HAZMAT SAFETY & SECURITY

FIELD OPERATIONAL TEST

TASK 2: EXECUTIVE SUMMARY

CONCEPT OF OPERATIONS

To

Federal Motor Carrier Safety Administration

U.S. Department of Transportation

Washington, DC 20590

In association with Qualcomm

American Transportation Research Institute (ATRI)

Commercial Vehicle Safety Alliance (CVSA)

March 21, 2003

Battelle
. . . Putting Technology To Work

Executive Summary

Following the September 11, 2001 terrorist attacks on the U.S., the Department of Transportation (DOT) was asked to identify areas within the transportation system that were vulnerable to terrorist attack. One major area of concern identified was the transportation of hazardous materials (hazmat). The Federal Motor Carrier Safety Administration is conducting a field operational test (FOT) to quantify the security costs and benefits of an operational concept that applies technology and improved enforcement procedures to hazmat transportation. The FOT will demonstrate an approach that enhances the safety and security of hazmat shipments from origin to destination.

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

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

- The technologies selected must account for the unique characteristics of each segment of the hazmat marketplace (long-haul, short-haul, pick up and delivery, etc.)
- The impact of using the technologies (cost, security) must be appropriate for the operational characteristics of the market segment. For example, munitions and explosives carriers are typically long-haul, for-hire carriers and already may be required to have communications and tracking capabilities. In contrast, the short-haul petroleum segment generally involves local fleets, working from a centralized dispatch and operating on thin profit margins and are not required to have the communications and tracking capabilities. Thus, technological solutions to the security issues must take into account the operating environment and the need to minimize the costs of the technological solutions.
- A goal to address all the functional requirements identified by DOT.

Technology Selection

One of the key aspects in the selection of the technologies to be tested as part of this FOT was the RFP requirement to utilize "…commercial-off-the-shelf technologies that can be implemented rapidly by the motor carrier industry." In essence, this FOT is not a technology development activity, rather an integration of existing technologies that can address the specific functional requirements laid out in the SOW. Table ES 1 lists the Battelle Team members providing technology solutions for the FOT.

Table ES 1: Battelle Team Technology Partners

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

Listed below are the major technological components included in the FOT and a brief description of the functionality of each component.

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

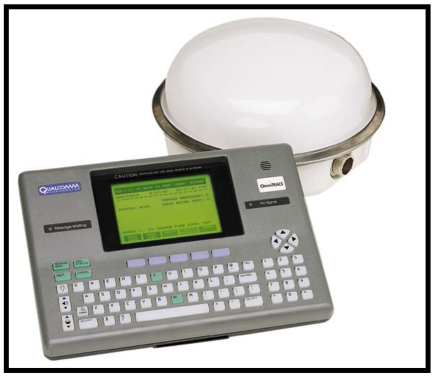

Figure ES-1: Wireless Satellite

Trucks will receive wireless tracking and communications systems, with integrated Global Positioning System (GPS) working in conjunction with the dispatch systems that provide for load/cargo positions and status. The system (Figure ES-1) will also include a Driver Interface Unit for two-way text communications. Positions are automatically displayed to the carrier's dispatcher at a regular frequency determined by the carrier.

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

Figure ES-2: Digital Phone

Digital Phone (wo/GPS)

This technology provides integrated work order assignment and status messaging between a carrier's dispatch and a driver using a low-cost digital cellular handset (Figure ES-2) with specialized operating software. Store-and-forward guaranteed messaging ensures message delivery upon returning to digital cellular coverage areas.

Along with messaging, ancillary services such as mapping and directions, for example, are also available.

Panic Buttons

The Panic Buttons will provide real-time emergency alert message notification by the driver to the dispatcher. An emergency alert message will be generated via the use of a panic button, which comes in two configurations:

a. A panic button mounted inside the vehicle to send an emergency alert (Figure ES-3).

b. A wireless panic button that can be carried by the driver to remotely send an emergency alert and/or use the remote panic button to disable the vehicle (Figure ES-4).

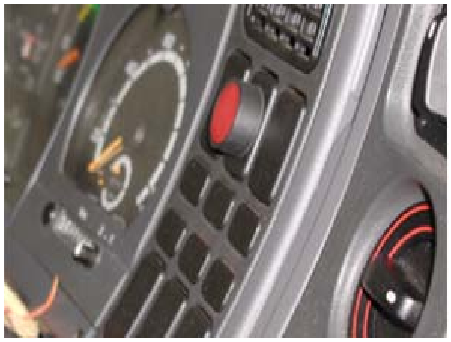

Figure ES-3: Dash Mounted Panic Button

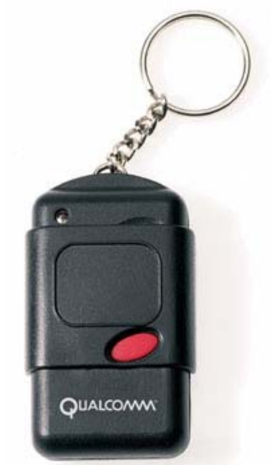

Figure ES-4: Wireless Panic Button

The functionality implemented with the panic buttons (either dash mounted or wireless) is configurable. Functions enabled by pressing the panic button can include:

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

Driver Authentication

Driver authentication is necessary to make sure the only authorized drivers are operating hazmat vehicles and picking up hazardous materials shipments. This FOT will test two separate technologies designed to authenticate drivers.

Driver Authentication with Global Login

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

Driver Authentication with Biometric Identification

This technology will require having a biometric verification unit (figure ES-5) on the vehicle. This will be a customized system designed to satisfy the environmental and usage characteristics required for installation in a trucking rig. The biometric system consists of a Central Processing Unit (CPU) with proprietary firmware which controls an attached smart card reader and fingerprint scanner, and which performs biometric verification. The biometric system will be customized to communicate with the on-board tracking and communications system.

Figure ES-5: Biometric Identification

Electronic Supply Chain Manifest (ESCM)

The ESCM system provides technologies that allow positive identification of the person responsible for the cargo and tracking capabilities for cargo movement within a hazardous materials shipment. Combining biometric verification, smart-cards, Internet applications and the on-board wireless communications, the system insures proper chain-of-control for the hazardous materials throughout the lifecycle of a hazardous materials shipment. It also provides visibility into the location and status of the shipment to the shipper, carrier and consignee, thus enhancing both security and customer service.

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

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

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

Intelligent Onboard Computers (OBC)

The OBC will be integrated with the wireless communications and vehicle operating systems to allow a variety of security related functions, based on configurable input. The OBC can be used to control the disabling of the vehicle in a variety of means. These methods include blocking fuel, or sending proprietary system instructions via the wireless communications system directly to the vehicle's data bus. The primary mode of disabling for this FOP will be retarding the vehicle into a limp mode where the vehicle still has electrical power but little throttle response past idle. The actual mode of shutdown will depend on the make, model, and year of the vehicle during installation. This unit will also be configured to shut the vehicle down if there is a loss of satellite signal strength (i.e., cut the feed cable). The driver also will be able to call the monitoring center and inform them that the vehicle needs to be disabled (in case of theft, for example). At that time the dispatcher could send an over-the-air command to disable the vehicle.

A cargo door lock (Figure ES-6) that requires the driver to request authorization from the carrier's dispatcher to lock or unlock the trailer door will also be demonstrated. This lock is a rugged unit that is bolted to the inside door of the trailer. Using over-the-air communications, a message requesting the doors to be unlocked/locked is sent to the dispatcher. The dispatcher then sends a message to the vehicle OBC device, which sends a command to the door, allowing the driver to unlock/lock the cargo door.

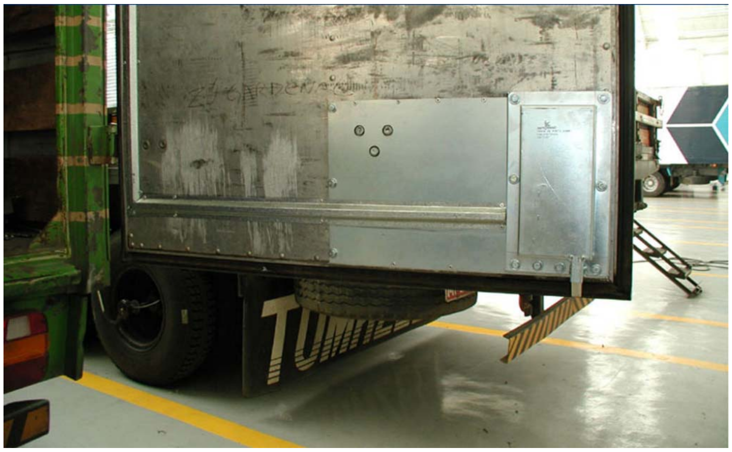

Figure ES-6: Cargo Locking

Electronic Cargo Seals

This technology includes a cargo E-seals (Figure ES-7) that automatically generates an alert if the seal is broken without proper authorization. The seal uses short-range wireless communications to interface with a mobile E-Seal reader (located in the vehicle). The mobile reader is interfaced to the on-board wireless communications device and the cargo "alerts" are forwarded automatically to the dispatcher. These alerts will include the date, time and location where the seal was breached.

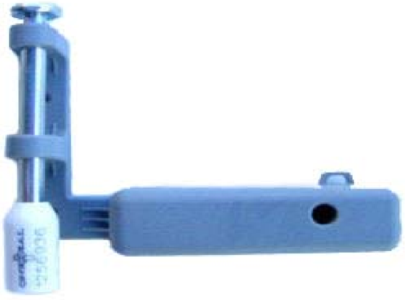

Figure ES-7: Smart Seal Tag

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

1. Dispatcher will send a message to alert the driver
2. The hand-held device will have a driver display
3. The system is integrated with the OBC and is hooked to a buzzer to alert the driver.

Routing and Geo-fenced Mapping Software

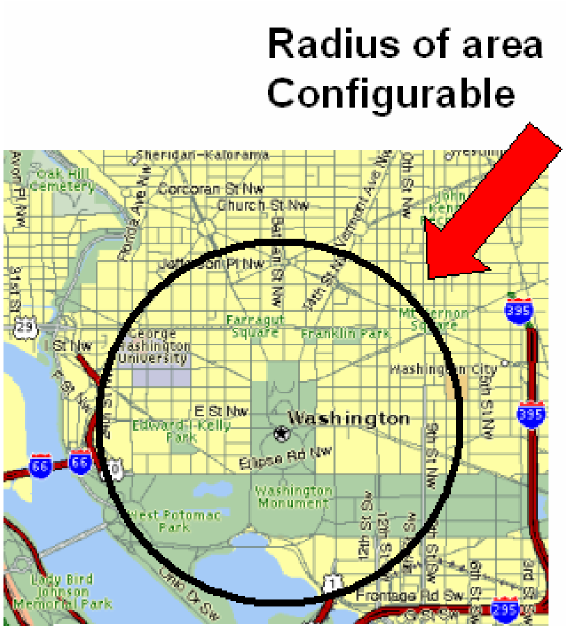
Radius of area Configurable

Figure ES-8: Geofencing

This technology will deploy specialized software that allows the operator to define a risk area or a route to monitor. An "electronic fence" is set around any given route or point on a displayable map.

The dispatcher can define a risk area (i.e., the White House) and if the vehicle enters the risk area or deviates from its route, an alert is sent to the carrier's dispatch center. A safe-haven can also be setup as a geo-fenced area and notifications can be configured if a vehicle leaves the area.

The geo-fencing capability interacts with frequent positioning and the on-board wireless communications system. If the geo-fence application has received a security breach, the system will automatically increase the positioning reports to a configurable time interval.

Untethered Trailer Tracking

The trailer tracking subsystem (Figure ES-9) provides trailer position information to the dispatcher on a regular basis.

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

Using the tethered device (Figure ES-10), connect and disconnect events are captured and transmitted as alerts to the dispatcher. This will notify the dispatcher that a trailer has been connected or disconnected from the tractor.

Figure ES-9: Trailer Tracking Subsystem

Figure ES-10: Tethered Device

Selecting the Technologies

It was recognized early on in the FOT that the unique operational characteristics of many of the hazardous materials carriers around the country would not lend to a full-scale deployment of all the technologies described above on every vehicle. While it may be prudent (and the market may bear the cost) to deploy more technologies on certain types of shipments (i.e., explosives), other carriers operate on thin profit margins and the marginal cost of deploying some of these technologies in their vehicles would be prohibitive. To represent these concerns of the market, the FOT team has separated the various technology components into six technology tiers, ranging from a low-end cost of approximately $250 per vehicle to a high-end of approximately $3,500 per vehicle. Table ES-2 provides a brief summary of each technology tiers.

Table ES-2: Technology Tiers

Tier (cost)	Description
1 ($250)	Include a digital cellular phone with pickup and delivery software with on-phone/on-board directions/mapping. This option would also include on site vehicle disabling with the wireless panic remote. This would not be able to send a panic message but would give the ability to shut it down remotely. This would not include positioning until position location is turned on to national networks.
2 ($800)	Includes terrestrial communications with in-dash panic button.
3 ($2,000)	Includes satellite communications with an in-dash panic button and Global Login.
4 ($2,500)	Includes all of what is in tier 3 but adds the additional OBC. The other variant includes satellite communications with an in-dash and wireless panic button with Biometric authorization, and E-manifest.
5 ($3,000)	Includes satellite communications with an in-dash and wireless panic button with Biometric authorization, E-manifest and an additional OBC. The other variant is swapping the OBC for an untethered trailer tracking device.
6 ($3,500)	Includes satellite communications with an in-dash and wireless panic button with Biometric authorization, E-manifest and E-Seals.

The price estimates by tier reflect only the hardware installed on the truck in commercial quantities. It does not reflect the price of servers and dispatch systems amortized over the number of vehicles since this can vary widely depending on customer set up. In addition, the price estimates reflect the cost of an initial install (assuming no technology previously installed on the truck).

Scenario Development

The final step in developing the concept of operations for the FOT was to match up each technology component with a testing scenario. The scenarios were developed to address the functional requirements in the FMCSA's RFP, the threats and vulnerabilities identified in the Task 1 Threat/Risk Assessment, and the selected technology components described above. The overall goal of the FOT was to test technologies installed in 100 vehicles. Each scenario will test a total of 25 vehicles, with various combinations of technology installed on each vehicle. In selecting the scenarios, attempts were made to match the shipment types – bulk, less than truckload (LTL), and truckload (TL) with specific hazardous commodities. Scenario 1 will involve the delivery of Class 2 Flammable Gas and Class 3 Flammable Liquids in the bulk delivery environment, Scenario 2 will involve the delivery of high hazards in the LTL environment, Scenario 3 will bulk chemical (Class 2.2 and Class 3 with inhalation hazard) delivery vehicles, and Scenario 4 will involve the truckload of Class 1.1 – 1.6 Explosives. Table ES-3 provides a summary of each scenario and the technology components to be tested by scenario.

Table ES-3: Technology Components by Scenario

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