ZIP: 33955
Country: USA
Phone: 941 575 0243
FAX: 941 575 0971
Lab Testing Facilities □
e-Mail: tamperguru@comcast.net
Web Site: www.airbrakesecurity.com; www.rigsecure.com
Product: TS4A Tractor Air Brake Lock

Main Contact Information

Name: Mr. Erik Hoffer
Title: President
Phone:
e-Mail:

Secondary Contact Information

Name: Mr. Tony Shupin
Title:
Phone:
e-Mail:

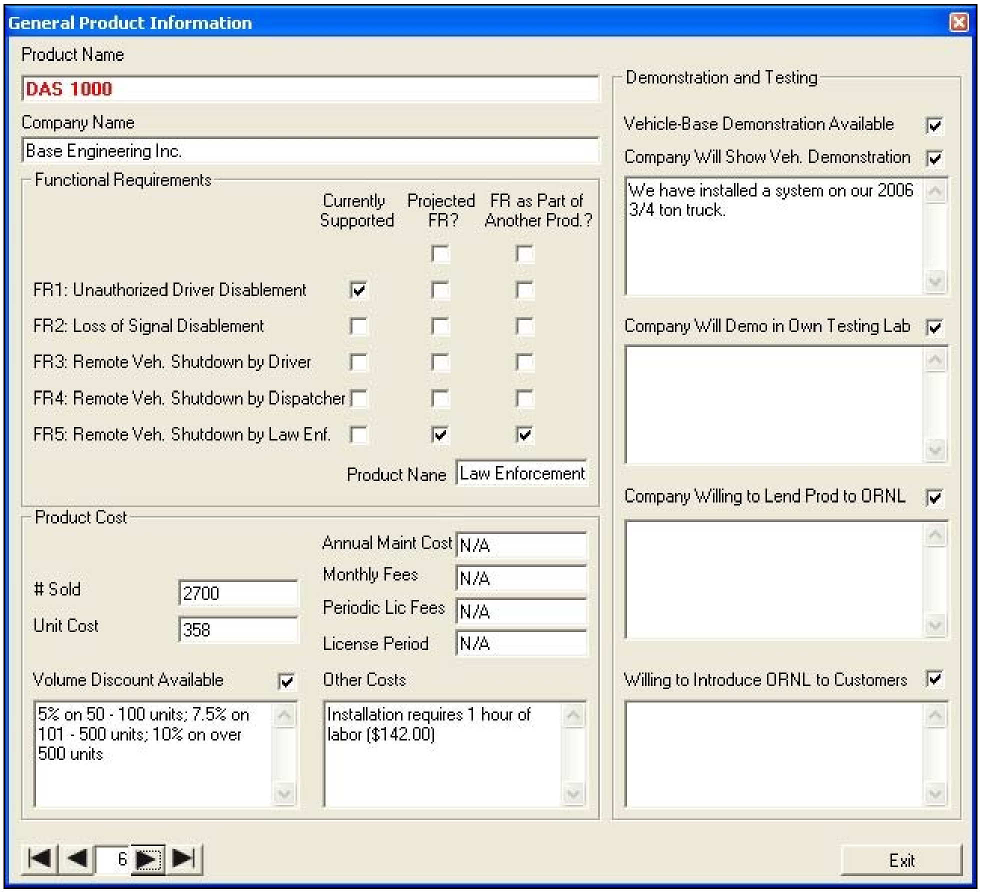
3

Figure 63. VIT Vendor Contact Information

In the same way as in the case of "Company Information," general and technical product information can be access from the main screen (Figure 61). By clicking on the "Product General

Info" and "Product Technical Info" options, dialog boxes are displayed similar to the ones shown in Figure 64and Figure 65, respectively. As in the case of the company contact information dialog box, database navigation is accomplished using the controls located on the lower left corner of the dialog boxes. All the dialog boxes can be closed by clicking on the "Exit" button (lower-right corner).

The information displayed on these three dialog boxes is contained in a Microsoft Access database, which can be found in the "Database" folder included in the CD.



General Product Information

Product Name: DAS 1000

Company Name: Base Engineering Inc.

Functional Requirements

	Currently Supported	Projected FR?	FR as Part of Another Prod.?
		□	□
FR1: Unauthorized Driver Disablement	☑	□	□
FR2: Loss of Signal Disablement	□	□	□
FR3: Remote Veh. Shutdown by Driver	□	□	□
FR4: Remote Veh. Shutdown by Dispatcher	□	□	□
FR5: Remote Veh. Shutdown by Law Enf.	□	☑	☑

Product Nane: Law Enforcement

Product Cost

# Sold	2700
Unit Cost	358
Annual Maint Cost	N/A
Monthly Fees	N/A
Periodic Lic Fees	N/A
License Period	N/A

Volume Discount Available ☑

5% on 50 - 100 units; 7.5% on 101 - 500 units; 10% on over 500 units

Other Costs: Installation requires 1 hour of labor ($142.00)

Demonstration and Testing

Vehicle-Base Demonstration Available ☑

Company Will Show Veh. Demonstration ☑

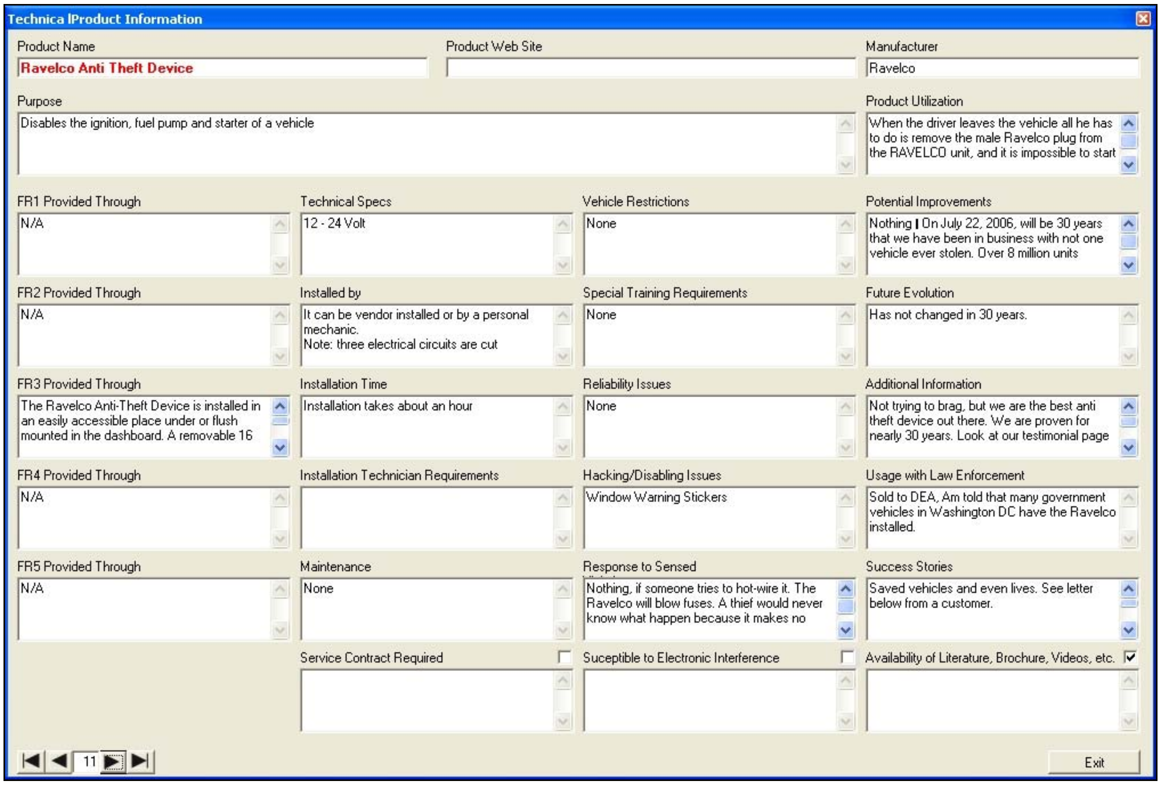
We have installed a system on our 2006 3/4 ton truck.

Company Will Demo in Own Testing Lab ☑

Company Willing to Lend Prod to ORNL ☑

Willing to Introduce ORNL to Customers ☑

Figure 64. VIT Product General Information



Product Name
Ravelco Anti Theft Device

Product Web Site

Manufacturer
Ravelco

Purpose
Disables the ignition, fuel pump and starter of a vehicle

Product Utilization
When the driver leaves the vehicle all he has to do is remove the male Ravelco plug from the RAVELCO unit, and it is impossible to start

FR1 Provided Through
N/A

Technical Specs
12 - 24 Volt

Vehicle Restrictions
None

Potential Improvements
Nothing | On July 22, 2006, will be 30 years that we have been in business with not one vehicle ever stolen. Over 8 million units

FR2 Provided Through
N/A

Installed by
It can be vendor installed or by a personal mechanic.
Note: three electrical circuits are cut

Special Training Requirements
None

Future Evolution
Has not changed in 30 years.

FR3 Provided Through
The Ravelco Anti-Theft Device is installed in an easily accessible place under or flush mounted in the dashboard. A removable 16

Installation Time
Installation takes about an hour

Reliability Issues
None

Additional Information
Not trying to brag, but we are the best anti theft device out there. We are proven for nearly 30 years. Look at our testimonial page

FR4 Provided Through
N/A

Installation Technician Requirements

Hacking/Disabling Issues
Window Warning Stickers

Usage with Law Enforcement
Sold to DEA, Am told that many government vehicles in Washington DC have the Ravelco installed.

FR5 Provided Through
N/A

Maintenance
None

Response to Sensed
Nothing, if someone tries to hot-wire it. The Ravelco will blow fuses. A thief would never know what happen because it makes no

Success Stories
Saved vehicles and even lives. See letter below from a customer.

Service Contract Required ☐

Suceptible to Electronic Interference ☐

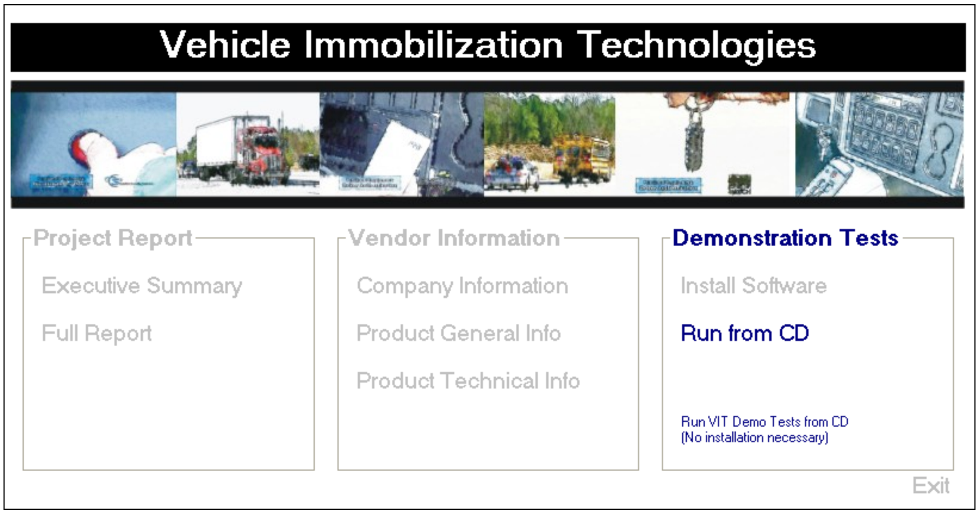
Availability of Literature, Brochure, Videos, etc. ☑

Figure 65. VIT Product Technical Information

D.3 DEMONSTRATION TESTS SOFTWARE INTERFACE DESCRIPTION

The main screen (Figure 61) also allows the user to access the information collected during the demonstration tests. Two options are provided: to install the visualization software and run it from the user’s computer or run it directly from the CD. Each one of these options can be accessed as discussed in the previous sections.

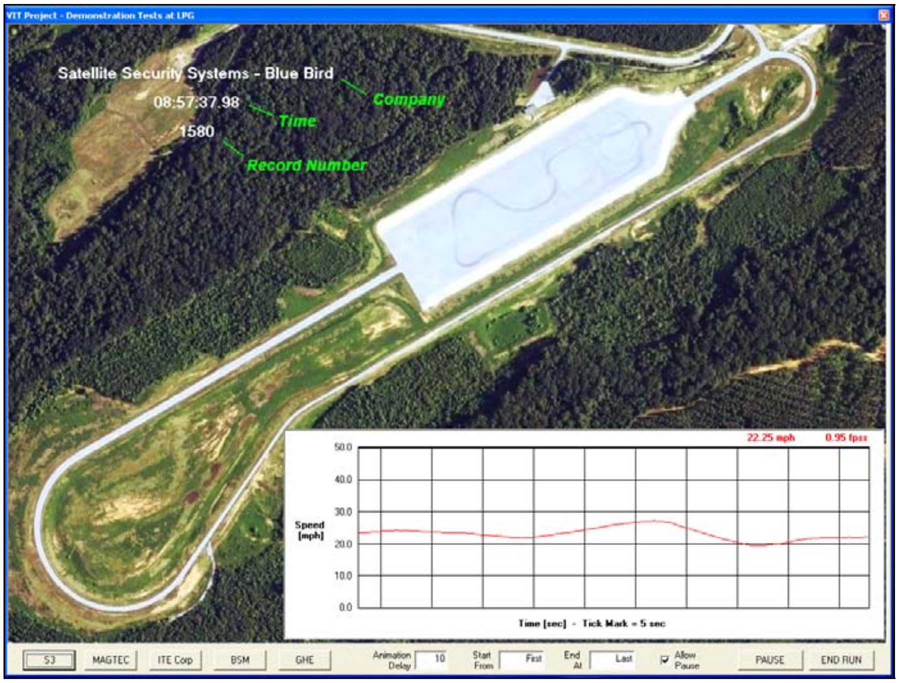
The visualization software allows the user to see the truck’s location on the track, the current time, the vehicle’s speed, and the record number currently being analyzed. The interface consists of three main elements: a map of the test track, a graph displaying vehicle speed, and a control tool bar. To load this interface directly from the CD, the user clicks on the “Run from CD” option (highlighted in Figure 66), and a window, similar to that shown in Figure 67, is immediately displayed.



Run VIT Demo Tests from CD
(No installation necessary)

Figure 66. Running the Demonstration Tests Visualization Software from the CD

The Map: The map portion of the interface (i.e., the background) is simply an aerial photograph of the test track that was used for the testing at Laurens Proving Grounds in South Carolina (Figure 67). When the software is run, a red dot representing the selected truck will appear and travel around the track indicating the truck's position. At the same time, in the upper-left corner, the name of the vendor is shown together with a clock that displays the current time as the vehicle moves and a counter showing the data record id.



Satellite Security Systems - Blue Bird
08:57:37.98
1580

Animation Delay 10
Start From First
End At Last
☑ Allow Pause

Figure 67. Interface Background

Speed Profile Graph: The lower right-hand corner of the interface contains a graph that displays the current speed of the vehicle (Figure 68). When a simulation is in progress, the current speed of the vehicle is plotted versus time (i.e., a speed profile). The window always displays 50 seconds worth of speed data and scrolls from left to right to allow the user to always see the current speed of the vehicle as well as a portion of the speed history. The graph also contains a digital readout of the current speed in miles-per-hour (mph) and linear acceleration in feet-per-second-squared (fpss) in the upper right-hand corner.

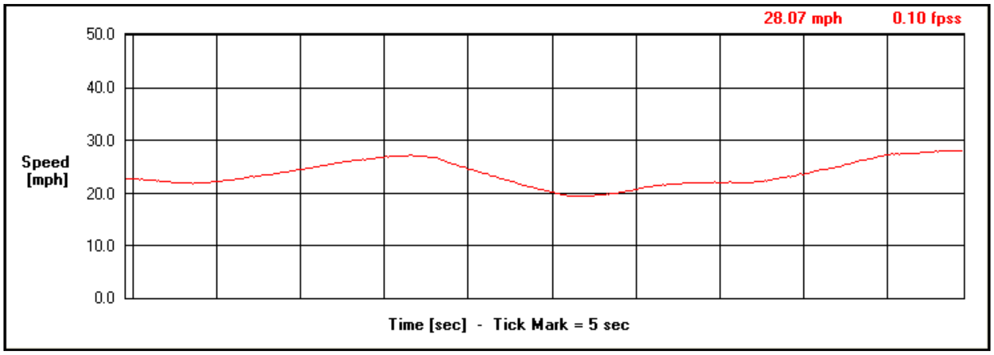
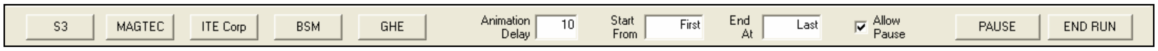


Figure 68. Speed Profile Graph

The Tool Bar: The tool bar at the bottom of the window provides the user a set of controls to manipulate the displaying of the demonstration tests information (Figure 69).



Animation Delay 10

Start From First

End At Last

☑ Allow Pause

Figure 69. Control Tool Bar

There are five buttons on the left side that represent the nine corporations (including six VIT providers, two companies using vehicle immobilization technologies, and a GPS tracking provider) that demonstrated VIT devices:

1. "S3"—Satellite Security Systems and Blue Bird Body Co.
2. "MAGTEC"—MAGTEC, Qualcomm, and Celadon Trucking
3. "ITE Corp"—International Truck and Engine Corporation
4. "BSM"—BSM Wireless Inc.
5. "GHE"—GlenHugh Enterprise and ARCHETYPE

Clicking a company's button will start the simulation for one of their truck runs.

To the right of these are three text boxes. The first, titled "Animation Delay," allows the user to modify how fast the displaying of the data runs. Smaller numbers mean less delay and thus the animation runs faster; similarly, higher numbers correspond to more delay and thus cause slower animations. Note that any delay time change must be followed by clicking the "Pause" button and then clicking "Continue" for the change to take effect.

The next two text boxes are titled “Start From” and “End At”; these control at what record numbers a simulation begins and stops. These boxes can either be populated with any positive number, or the words “First” (representing the first record number) or “Last” (representing the last record number). The “Start From” box can also be populated with a number that is higher than the “End At” number, in which the case the animation will run backwards between these two record numbers. Note that an animation run must be ended and then restarted for changes in these text boxes to take effect; pausing and continuing will not recognize them.

There are two buttons at the right of the tool bar that are labeled “Pause” and “End Run.” The pause button only has an effect when an animation is in progress and will stop the animation without resetting it. The button text then changes to “Continue” and pressing it again will cause the animation to resume from where it was paused. The “End Run” button also stops the animation, but it resets the program so that a new truck run must be selected to resume viewing animations and it will start from the beginning of the run (or whatever record number is entered into the “Start From” box).

There is a check box labeled “Allow Pause” to the left of the pause button that enables or disables pausing or stopping a run once it has been started. This feature has been included because it increases the maximum animation speed by allowing the program to only process the run and not poll for user input. When the check box is unchecked, the “Pause/Continue” and “End Run” buttons will both be disabled. Note that once a run has been started in this mode, attempting to click on another control (such as a different company name) before the run has completed could cause the program to freeze. Thus, it is important to allow the simulation to completely finish before attempting to issue any other command.

Finally, there is one control that is not listed on the tool bar at the bottom of the screen; double-clicking anywhere on the map will resize the interface to accommodate different monitor resolutions. There are two sizes and repeated double-clicking will toggle between the two (Figure 70).

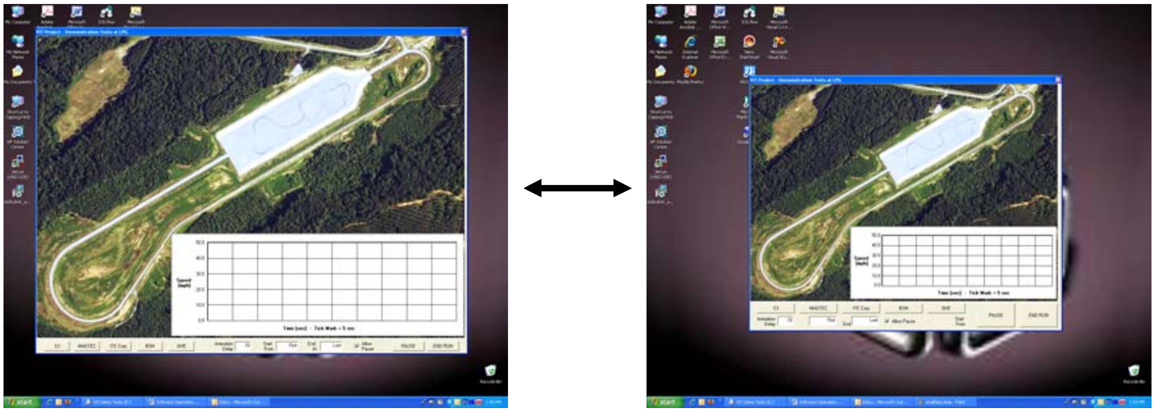


Figure 70. Resizing Interface Window

APPENDIX E:
VIT STAKEHOLDERS LIST

E.1 BACKGROUND

The following table (Table 14) includes contact information for all the stakeholders with whom the research team interacted for this project. The columns to the left of each name show the type of interaction of that person with the project, with CVSA W indicating participation in the CVSA Workshop; IW participation in the industry-focused webinar; LEW, law enforcement webinar; D, direct contact; DT, demonstration tests; Q, vendors' questionnaire; and V, personal visits. The table also show contact information for the research team (RT).

Table 14. VIT Stakeholders List and Contact Information

CVSA Interaction	Contact Information	CVSA Interaction	Contact Information
Q	**Lew Arcari** AirIQ Inc. 1099 Kingston Road, Suite 233 Pickering, ON L1V 1B5 Canada Ph: 905-831-6444 Fx: 905-831-0567 E-mail: larcari@airiq.com www.airiq.com	CVSA SW	**Jerry Baker** HazMat Training Coordinator Missouri State Highway Patrol 1510 E. Elm St. Jefferson City, MO 65101 Ph: (573) 526-6128 ext. Fx: (573) 526-4637 E-mail: cindy.martin@mshp.dps.mo.gov
D	**Jim Balestra** Safefreight Technologies, Inc. 8000 N.E. Parkway Drive, Suite 200 Vancouver, WA 98662 Ph: 360-944-6722 Fx: 360-253-6424 E-mail: jbalestra@safefreight.com www.safefreight.com	IW	**Thomas Ballard** NAM Driving Special Projects Schlumberger 200 Gillingham Ln. Sugar Land, TX 77478 Ph: (281) 285-7606 ext. Fx: (281) 285-8526 E-mail: ballards@slb.com
D	**Ed Bass** First Horizon National Corporation 165 Madison Memphis, Tennessee 38103 Ph: 630-294-4337 E-mail: ebass@firsthorizonins.com	V	**Mark Bauckman** Director, Business Development Qualcomm 5775 Morehouse Dr. San Diego, CA 92121 Ph: 619-517-7295 E-mail: mbauckman@qualcomm.com www.qualcomm.com
D	**David Beasley** Master Sergeant Illinois State Police, Commercial Vehicle Section 500 Iles Park Place, Suite 400 Springfield, IL 62703 Ph: 217-558-4060 Fx: 217-524-2391 E-mail: David_Beasley@isp.state.il.us	Q, D	**Stephen A. Belyea** Base Engineering Inc. 600 Rothesay Ave. Saint John, New Brunsw E2H 2H1 Canada Ph: 800-924-1010 E-mail: s.belyea@baseng.com www.baseng.com

CVSA Interaction	Contact Information	CVSA Interaction	Contact Information
RT	**Capt Steve Binkley** Tennessee Highway Patrol Tennessee Department of Safety 1148 Foster Avenue Nashville, Tennessee 37210 Ph: 615-687-2317 E-mail: Steve.Binkley@state.tn.us	**IW**	**Paul Black** PO Box 5010, 825 Highway 33 Freehold, NJ 07728 Ph: 732-462-1001 E-mail: pblack@freeholdcartage.com
V, DT	**Michael Bray** Business Development Mgr. Qualcomm 5775 Morehouse Dr. San Diego, CA 92121 Ph: 858-651-6241 Fx: 858-651-3740 E-mail: mbray@qualcomm.com www.qualcomm.com	**CVSA SW**	**Bruce Bugg** Captain Georgia Department of Public Safety 959 E. Confederate Ave. Atlanta, GA 30316 Ph: (404) 624-7226 ext. Fx: (404) 624-7295 E-mail: obbugg@gsp.net
CVSA SW	**Reggie Bunner** Supervisor Public Service Commission of West Virginia P. O. Box 812 Charleston, WV 25323 Ph: (304) 340-0322 ext. Fx: (304) 340-3742 E-mail: crandolph@psc.state.wv.us	**IW**	**Jerry Bunning** Fleet Safety Manager RSC Equipment Rental 215 E. Baseline Road Gilbert, AZ 85234 Ph: 602-448-7690 E-mail: Jerry.Bunning@RSCrental.com http://www.RSCrental.com
IW	**Michael A. Caldarera, P.E.** Vice President, Regulatory and Technical Services National Propane Gas Association 1150 17th Street NW, Suite 310 Washington, D.C. 20036 Ph: 202-466-7200, ext. 223 E-mail: mcaldarera@npga.org	**CVSA SW**	**Kenneth Carr** Major Florida DOT, Motor Carrier Compliance 325 John Knox Rd., Bldg. K Tallahassee, FL 32303 Ph: (850) 245-7900 ext. E-mail: kenneth.carr@dot.state.fl.us
V	**Eric Chapman** President Satellite Security Systems Inc. 6779 Mesa Ridge Road, Suite 100 San Diego, CA 92121 Ph: 858-638-9700 E-mail: echapman@satsecurity.com www.satsecurity.com	**CVSA SW**	**Rose Clark** Section Head Maryland Department of Environment 1800 Washington Blvd. Baltimore, MD 21230 Ph: (410) 537-3400 ext. Fx: (410) 537-3017 E-mail: rclark@mde.state.md.us
D	**John Conley** President National Tank Truck Carriers, Inc 2200 Mill Rd. Alexandria, VA 22314 Ph: 703-838-1960 E-mail: jconley@Tanktruck.org	**IW**	**Richard Craig** Director of Regulatory Affairs OOIDA P.O. Box 1000 Grain Valley, MO 64029 Ph: (816) 229-5791 ext.1603 Fx: (816) 427-4468 E-mail: denise_volmer@ooida.com

CVSA Interaction	Contact Information	CVSA Interaction	Contact Information
Q	**Chris Crowle** Director Prod.Dev. Safefreight Technologies, Inc. 4220 98 Street, Suite 303 Edmonton, Alberta, T6E 6A1 Canada Ph: 780-421-9055 232 Fx: 780-421-9011 E-mail: ccrowle@safefreight.com www.safefreight.com	**CVSA SW**	**Gary Davenport, CDS** Director of Safety & Risk Management Kansas Motor Carriers Association P.O. Box 1673 Topeka, KS 66601 Ph: (785) 267-1641 ext.102 Fx: (785) 266-6551 E-mail: gary@kmca.org
IW	**Donald Davis** SPILL CENTER 22 Kane Industrial Dr. Hudson, MA 01749 Ph: (978) 568-1922 x222 Fx: (978) 580-7416 cell E-mail: ddavis@spillcenter.com	**IW**	**Joe Delfino** Security Manager Trans Bridge Lines, Inc. 2012 Industrial Drive Bethlehem, Pa. 18017 Ph: 610-868-6001 ext.163 Fx: 610-868-9057 fax E-mail: jdelfino_tbl@fast.net
RT	**Joseph DeLorenzo** HazMat Program Manager U.S. DOT/FMCSA 19900 Governors Dr., Ste. 210 Olympia Fields, IL 60461 Ph: (708) 283-3572 ext. Fx: (708) 283-3579 E-mail: joseph.delorenzo@dot.gov	**IW**	**William F. Downey** Vice President - Security Kenan Advantage Group 4895 Dressler Road Canton, Ohio 44718 Ph: 800-969-5419 E-mail: bdowney@thekag.com www.thekag.com
Q	**Christopher Farmer** Sr Account Executive Vericom 9881 Broken Land Pky. Columbia, MD 21046 Ph: 410-381-5707x36 Fx: 410-381-2997 E-mail: cfarmer@vericomtech.com www.vericomtech.com	**CVSA SW**	**David Feather** Sgt. Virginia State Police P.O. Box 27472 Richmond, VA 23261 Ph: (804) 674-2005 ext. Fx: (804) 674-2916 E-mail: herbert.bridges@vsp.virginia.gov
Q, D	**Jake Fifelski** President AutoMotive Wireless Incorporated P.O. Box 172 Dorr, MI 49323 Ph: 616-308-3960 E-mail: j.fifelski@automotivewireless.com www.automotivewireless.com	**CVSA SW**	**Michael Filiaggi** Program Manager Transportation Security Administration 601 S. 12th St. Arlington, VA 22202 Ph: (571) 227-4262 ext. Fx: (571) 227-2935 E-mail: michael.filiaggi@dhs.gov
IW	**Jack Foley** Director, Regulatory Compliance P. S. MARSTON ASSOCIATES 38B South Road North Hampton, NH 03862 Ph: 800-643-9537 ext. 17 Fx: 603-964-8269 (fax) E-mail: jack@abenaquicarriers.com	**RT**	**Oscar Franzese** Sr. Researcher Oak Ridge National Laboratories 2360 Cherahala Blvd. Knoxville, TN 37932 Ph: (865) 946-1304 E-mail: franzeseo@ornl.gov

CVSA Interaction	Contact Information	CVSA Interaction	Contact Information
CVSA SW	**Sgt. Thomas Fuller** New York State Police 1220 Washington Ave. Bldg. 22 Albany, NY 12226 Ph: (518) 457-3258 ext. Fx: (518) 457-9620 E-mail: rweiss@troopers.state.ny.us	**D**	**Winston Gaffron** Director, TN DOT Region 3 6601 Centennial Blvd. Nashville, TN 37243-0360 Ph: 615-350-4300 Fx: 615-350-4396 Winston.Gaffron@state.tn.us
Q, D, DT	**Sherwin Gilbert** Business Development Manager International Truck and Engine Corporation 4201 Winfield Rd Warrenville, IL 60555 Ph: 630-753-6153 Fx: 630-753-3000 E-mail: Sherwin.Gilbert@NAV-INTERNATIONAL.com www.internationaldelivers.com	**IW**	**Dale Goetz** Director - Safety & Environmental Services YRC Worldwide 10990 Roe Ave. Overland Park , KS 66211 Ph: (913) 344-5375 ext. Fx: (913) 344-3614 E-mail: dale.goetz@yellowcorp.com
LEW	**Sgt. Alan Hageman** Oregon State Police - GHQ/PSD 255 Capitol St NE Salem, OR 97310 Ph: 503-378-3725 ext. 4201 E-mail: alan.hageman@state.or.us	**V**	**Jeff Hall** Field Engineer, Sr. Qualcomm 5775 Morehouse Dr. San Diego, CA 92121 Ph: 619-517-7295 E-mail: jhall@qualcomm.com www.qualcomm.com
V	**John Harvey** Engineer, Sr. Staff Qualcomm 5775 Morehouse Dr. San Diego, CA 92121 Ph: 619-517-7295 E-mail: jharvey@qualcomm.com www.qualcomm.com www.tandet.com	**IW**	**Dave Herdman** Safety/ Training Supervisor 1006 Prescott Drive Sarnia, ON N7T 7H3, Canada Tandet Logistics Inc. Ph: 519-332-6000 ext. 2111 Fx: 519-332-5986 E-mail: dherdman@tandet.com www.tandet.com
IW	**Bill Hershey** PGT Trucking Inc One PGT Way Monaca, PA 15061 Ph: 724-987-1715 E-mail: BHershey@pgttrucking.com	**Q, D**	**Erik Hoffer** President CGM Security Solutions, Inc 24156 Yacht Club Blvd Punta Gorda, FL 33955 Ph: 941-575 0243 Fx: 941-575 0971 E-mail: tamperguru@comcast.net www.airbrakesecurity.com
CVSA SW	**Dean House** Captain Iowa DOT/Motor Vehicle Enforcement Park Fair Mall, 100 Euclid Ave. Des Moines, IA 50313 Ph: (515) 237-3278 ext. Fx: (515) 237-3387 E-mail: dean.house@dot.iowa.gov	**LEW**	**Ron Hughes** Research Support NC State Highway Patrol 7760 Netherlands Dr. Raleigh, NC 27606 Ph: (919) 515-8523 ext. E-mail: rghughes@ncshp.org

CVSA Interaction	Contact Information	CVSA Interaction	Contact Information
V	**Patricia Hurst-Alger** Lawrence Livermore National Laboratory 7000 East Avenue Livermore, CA 94550 Ph: 925-422-0246 Fx: 925-423-0411 E-mail: hurstalger1@llnl.gov www.llnl.gov	LEW	**Dennis Hult** Chief, MCS Operations Bureau Montana DOT P.O. Box 4639 Helena, MT 59604-1001 Ph: (406) 444-9237 ext. Fx: (406) 444-9263 E-mail: dhult@mt.gov
CVSA SW	**Thomas B. Jacobs** L/Cpl. SCDPS - State Transport Police Division 10311 Wilson Blvd. Blythewood, SC 29016 Ph: (803) 896-5500 ext. Fx: (803) 896-5526 E-mail: tbjacobs@scstp.org	V	**Larry Jones** Trackn/Aircept 27758 Santa Margarita Pkwy, Suite 363 Mission Viejo CA, 92691 Ph: 877-684-2040 Fx: 949-260-0889 www.aircept.com
IW	**Patrick Kaigle** National Transportation Manager Air Liquide Canada Inc. - Process Industries 1250 Rene-Levesque Blvd. West, Suite 1700 Montreal, Quebec H3B 5E6 Ph: 514-846-3917 phone Fx: 514-846-3915 fax E-mail: patrick.kaigle@airliquide.com	V, D	**Doug Kenner** Operations Manager Swain Oil Transport P.O. Box 131567 Carlsbad, CA 92013 Ph: 760-607-0242 (Office) E-mail: Doug@swainoiltrans.com www.swainoiltrans.com
V, D, DT	**Tom King** VP Product Development Satellite Security Systems Inc. 6779 Mesa Ridge Road, Suite 100 San Diego, CA 92121 Ph: 858-638-9700 E-mail: tking@satsecurity.com www.satsecurity.com	CVSA SW	**Jim Kitchen** Load Engineering Manager Schneider National Carriers P.O. Box 2417 Green Bay, WI 54306 Ph: (920) 592-6248 Fx: (920) 592-6169 E-mail: kitchenj@schneider.com
RT	**Helmut Knee** Group Leader Oak Ridge National Laboratory 2360 Cherahala Blvd. Knoxville, TN 37932 Ph: (865) 946-1300 Fx: (865) 946-1314 E-mail: kneehe@ornl.gov	CVSA SW	**Mark Lepofsky** Manager, Transportation Analysis & Risk Assessment Battelle Memorial Institute 901 D St, SW, Ste. 900 Washington, DC 20024-2115 Ph: (202) 646-7786 ext. Fx: (614) 458-6656 E-mail: lepofskym@battelle.org
V	**Pat Lewis** Lawrence Livermore National Laboratory 7000 East Avenue Livermore, CA 94550 Ph: 925-422-0042 E-mail: lewis26@llnl.gov www.llnl.gov	IW	**Tom Lynch** Vice President The National Tank Truck Carriers, Inc. 2200 Mill Road Alexandria, VA 22314 Ph: 703-838-1960 Fx: 703-684-5753 E-mail: tlynch@tanktruck.org

CVSA Interaction	Contact Information	CVSA Interaction	Contact Information
Q, D, DT	**David McMillan** Manager of Product Development MAGTEC Products, Inc 9152 - 52nd Street SE Calgary, Alberta T2C 5A9 Canada Ph: 403-215-0748 E-mail: dmcmillan@magtecproducts.com www.magtecproducts.com	**V**	**Al Milligan** Executive Vice President Wireless Matrix 12369-B Sunrise Valley Drive Reston, VA 20191 Ph (703) 262-0500 Fax (703) 262-0380 www.wirelessmatrixcorp.com
D	**Jim Moberg** Vice President Sales Blue Bird Body Company 402 Blue Bird Boulevard Fort Valley, GA 31030 Ph: 478-822-2239	**Q, D**	**Bob Morisset** President MAGTEC Products, Inc 9152 - 52nd Street SE Calgary, Alberta T2C 5A9, Canada Ph: 403-252-2169 E-mail: rmorisset@magtecproducts.com www.magtecproducts.com
CVSA SW **IW** **DT**	**M. R. (Mitch) Morisset** Manager, Field Operations MAGTEC 9152 - 52nd Street SE Calgary, Alberta T2C 5A9 Canada Ph: 403-252-2169 E-mail: mmorisset@magtecproducts.com	**CVSA SW**	**Douglas Morris** Commander Maryland State Police 901 Elkridge Landing Rd., Ste. 300 Linthicum, MD 21090 Ph: (410) 694-6100 ext. Fx: (410) 694-6135 E-mail: cved@mdsp.org
Q, V, DT	**Hugh Morris** GlenHugh Enterprise 19 Muir Crescent Alma, ON N0B 1A0 Canada Ph: 519-846-8941 Fx: 519-846-2870 E-mail: h_autowatch@highspeedfx.net www.autowatchamerica.com	**IW**	**Thomas Moses** President SPILL CENTER 22 Kane Industrial Drive Hudson, MA 01749 Ph: 978-568-1922 x222 Fx: 978-580-7416 cell E-mail: tmoses@spillcenter.com
IW	**Richard Moskowitz** Assistant General Counsel and Regulatory Affairs Counsel American Trucking Associations 2200 Mill Road Alexandria, Va. 22314 Ph: 703-838-1910 E-mail: RMoskowitz@trucking.org	**CVSA SW**	**Steven Niswander** VP, Safety & Regulatory Relations Groendyke Transport Inc P.O. Box 632 Enid, OK 73702 Ph: (580) 213-9237 ext. Fx: (580) 234-2150 E-mail: sniswander@groendyke.com
CVSA SW	**David O'Neal** Safety Coordinator Martin Transport, Inc. 4200 Stone Rd. Kilgore, TX 75663 Ph: (903) 812-1069 ext. Fx: (903) 981-3199 E-mail: david.oneal@martinmlp.com	**CVSA SW**	**Ron Ostler** Captain Utah Highway Patrol 5500 W. Amelia Earhart Dr., Ste. 360 Salt Lake City, UT 84116 Ph: (801) 596-9248 ext. Fx: (801) 596-9751 E-mail: rostler@utah.gov

CVSA Interaction	Contact Information	CVSA Interaction	Contact Information
Q, D	**Mark Ochitwa** Vice President, Operations and Product Development MAGTEC Products, Inc 9152 - 52nd Street SE Calgary, Alberta T2C 5A9 Canada Ph: 403-215-0748 E-mail: mochitwa@magtecproducts.com www.magtecproducts.com	**CVSA SW**	**Wes Pace** Director, Hazmat & Trade Compliance Landstar Carrier Services 13410 Sutton Park Jacksonville, FL 32224 Ph: (904) 306-2372 ext.2372 Fx: (904) 306-2668
Q, D, DT	**Chris Panczuk** BSM Wireless Inc 5875 Highway 7, Suite 200 Woodbridge, Ontario L4L 1T9 Canada Ph: 905-265-1200 (266) Fx: 905-265-1288 E-mail: cpanczuk@bsmwireless.com www.bsmwireless.com	**D**	**Michael Paton** Skywave Sales Manager 1145 Innovation Drive, Suite 288 Ottawa, ON K2K 3G8, Canada Ph: 613-836-6288 ext 234 Fx: 613-836-1088 E-mail: michael.paton@skywave.com www.skywave.com
CVSA SW	**Rob Patrick** Captain California Highway Patrol 444 N. 3rd St., #310 Sacramento, CA 95814 Ph: (916) 445-1865 ext. Fx: (916) 446-4579 E-mail: RPatrick@chp.ca.gov	**CVSA SW**	**Bob Powers** Captain Michigan State Police 4000 Collins Rd. Lansing, MI 48910 Ph: (517) 336-6447 Fx: (517) 333-4414 E-mail: powersr@michigan.gov
CVSA SW	**Joseph Rajkovacz** Regulatory Affairs Specialist OOIDA P.O. Box 1000 Grain Valley, MO 64014 Ph: (816) 229-5791 ext.1680 Fx: (816) 427-4468 E-mail: denise_volmer@ooida.com	**Q**	**Vincent Raviele** President Ravelco 6920 Oak Knoll Drive Richmond, TX 77469 Ph: 281-341-6222 E-mail: ravelco@aol.com www.ravelco.com
CVSA SW	**Michael Ritchie** Hazardous Materials Specialist Minnesota DOT 395 John Ireland Blvd. St. Paul, MN 55155 Ph: (651) 366-3697 ext. Fx: (651) 366-3719 E-mail: michael.ritchie@dot.state.mn.us	**RT**	**Lt Ray Robinson** Tennessee Highway Patrol Tennessee Department of Safety 1148 Foster Avenue Nashville, Tennessee 37210 United States of America Ph: (615) 687-2304 E-mail: Ray.Robinson@state.tn.us
IW	**Drew Schimelpfenig** Ops Contact Center Mgr. J B Hunt Corp 300 Delaware Avenue Wilmington, DE 19801-1607 Ph: 479.820.6676 E-mail: Drew_Schimelpfenig@jbhunt.com	**Q, V**	**Marvin Serhan** Vice President of Business Development Satellite Security Systems Inc. 6779 Mesa Ridge Road, Suite 100 San Diego, CA 92121 Ph: 858-638-9700 E-mail: mserhan@satsecurity.com www.satsecurity.com

CVSA Interaction	Contact Information	CVSA Interaction	Contact Information
IW	**Kirk Shrader** Manager of Safety Services Trimac Transporation Inc 3663 N. Sam Houston Parkway E. Houston, Texas 77032 Ph: 918-439-4642 Fx: 918-439-4760 E-mail: kshrader@trimac.com	Q	**Barry Smith** GPS Management Systems 480 Northfield Drive, Suite 500 Brownsburg, IN 46112 Ph: 317-852-5229 E-mail: bsmith@gpsmanagement.com www.gpsmanagement.com
CVSA SW	**Carlisle J Smith** Hazardous Materials Supervisor Public Utilities Commission Ohio 180 E. Broad St., 14th Fl. Columbus, OH 43215-3793 Ph: (614) 728-9126 ext. Fx: (614) 752-8349 E-mail: Carlisle.Smith@puc.state.oh.us	CVSA SW	**Forrest Smith** Col. NM Department of Public Safety P.O. Box 1628 Santa Fe, NM 87504 Ph: (505) 827-0148 ext. Fx: (505) 827-0324 E-mail: forrest.smith@state.nm.us
CVSA SW	**Joseph Smith** Sgt. DPS/Nevada Highway Patrol 555 Wright Way Carson City, NV 89711 Ph: (702) 432-5121 ext. Fx: (702) 486-4143 E-mail: tshaw@dps.state.nv.us	CVSA SW	**Thomas Snyder** Safety and Compliance Austin Powder Company 11910 V.O. Dr. Poseyville, IN 47633 Ph: (812) 963-9293 ext. Fx: (216) 464-4418 E-mail: tom.snyder@austinpowder.com
CVSA SW	**Rion Stann** Motor Carrier Enforcement Supervisor Pennsylvania State Police 20th and Herr Streets Harrisburg, PA 17120 Ph: (717) 346-7350 ext. E-mail: rstann@state.pa.us	CVSA SW	**Daniel Stock** Sr. Transportation Specialist SAIC 5 Mitchell Ave. Wakefield, RI 02879 Ph: (401) 792-8175 ext. Fx: (401) 792-8176 E-mail: stockd@saic.com
Q, V	**James Tatoian** President Eureka Aerospace 3452 E. Foothill Blvd, Suite 528 Pasadena, CA 91107 Ph: 626-844-6664 Fx: 626-844-6665 E-mail: tatoian@eurekaaerospace.com www.eurekaaerospace.com	LEW	**Sergeant Doug Taylor** Tennessee Highway Patrol Research, Planning, and Development Ph: 615-687-2400 Fx: 615-253-2096 E-mail: Doug.Taylor@state.tn.us
D, DT	**Gregg Tilston** Fleet and Data Solutions Specialist - Government Sector BSM Wireless 5875 Hwy 7., Suite 200 Woodbridge, ON L4L 1T9, Canada Ph: 905-265-1200 x255 E-mail: gtilston@bsmwireless.com www.bsmwireless.com	RT	**Tom Urbanik** Professor University of Tennessee 219-B Perkins Knoxville, TN 37996 Ph: (865) 974-7709 Fx: (865) 974-2669 E-mail: turbanik@utk.edu

CVSA Interaction	Contact Information	CVSA Interaction	Contact Information
CVSA SW	**Brad Wagner** Sgt. Nebraska State Patrol 3920 W. Kearney St. Lincoln, NE 68524 Ph: (402) 471-0105 ext. Fx: (402) 471-3295 E-mail: bwagner@nsp.state.ne.us	**Q, V, D**	**Tom Wainwright** Vice President, Sales & Marketing Wireless Matrix (ex. MobileAria) 800 W El Camino Real Mountain View, CA 94040 Ph: 650-237-4455 E-mail: TWainwright@MobileAria.com www.wirelessmatrixcorp.com
V	**Jeff Waterstreet** Sr. Mgr, Business Development Qualcomm 5775 Morehouse Dr. San Diego, CA 92121 Ph: 619-517-7295 E-mail: jwaterstreet@qualcomm.com www.qualcomm.com	**V**	**Bill Wattenburg** Consultant Lawrence Livermore National Laboratory BillWattenburg2 @yahoo.com
IW	**Dave West** DOT Compliance Manager RSC Equipment Rental A Company within the Atlas Copco Group P.O. BOX 19 West Valley, NY 14171 USA Ph: 716-983-0140 E-mail: David.West@RSCrental.com	**CVSA SW**	**Mike Windsor** Sr. Manager - Hazardous Materials YRC Worldwide 10990 Roe Ave. Overland Park, KS 66211 Ph: (913) 344-3057 ext. Fx: (913) 344-3614 E-mail: mike.windsor@yellowcorp.com
D	**Bruce Wishart** Director of Security Celadon Trucking 9503 E.33rd Street Indianapolis, IN 46235-4207 (800) CELADON (317) 972-7000 www.celadontrucking.com	**V, D**	**Michael T. Yura** NBSP 150 Clay Street, Suite 350 Morgantown, WV 26501 Ph: 304-292-8800 Fx: 304-292-8803 E-mail: yura@nationalbiometric.org