Requirements Definition for ORNL Trusted Corridors Project

March 1, 2007

R. M. Walker
D. E. Hill
C. M. Smith
F. A. Denap
J. D. White
I. G. Gross
B. L. Gorman
L. M. Hively
R. K. Abercrombie

REQUIREMENTS DEFINITION FOR ORNL TRUSTED CORRIDORS PROJECT

R. M. Walker
D. E. Hill
C. M. Smith
F. A. Denap
J. D. White
I. G. Gross
B. L. Gorman
L. M. Hively
R. K. Abercrombie

March 1, 2007

CONTENTS

LIST OF FIGURES

ABSTRACT

The ORNL Trusted Corridors Project has several other names: SensorNet Transportation Pilot; Identification and Monitoring of Radiation (*in commerce*) Shipments (IMR(*ic*)S); and Southeastern Transportation Corridor Pilot (SETCP). The project involves acquisition and analysis of transportation data at two mobile and three fixed inspection stations in five states (Kentucky, Mississippi, South Carolina, Tennessee, and Washington DC). Collaborators include the State Police organizations that are responsible for highway safety, law enforcement, and incident response. The three states with fixed weigh-station deployments (KY, SC, TN) are interested in coordination of this effort for highway safety, law enforcement, and sorting/targeting/interdiction of potentially non-compliant vehicles/persons/cargo. The Domestic Nuclear Detection Office (DNDO) in the U.S. Department of Homeland Security (DHS) is interested in these deployments, as a Pilot test (SETCP) to identify Improvised Nuclear Devices (INDs) in highway transport. However, the level of DNDO integration among these state deployments is presently uncertain. Moreover, DHS issues are considered secondary by the states, which perceive this work as an opportunity to leverage these (new) dual-use technologies for state needs. In addition, present experience shows that radiation detectors alone cannot detect DHS-identified IND threats. Continued SETCP success depends on the level of integration of current state/local police operations with the new DHS task of detecting IND threats, in addition to emergency preparedness and homeland security. This document describes the enabling components for continued SETCP development and success, including: sensors and their use at existing deployments (Section 1); personnel training (Section 2); concept of operations (Section 3); knowledge discovery from the copious data (Section 4); smart data collection, integration and database development, advanced algorithms for multiple sensors, and network communications (Section 5); and harmonization of local, state, and Federal procedures and protocols (Section 6).

1. INTRODUCTION

Three high level requirements drive the ORNL transportation technology deployments for state police and DHS needs at the weigh stations in Tennessee (TN), South Carolina (SC) and Kentucky (KY). These requirements and their corresponding standards/sponsors are:

1. Compliance with the Code of Federal Regulations (CFR) for the Department of Transportation (DOT) 49 CFR highway safety regulations and State criminal/civil code and statues;

2. Event-driven data for requirement #1 (e.g., forensics and legal evidence), plus alarm-resolution data for the DHS S&T Data Integration Working Group for Advanced Algorithm development;

3. Data for technical reach-back to State Police as defined by the DHS DNDO Technical Reachback committee and industry spectroscopic experts.

1.1. COMPONENTS TO MEET HIGH-LEVEL REQUIREMENTS

Figure 1 shows the five components that must be addressed in order to meet the high- level requirements. Figure 1 also outlines the tasks for each component, along with the present status of each task (e.g., field testing today, notional but achievable, and goal under this effort). The key requirements are:
- Concept of operations;
- Knowledge discovery;
- Procedures and protocols;
- Human resource optimization and training;
- Communications.

This document discusses these components and the underlying tasks. Each of the five components is vital.

	Knowledge Discovery	Procedures Protocols and Policy	Con Ops Development Applications	Human Resource Optimization and Training	Communications
Field Testing Today	•Baseline Data Collection •Data Security •Data R&D •Data Transfer •Information Sharing	•State/Local Roles verses federal roles law enforcement •Legal issues •Key industry partners •Pilot procedures	•Corridor pilot test •Dual use application identification •GUI development •Alarm resolution •Commercial carrier and shipper participation •Infrastructure needs •Interdiction scenarios	•Training Program •Personnel training •Level of effort •Ongoing training •Training fusion •Scenario exercises	•Systems Architecture Definition •Information needed •Sensors available •Expertise needed •Equipment needs defined
Notional but Achievable	•Database mining •New database development •Advanced algorithm Development •Mobile data collection	•Industry participation •DOT, DHS, EPA, and NRC regulatory harmonization •Policy for regulatory development •Technology enablers that can be codified	•Mainline sorting •Tracking •Alignment with threat corridors •Deterrence •Surveillance	•Specialists at State/Local •Train the trainer State/Local •Mentoring	•Regional technical assistance •New Technology Beta Testing •Equipment standards •Automatically activated "Real-Time" access to mobile units
Goal	•National Automated/ Integrated Law Enforcement "BOLO" System *Be on the Lookout*	•Harmonized procedures and standards at Federal, State, and Local level	•Nationally supported standardized and institutionalized Program	•Standardized national training program for officer training	•National Deployment with virtually connected Regional Centers tied to Intel community

Figure 1. Key components for mission success.

1

For example, communications for fixed deployment are very different from mobile deployment (e.g., T1 line versus satellite). The legal requirements (procedures and protocols) are very different for interdiction of a personal occupancy vehicle (POV), versus interdiction of commercial motor vehicle (CMV) at a weigh station. Figure 2 items to be addressed as the multiple deployment strategies are implemented.

Figure 2. Detection and interdiction challenges.
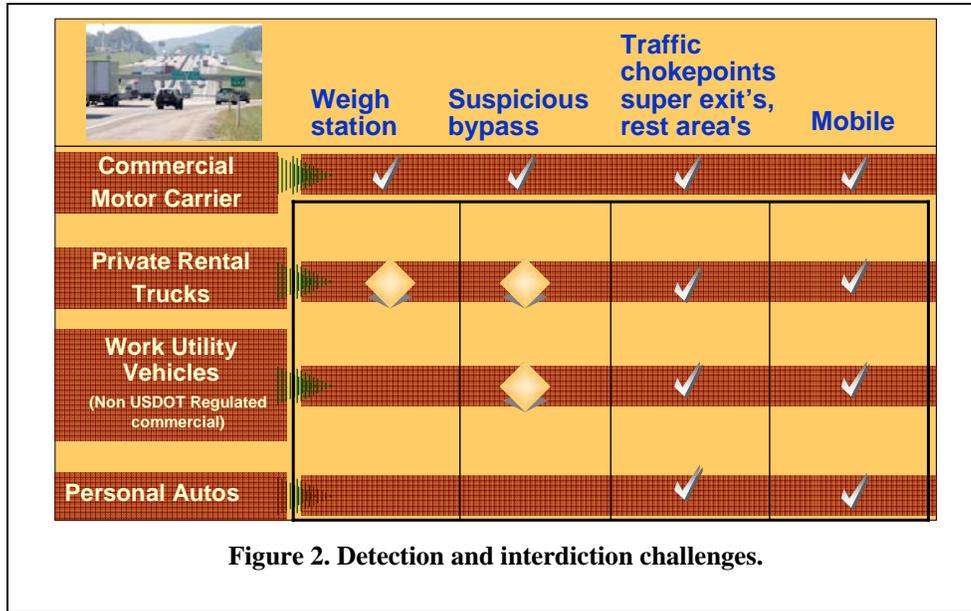
1.2. SENSORS DEPLOYED TO MEET HIGH LEVEL REQUIREMENTS

This work began in 2002 under an agreement between the U.S. Department of Energy (DOE) and the state of Tennessee. That agreement commissioned ORNL to study the use of radiation portal monitors (RPMs) in a weigh-station environment. One goal of this DOE-funded work is demonstration of bulk monitors to detect radiation where it ought not be. A second is enhancement of the weigh-station mission. ORNL deployed a radiation monitor (Exploranium AT 900, plastic scintillation for gamma detection) at the weigh station in Knox County, TN; this unit was subsequently upgraded to detect both gamma and neutron radiation. The Transportation Security Agency (TSA) also provided funding to deploy a Nucsafe RPM for gamma and neutron detection. ORNL's experience showed that the RPMs alone do not satisfy the goals for either Tennessee or DOE. Consequently, ORNL installed additional sensors to augment the RPMs. This work has now matured to include similar deployments in KY and SC. Table 1 summarizes the sensors and their purpose in the weigh-station environment; the second column shows the figure number that illustrates the sensor and its use. Figure captions provide more details about the sensors and their use for the State-police safety and security missions.

Some sensors employ sophisticated technology, while others are fairly simple. The idea in each case is detection of vehicle and payload features that fall outside the expected value(s). More specifically, a single sensor cannot accurately detect a weapon of mass destruction (WDM) or rouge shipment of radioactive material (RAM). Thus, a multi-detector system greatly increases the likelihood of finding such material. Integration of data from several different sensors provides a total situational awareness of a particular event. Indeed, these sensors should not be expected to make a specific determination. Rather, an alert from one (or more) sensors should spawn interest and precipitate further inspection, which is the key to safety and security of U.S. citizens.

Table 1. Current technologies for weigh-station deployments (overview in figure 3)

Short description of the technology	Figure	Specific data
Cellular communications		communications by cell phone
Chemical detectors: mass spectrometer & handheld	4	detection of explosives, etc.
Cyber security certificates		computer authentication
Digital cameras		vehicle configuration, status
Drivers license scanner		driver's identification
Handheld radioactive isotope identification devices	5	detailed radiation scan
Infrared cameras	6	local hot spots on vehicle
Integrated viewer		
Laser axle counter & vehicle length identifier		vehicle length, number of axles
Multiple user/viewer of real-time-data capability		
Optical character recognition cameras	7	vehicle license-plate number
Optical scanners	8	vehicle configuration/occupancy
Radiation Portal Monitors for gammas & neutrons	9	gamma & neutron radiation
RFID by NORPASS, PrePass®, EPA RadStraM	10	vehicle identification wirelessly
Satellite communications		satellite link for data
SensorNet node		interface to SensorNet
Static scales	11	vehicle weight while stationary
T1 communications		land-line for data link
Video cameras		images for truck surveillance
Weather sensors		wind velocity, temperature
Weigh-in-Motion (WIM) scales	11	vehicle weight while in motion
Wrapper software applications		integration of sensor outputs
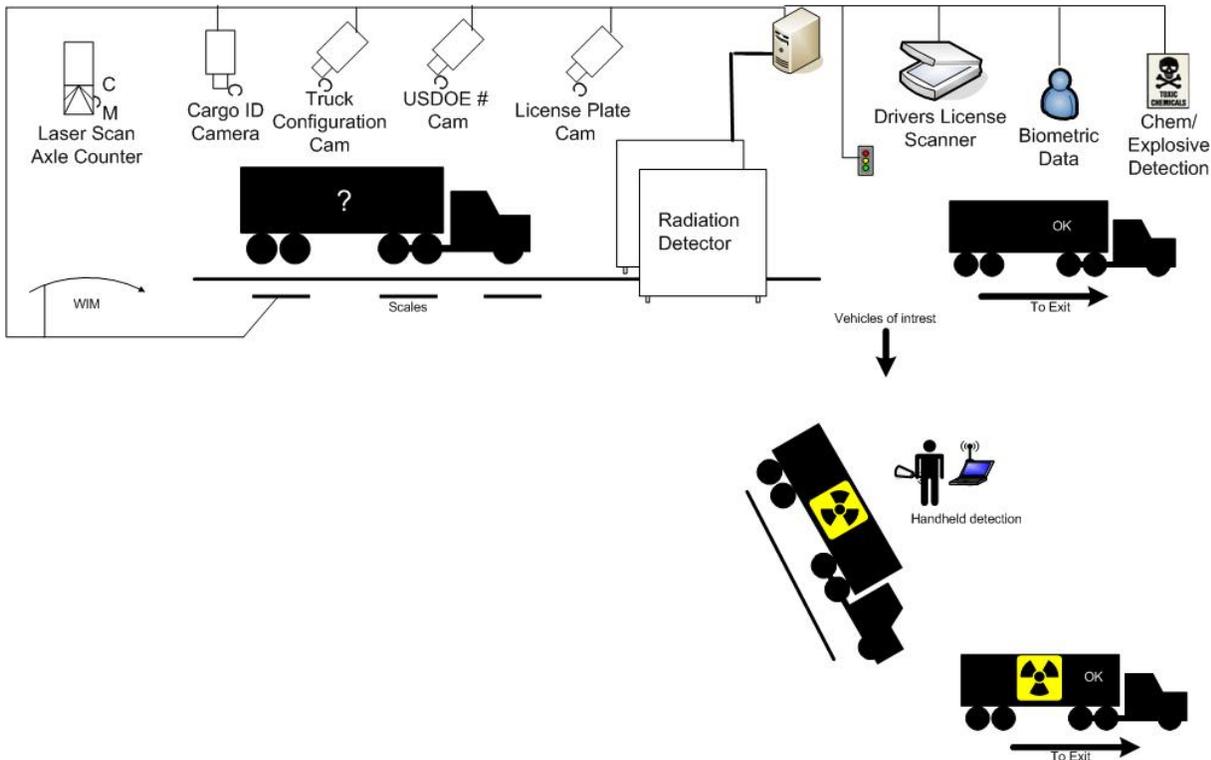
Figure 3. Multi-sensor, weigh-station deployment and conceptual traffic flow.

Trace Detection

Chemical, Narcotic and Explosive Detector - Available in both stationary and portable models, these detectors can detect and identify trace amounts of threat substances including explosives, chemical warfare agents, toxic industrial chemicals and narcotics.

500DT

Sabre4000

Figure 4. Chemical sensors.

Handheld Radiation Detection

Handheld Radiation Detectors - This handheld detector can give counts per second as well as give indication of Gamma and/or Neutron activity. Many handheld radiation detectors give indication if the personnel should move back away from the source of radiation. A handheld unit should be able to identify the radioactive isotope with indication of confidence level.
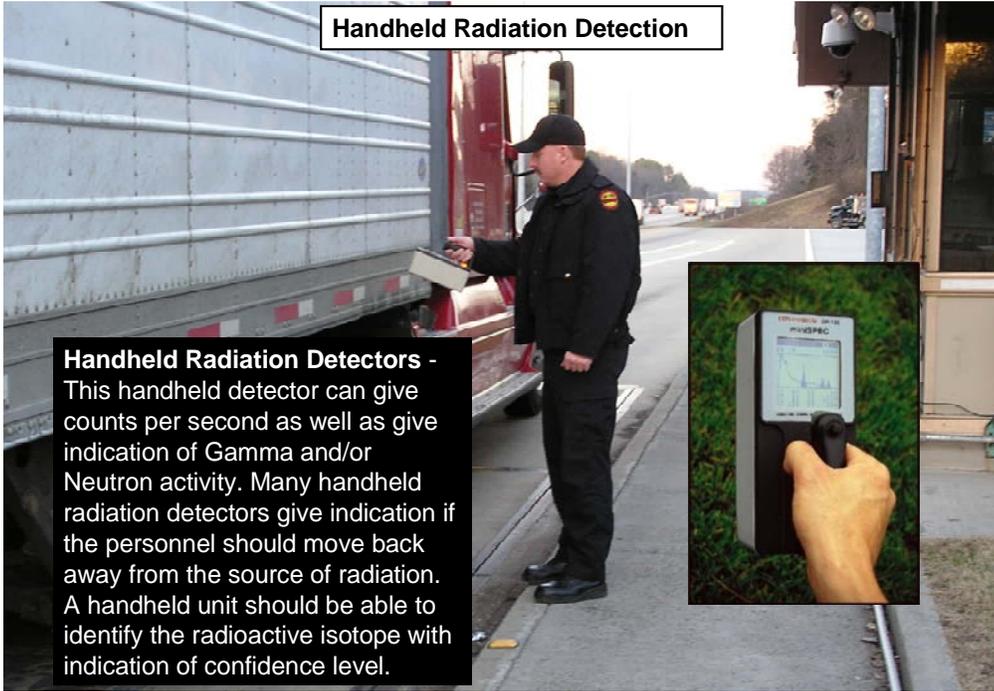
Figure 5. Handheld radiation detection.

Infrared Camera – The infrared camera can be used for detection of bad brakes. Infrared can detect heat in locations where heat should not be or appears to be extreme. Indication of extreme heat has enabled the detection of bad bearings and broken springs and cracks in chassis frames.

Figure 6. Infrared camera.
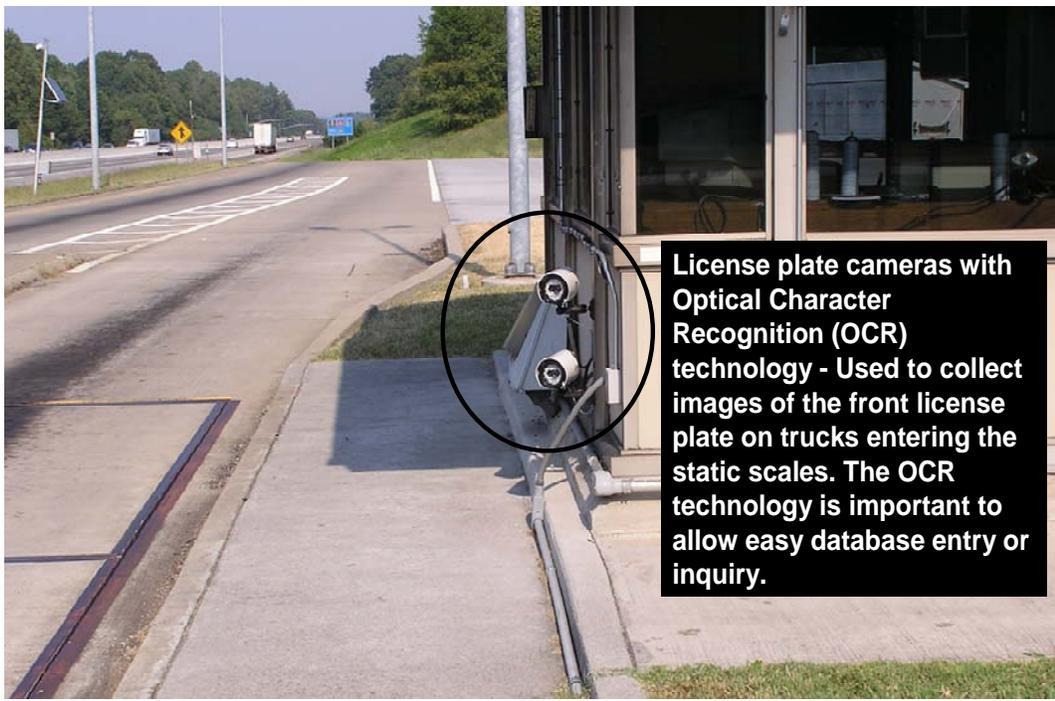
License plate cameras with Optical Character Recognition (OCR) technology - Used to collect images of the front license plate on trucks entering the static scales. The OCR technology is important to allow easy database entry or inquiry.

Figure 7. License plate cameras

Vehicle Classification and Configuration

Optical Laser Scan – Used to detect occupancy of a vehicle upon entering the static scale. This scanner scans the axles on a semi truck to determine the number of axles, speed, truck configuration, and overall length of the vehicle.

Figure 8. Optical laser scanner.

Radiation Detection

Exploranium

NucSafe

Radiation Portal Monitor - Radiation portal monitors can include Neutron and Gamma detection. Most of these systems are not designed to identify the radioactive isotopes. However, they can give Counts Per Seconds usually graphed by location on the vehicle.

PASSENGER: 01-10-2006 10:27:40, Vehicle # 7170 11.8 sec   DR: 0.0000 mR/hr   GAMMA ALARM

G584

G811

DRIVER   GAMMA ALARM

Figure 9. Radiation portal monitors.

Radio Frequency Identification (**RFID**) - An automatic identification method that uses an RFID Reader to retrieve data from an RFID tag. The data transmitted by the tag may provide identification or location information, or specifics about the tagged cargo. RFID technologies can be used to track valuable assets, hazardous cargo or pre-approved radioactive shipments.

Figure 10. Radio-frequency identification sensors.

Weigh In Motion – The WIM scale is a static scale designed to weigh vehicles while the vehicle is in motion. The WIM scale can give information such as the weight of the truck and configuration. If overweight is detected, the driver is directed by a signal arrow to pull onto the static scale.

Static scale – The static scale is used for accurately weighing trucks for compliance enforcement.

Figure 11. Weigh-in-Motion and static scales for vehicle weight.

A participating truck crosses the Weigh-in-Motion (WIM) scale and is identified and weighed electronically (Figure 11). Automatic vehicle identification systems (Figure 10) include RFID transponders on the commercial vehicles. If the truck's credentials or weight cannot be verified, the driver is signaled to enter the weigh station. These systems also allow transponder-equipped commercial vehicles to bypass designated inspection stations.

1.3. CHARACTERISTICS OF THE SOUTHEASTERN TRANSPORTATION CORRIDOR

The thirteen southeast states have 14,500 miles of interstate highways, compared to 46,600 miles of Interstate roads across the entire U.S. SETCP presently has deployed sensors at three weigh stations between Charleston SC, through Atlanta GA, to Cincinnati OH. The specific roads (lower right to upper left of Figure 12) are: I-26 north from Charleston to Columbia SC (790 miles); I-20 to I-285 (the Atlanta beltway, which is the required route for commercial vehicles); I-75 northbound through Chattanooga, Knoxville, and Kentucky to Cincinnati. The weigh-station locations are: Dorchester County SC on I-26 westbound, 45 miles west of Charleston SC; Knox County TN on the northbound side of I-75 just outside the city limits of Knoxville TN near the Watt Road exit; and Laurel County KY on the northbound side of I-75, about 5 miles north from the Corbin exit. These locations (north- and west-bound) capture the flow from Charleston to Cincinnati. The Knox County weigh station typically inspects 19,500 trucks/day or, 90 million tons/year. The population along both sides of this route is: 305,506 within 400 meters; 476,842 within 800 meters; and 1,244,214 within 2500 meters. These values come from the TRAGIS model using LandScan USA Interim population data. Two additional deployments are under consideration: Ringgold and Augusta Georgia. These sites are among the most heavily traveled routes out of the Charleston port. The Augusta site in currently under construction; deployment of SETCP equipment would be relatively inexpensive there. Both sites will have adequate network capability to handle the communications traffic.

A second (proposed) SETCP route is Interstate 95 from the North Carolina/Virginia line to Washington DC. The Virginia section spans 170 miles of I-95 through Virginia to Washington DC. The population along both sides of this route is: 113,348 within 400 meters; 196,356 within 800 meters; and 594,043 within 2500 meters. Commercial traffic along these two routes is some of the largest in the United States, as shown in Figure 13. Together these routes make up 1,224 miles of interstate highways in the Southeast.

Figure 12. Map of the two routes in the Trusted Corridor Project.

8
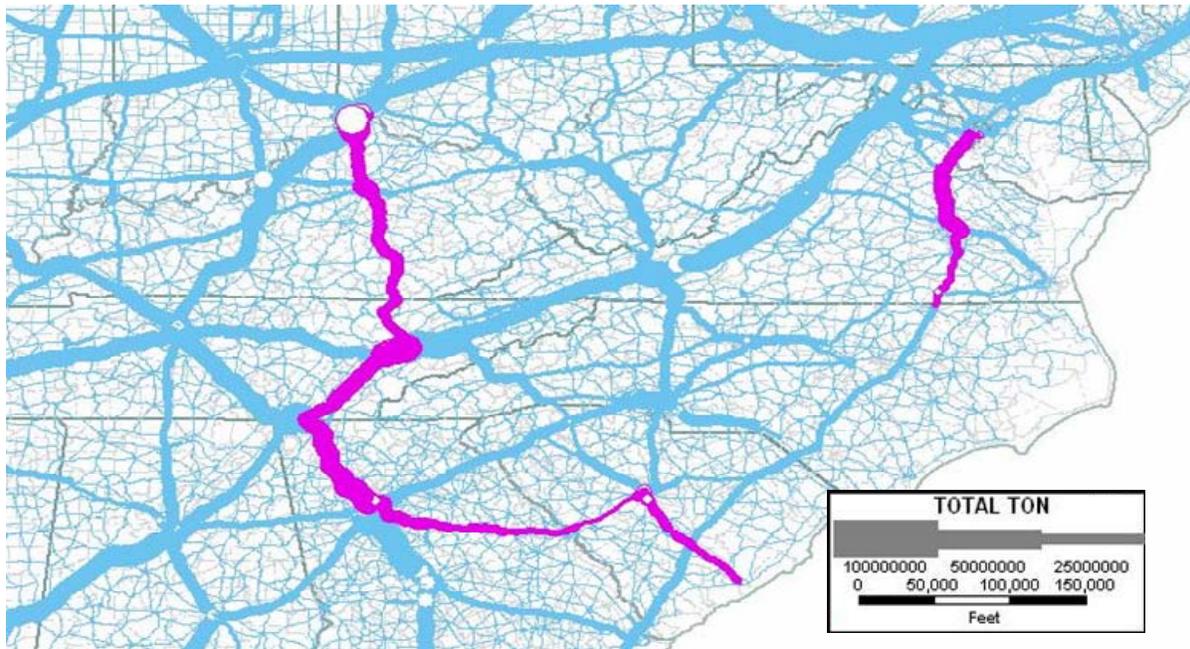
Figure 13. Commercial traffic (tons) over southeastern highways.

1.3.1. Interstate Connections to Southeast US Seaports

Many major coastal cities have seaports that handle ship-bound cargo to and from the U.S. Freight is typically shipped in inter-modal containers, which can be stacked for storage or transported by truck, rail, or air. These containers avoid freight handling during changes in transportation, thus improving security, reducing damage/loss, and allowing faster freight transfer. A measure of inter-modal container capacity is twenty-foot equivalent units (TEU), corresponding to standard container size (20 feet long, 8 feet wide, and 8.5 feet high). Most current containers are of the 40-foot variety or 2 TEU.

1.3.2. Southeastern Seaports

The port in Charleston SC (PortCharleston) is the busiest container port along the Southeast and Gulf coasts. PortCharleston is one of the nation's most efficient and productive ports, consisting of 5 different terminals with both rail and truck connections. The PortCharleston handled nearly two million TEUs in 2005. I-26 is within two miles of all PortCharleston terminals.

The Port of Miami Terminal Operating Company (POMTOC) occupies 518 acres in Dade County, Florida. POMTOC serves over 30 ocean carriers and handles over 0.5 million TEUs annually. I-95 is located only one mile from POMTOC.

The Port of New Orleans is located at the mouth of the Mississippi (MS) River, and is the ninth busiest in the nation. The 61-acre facility has an annual capacity of 0.37 million TEUs. I-10 is the primary access to and from the terminal.

Virginia International Terminals Incorporated (VIT) is located along the Chesapeake Bay in Norfolk, VA. VIT has four major terminals, which handled nearly two million TEUs in 2005. I-64 is the closest major highway, 100 miles west of the VIT.

2. HUMAN RESOURCE OPTIMIZATION & TRAINING

The most important of the five major components for mission success is human resource optimization and training. ORNL and vendors have conducted at least two training courses on radiation awareness for each state police department. These one-day courses (Figure 14) have included:
- DOE-developed U.S. Customs and Border Patrol training for radiation awareness;
- Brief overview of DOT regulations about RAM transportation;
- Hands-on training with real radiation sensors and live gamma and neutron sources.

ORNL also has participated in tabletop exercises in SC and TN. The exercise in SC included demonstrations at the weigh station in Dorchester County, SC.

Figure 14. ORNL awareness training in KY, MS, SC, TN, and WA.

The states of SC, TN, KY and MS have voluntarily committed to deploy DHS-type equipment at certain weigh stations. However, additional personnel are presently unavailable for these deployments. While DOT provides regular and overtime funding for compliance with their mandates, DHS does not follow this model. Without funding, additional requirements for state law enforcement personnel are not a prescription for success. This issue requires resolution for cross-agency interactions under SETCP.

Experience to date at the State level has validated the training approach by the Commercial Vehicle Safety Alliance (CVSA), in cooperation with DOE, Federal Motor Carrier Safety Administration (FMCSA), and the Department of Transportation. This training provides FMCSA certification up to level VI, including inspection of the vehicle and cargo, paperwork completion, and driver assessment. Shipments under a hazardous materials safety permit require inspection at point of origin by the FMSCA program. The training is especially helpful in guiding the officer's intuition about "routine" gamma alarms. Ongoing training will further develop these specialists and foster their certification. These specialists can (in turn) become mentors for the later deployment nationally.

2.1. INTEGRATED AND STANDARDIZED TRAINING

SETCP allows training integration with existing requirements. The following training attributes are recommended on the basis of our previous training successes at ORNL, SC, TN, KY, and MS:
- Standardized training program;
- Certification and testing;
- Requirements for recurrent training;
- Training fusion with DOT HAZMAT;
- State and local train-the-trainer instruction;
- training centers of excellence;
- Equipment calibration and diagnostics;
- Standard operating procedures.

2.2. MULTI-STATE/AGENCY THREAT SCENARIO EXERCISES

Separate exercises have been conducted in TN and SC. First responders and other participating agencies received valuable training and experience from these exercises. SETCP affords an opportunity to do multi-state exercises with many agencies. Such exercises should be included in personnel training requirements, including:
- Multiple agencies and states;
- Threat and non-threat incidences;
- Thrust needs;
- Communications challenges;
- Reach-back resources at a national and regional level.

2.3. REGIONAL TECHNICAL ASSISTANCE

One of the most controversial and difficult issues to date is the need for technical assistance to officers who are reluctant to ask for assistance. The U.S. Customs and Border Patrol have the most mature technical assistance program, which is designed for Customs officers at border crossings. However, current staff cannot handle a SETCP deployment from five are more weighs stations. Many states already have Fusion Centers, which provide command and control for emergency responses.

SETCP should develop a Pilot Fusion Center for primary reach-back with the following features:
- Multiple discipline expertise;
- Manned 24/7;
- Co-manned by state law enforcement officials;
- Real time access to the data at the weigh stations;
- Access to data and officers at mobile units;
- Procedures and secure data link to secondary reach-back resources;
- Multiple communications capabilities;
- Other redundancies (e.g., sensors, computers).

3. CONCEPT OF OPERATIONS

Results from the first deployment (Knox County TN) revealed that additional sensors were needed to capture essential data. Other equipment was necessary for operator assistance, data recording, and communications. Ongoing tests exposed law enforcement issues with Naturally Occurring Radioactive Materials (NORM) in agricultural products (e.g., tobacco) and manufactured goods (e.g., kitty litter and ceramic tile). The Tennessee State Police wanted technology to detect smuggled agricultural products (e.g., untaxed tobacco and illegal drugs) and environmental violations (e.g., RAM in sanitary waste vehicles). This shift in requirements focused on better data collection and sensor fusion, in terms of rule- and data-based knowledge discovery, as discussed in Section 4.

Sensors were identified to satisfy the new requirements. Those sensors were then categorized by the data they collect (Figures 15-18). We procured commercial-off-the-shelf (COTS) sensors that have a high degree of technology maturity. We also provided a graphical user interface (GUI) to integrate the outputs from these sensors in an "Officer Friendly" format with drill-down capability for more detail.
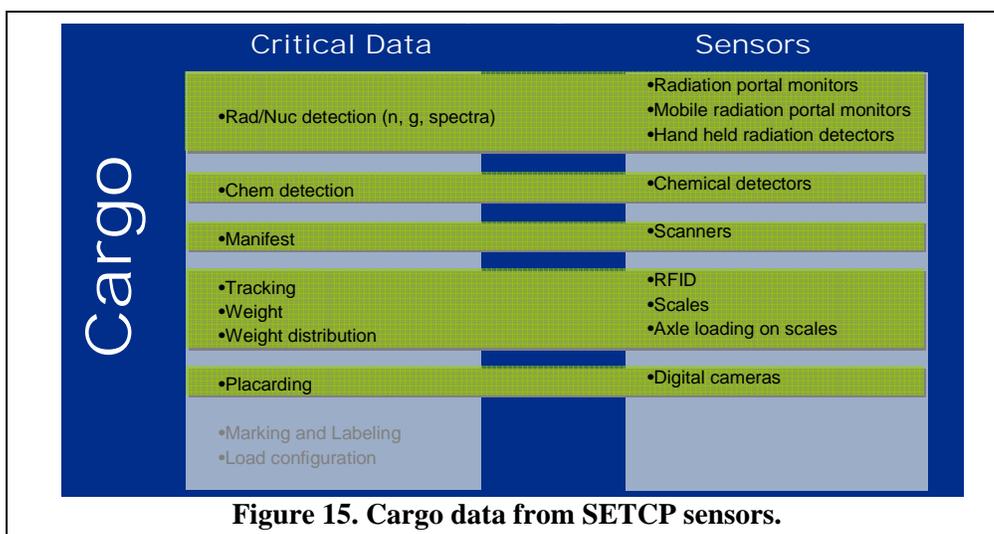
Figure 15. Cargo data from SETCP sensors.
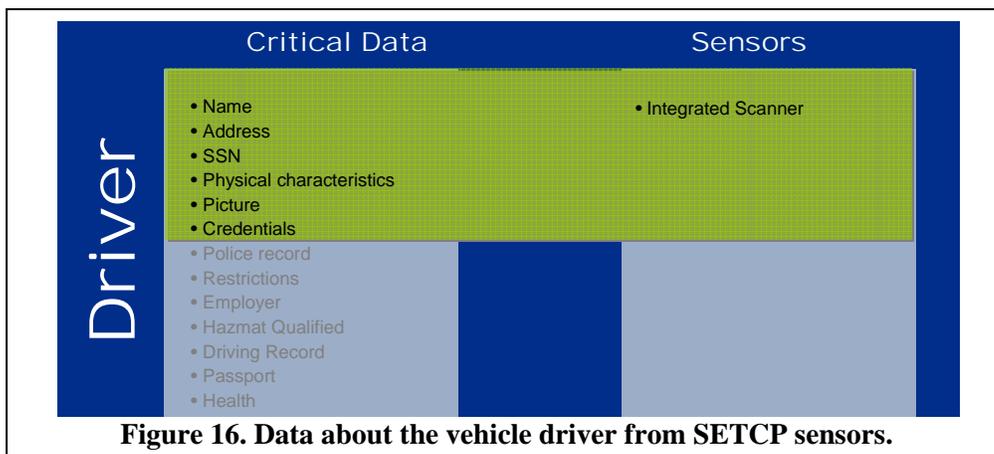
Figure 16. Data about the vehicle driver from SETCP sensors.
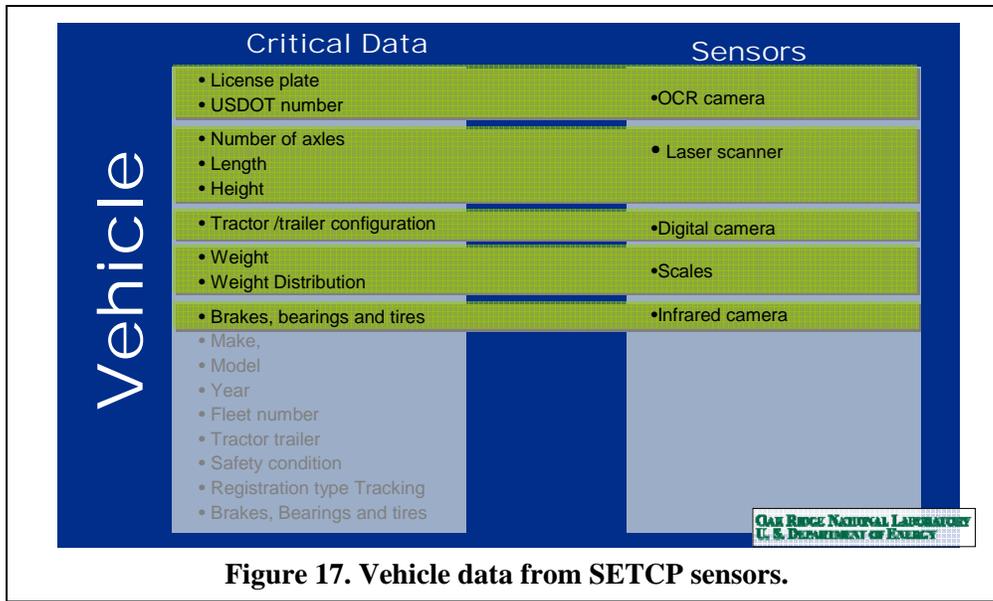
Figure 17. Vehicle data from SETCP sensors.
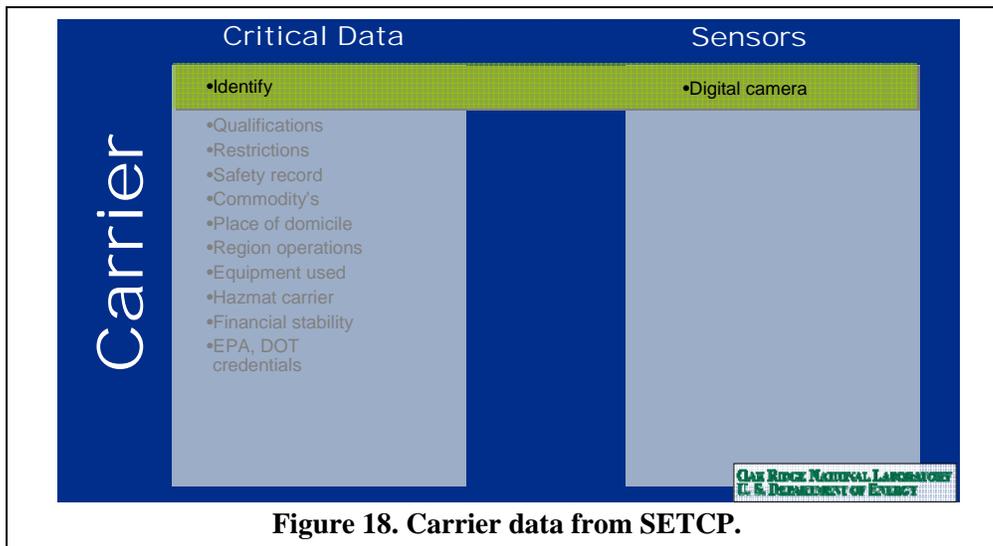
Figure 18. Carrier data from SETCP.

We subsequently identified easily accessible databases, with which to compare sensor output (e.g., DOT's CVISN for license plates). The additional sensors motivated sensor fusion issues (e.g., fusion of a radiological signature for tobacco, OCR identification for tobacco haulers, and weigh-scale output for tobacco loads). This approach allows anomaly detection to identify suspicious vehicles for closer inspection. This methodology is consistent with the current law enforcement model for illegal drug interdiction and highway safety enforcement.

The SC State Transport Police (SCSTP) asked ORNL to deploy a sensor system at their Dorchester County weigh station in 2003 under funding from the DHS Office of Domestic Preparedness (ODP). We provided procedures and protocols for handling alarms in accord with DHS guidelines, on the basis of experience with NORM and RAM alarms at the Knox County deployment. We developed a generic procedure for handling RAM alarms (Figure 19). This procedure has been used at the deployments in SC and TN, and is under consideration for use by KY at their Laurel County deployment.

DRAFT Portal Alert Truck Flow Chart

Figure 19. Safety-driven weigh-station response protocol for handling RAM alarms.
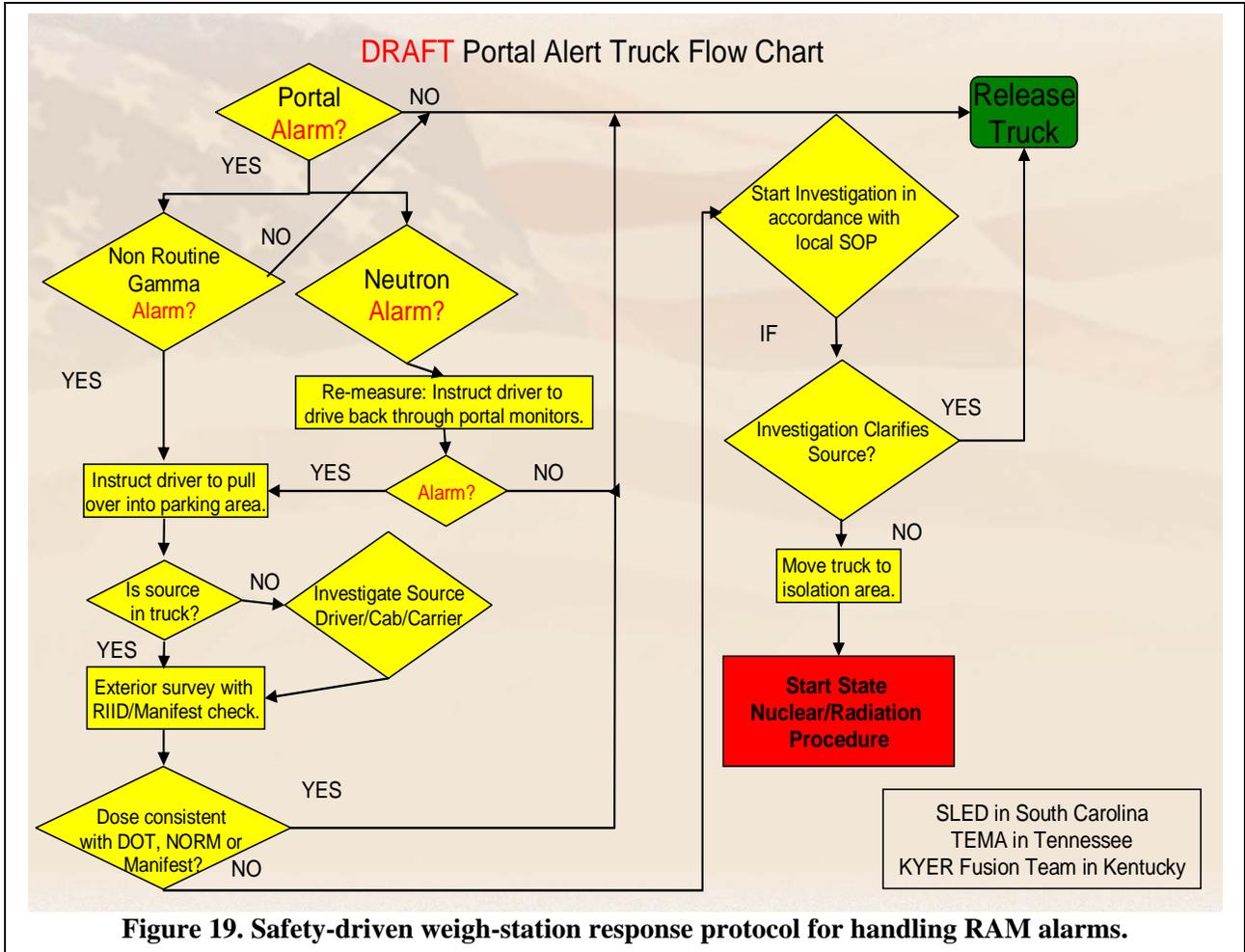
The most important DHS requirement is technical reachback, which involves getting the right data to the right people in a timely manner so that decisions can be about suspicious vehicles or cargo. This requirement motivated the ORNL team to incorporate spectroscopic data into the GUI viewer with presentation of the same data to reachback personnel in real time.

The ORNL/TN weigh station deployment was based on the three high level requirements: (1) compliance with Federal highway safety regulations and State criminal/civil laws; (2) corresponding event-driven data; and (3) technical reach-back to the State and Federal levels. The DHS Domestic Nuclear Detection Office (DNDO) is now formulating a program for better requirements. Discussions are underway between interested southeastern states and DNDO under the SETCP effort. Subsequent paragraphs explain the concept of Operations (ConOps) that were summarized in Figure 1.

3.1. SOUTHEASTERN TRANSPORTATION CORRIDOR PILOT

Present SETCP States (TN, SC, KY) want to coordinate their efforts, while simultaneously improving homeland security, highway safety, drug enforcement, and detection of potentially non-compliant vehicles via DHS-funded technologies. DNDO can leverage this opportunity. However, a pilot project will not achieve these results by focusing on detector performance, technical reach-back, and advanced algorithm development for DHS needs. SETCP success depends on integration of the current weigh station ConOps with the DHS IND mission, including:

- Integration of additional technologies with RAM detection for law enforcement and safety;
- Limitations of radiation detection devices in a highway environment;
- Evaluation of State and Local resource needs for these technologies;
- Policies and procedures under which these technologies will be deployed.

A proposed SETCP route might leverage weigh station deployments in SC, TN, and KY and current Customs and Border Patrol (CBP) efforts in Charleston, SC. The proposed work not only leverages present ORNL weigh station deployments, but also:
- Costs associated with sensor integrations;
- State personnel training and experience;
- ORNL resources with five years of weigh station experience;
- Coordination with other agency partners who have programs associated with these deployments;
- Momentum associated with the existing work.

3.2. DUAL USE APPLICATION IDENTIFICATION

The State mission (Figure 20) focuses on vehicle enforcement. Consequently, stand-alone RPM detectors are inadequate, because the additional tasks (e.g., RPM paperwork and procedures) cannot be addressed without integration with existing information and responsibilities.
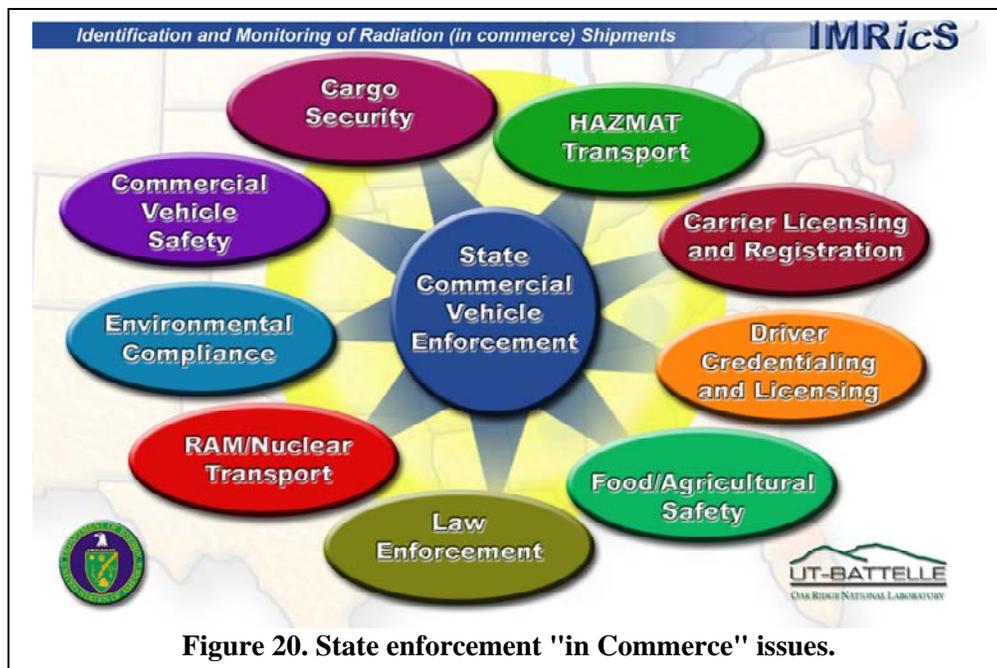
Figure 20. State enforcement "in Commerce" issues.

Most national deployments have been totally focused on detection/deterrence of improvised nuclear devices (INDs) and dirty bombs. Much of this effort has been devoted to detector improvements, technical resources for field personnel, and additional complimentary technologies (e.g., cameras). The highway weigh station environment offers the unique opportunity to explore dual use technologies, as well as integrated applications for law enforcement personnel, including:
- Unique features to access other data to determine the legitimacy of the vehicle;
- Detection of suspicious bypasses or mobile identification of vehicles;
- Regulatory changes that provide dual applications;

- Subject-matter experts who understand and support the DHS mission;
- Legal case law that enables the use of these technologies;
- "Trusted" carrier/shipper programs to identify/regulate material shipments.

3.3. DEVELOPMENT OF A GRAPHICAL USER INTERFACE

ORNL's experience to date in the multi-technology weigh-station deployments identified the need for GUI applications to merge sensor information, and to provide the Officer with data anomalies. While this technology will be transferred to the private sector for commercialization, certain aspects of GUI development are inherently governmental and can be performed only by the cognizant agency, including:
- Law enforcement for criminal applications;
- Technical reachback for IND applications;
- Emergency management for public safety applications;
- Intelligence for national security applications;
- Research and development for law enforcement and DHS applications.

3.4. ALARM RESOLUTION

Alarm resolution is one of the most controversial issues for the Federal, state and local stakeholders. State and local law enforcement is not a "written" procedure-driven process. Rather, this effort is driven by the enforcement officer's training, intuition, and experience. The philosophy is "Be on the Lookout" (BOLO) to provide continuous intelligence, in addition to intelligence from non-law-enforcement sources. Moreover, the mere presence of law enforcement officers provides deterrence. Alarm resolution is complicated by individual privacy laws for search and seizure of POVs, and by a lack of case law for RPM-alarm-driven searches. However, Federal deployments at international border crossings and ports use a standardized set of international entry procedures, which are inconsistent with the state and local approach, as discussed above. ConOps must be developed for law enforcement that includes:
- Dual use applications for detection;
- Integration of sorting or targeting into deployments and software;
- Acceptable levels of NORM alarms;
- Better identification of routine NORM;
- Officer experience, intuition and training;
- Risk-based approach to resolution;
- Random inspection and search procedures;
- Automated collection of forensic information during missed alarms or equipment failure.

3.5. COMMERCIAL CARRIER AND SHIPPER PARTICIPATION

Figure 21 shows the regulations for interstate transportation, including 49CFR under DOT, 10CFR under the Nuclear Regulatory Commission (NRC), 29CFR under the Occupational, Safety, and Health Administration (OSHA), and 40CFR under the Environmental Protection Agency (EPA). These regulations include participation by the private sector (the regulated party), and typically involve administrative programs to reduce downtime and unnecessary delays. To foster this effort, existing programs such as Highway Watch, CVISN, CVIEW must be leveraged and benchmarked to provide for:
- Identification of shippers and carriers that are most affected by the deployments;
- State-driven but Federally-standardized programs for enforcement;
- Trusted carrier and shipper programs;
- Incorporation of identification of trusted carrier or shipper in existing highway sorting programs;
- A rulemaking process for input before issuance of requirements;

- Participation in other agency pilot programs.

Figure 21. Regulations for interstate transportation.
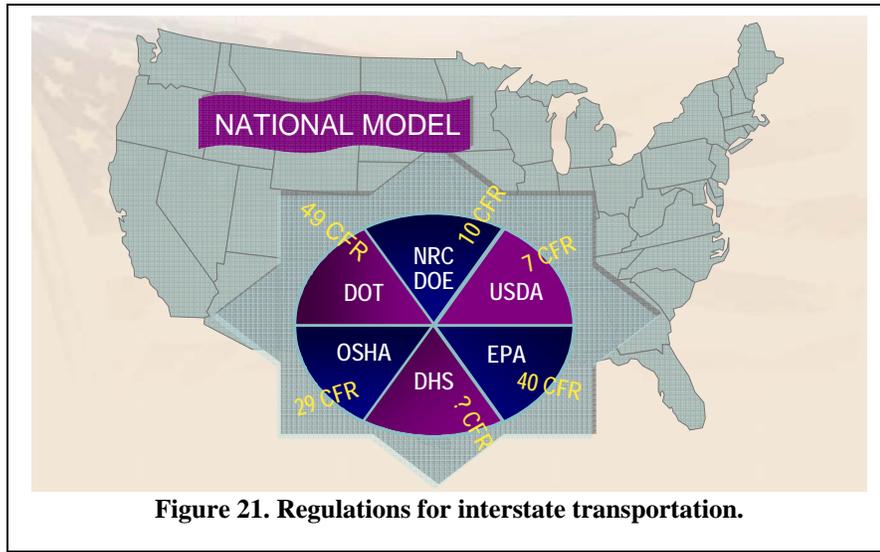
3.6. INFRASTRUCTURE NEEDS FOR SENSOR DEPLOYMENT

DHS deployments will require retro-fitting into existing facilities with various infrastructure capabilities. ORNL experience has revealed wide variation in site-specific ConOps and resources; see Figure 22 as an example. These factors complicate development of procedures and protocols, alarm resolution, and equipment installation. Many factors impact infrastructure requirements, including:

- Real estate availability;
- Traffic congestion;
- Threat conditions;
- Chokepoints;
- Weather and climate;
- Adequate communications;
- Ample space (outdoor and indoor);
- Ability to bypass or avoid inspection;
- Local community acceptance;
- Utilities (e.g., clean power);
- Backup or redundancy;
- Site access.

Figure 22. Present deployment sites.

3.7. INTERDICTION

Deployment requirements at the Nation's borders and ports are clearly defined, in terms of jurisdiction and interdiction of suspicious vehicles or persons. Moreover, the legal constraints are better defined in terms of access, privacy and case law. The interdiction process is further complicated by the long term goal of DOT and DHS for "on the fly" (i.e., mobile) detection via current technologies and procedures. Interdiction requirements include:
- Situational exercises for coordination between multiple states and localities;
- Covert tracking and surveillance of suspicious vehicles and cargo;
- Automated BOLOs;
- Local and state command and control;
- Evacuation modeling;
- Regional Fusion Centers for technical reachback;
- Total situational awareness capabilities.

3.8. MAINLINE SORTING/TARGETING

Although mobile and re-locatable units are desirable, they do not provide targeting or sorting of suspicious vehicles or cargo among the millions of vehicles on the nation's highways. Mainline sorting and targeting of vehicles is an established and desirable concept, especially in weigh station operations. Indeed, two major companies (e.g., NORPASS and PrePass®) are working with the law enforcement community and motor carrier industry on safety-driven weigh-station bypass. Mainline sorting/targeting is achievable in the Rad/Nuc detection environment, but most of the R&D funding for Rad/Nuc detection is focused on advanced portal spectroscopy (ASP) and advanced algorithms. These technology advances will be most effective for interdictions with strict entry-release control (e.g., international borders, ports). Mainline sorting/targeting is a critical component of highway ConOps, including Rad/Nuc technologies.

3.9. TRACKING

ORNL pilot tests have shown that well-defined commodities consistently activate the RPM alarms. Figure 23 shows a typical list of NORM at the Knox County inspection station. These commodities can certainly be tagged by the manufacturer, and then tracked in transit by RPMs at inspection stations or in mobile units, not unlike mainline sorting as discussed above. For example, Sandia National Laboratories at Livermore has conducted studies on NORM commodities and their radiological characteristics in transport. Radiological Source Tracking and Monitoring (RadSTraM) is an EPA-funded ORNL project to investigate radio frequency technologies for tracking and monitoring radiological sources in commerce; see Figure 24. RadSTraM includes procedures and protocols for an operational system, as well as a nationwide supply chain (Phase II) for major radioisotope suppliers and shippers. The criteria for these tests include:
- Type A package with electronic seal and active and/or passive, hybrid RFID tag(s);
- Type A quantities of medical radioisotopes;
- Shipments from PerkinElmer, Inc. in Boston, Massachusetts (major production facility);
- Transport via commercial DHL's Air Express service;
- Receiver at ORNL in Oak Ridge (Anderson County), Tennessee;
- Equivalency tests for gamma and neutron radiation;
- ORNL's SensorNet data collection application for data collection and documentation of results;
- Analysis of data and incorporation of lessons learned into Phase III tests;
- Configuration testing and RFID listeners at ORNL, Boston (PerkinElmer, DHL), and Knoxville.
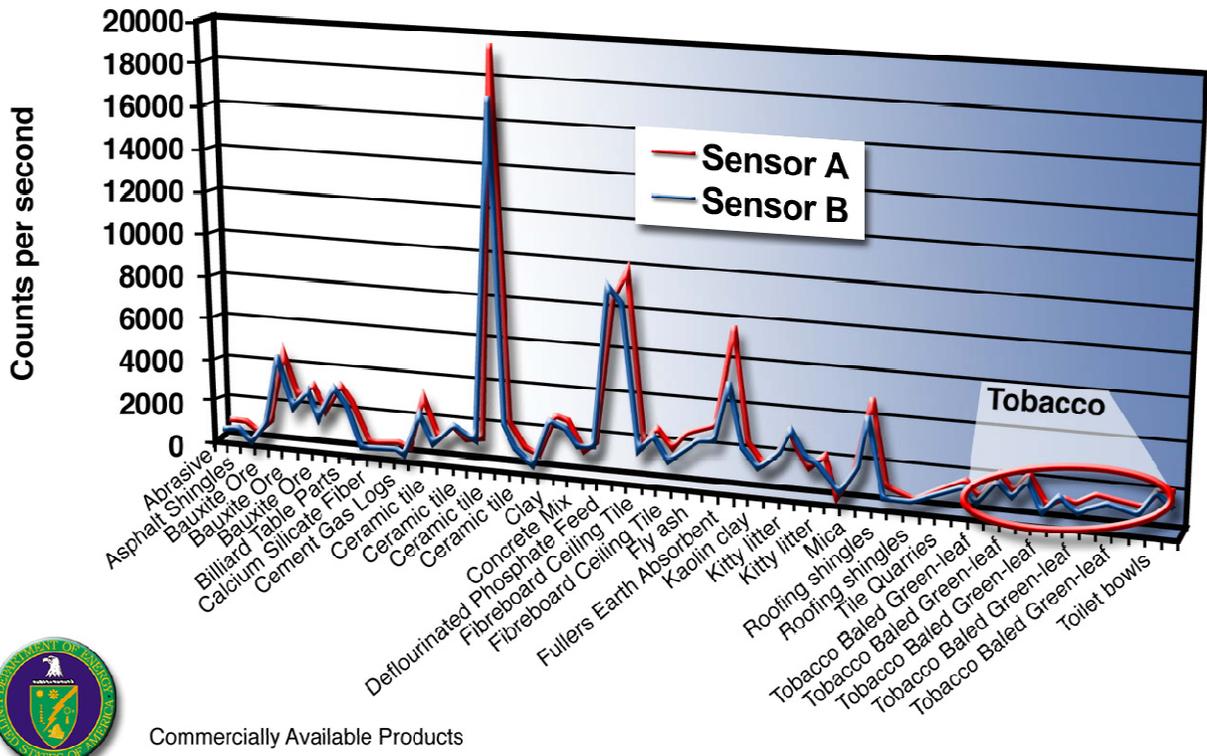
Figure 23. Identification of naturally occurring radioactive material at the Knox County site.

Figure 24. Collaboration on radiological source tracking and monitoring.

Currently DHS is funding an Engagement Analysis Study at ORNL that:
- Identifies the largest (top 80%) radioisotope commercial shippers and carriers;
- Identifies types, amounts, routes, commercial carriers, and distribution vendors/contractors;
- Analyzes the curent standards and procedures for these carriers and shippers;
- Identifies potential gaps in current requirements relative to DHS's radiological/nuclear mission;
- Analyzes technologies to identify/track these shipments through the supply chain;
- Imposes the least cost and with minimal disruption of commerce.

Additional pilot studies are being conducted for in-transit identification of high-risk or high-value commodities. The opportunity under the SETCP tracking task is integration of these technologies with RAD/Nuc deployments for NORM, Indutsrial and Medical isotopes, and existing infrastructure (i.e. PrePass® and NORPASS).

3.10. ALIGNMENT WITH THREAT CORRIDORS AND SURGE REQUIREMENTS

Present plans recognize the temporary, event-driven need for additional detection resources along certain routes or transportation corridors. Fixed deployments (e.g., weigh stations) are inadequate for these temporary or "surge" requirements. However, fixed deployments are required to establish the basic inspection infrastructure (e.g., sensor integrations, personnel training and experience, communications, knowledge discovery, procedures and protocols, and ConOps). Moreover, these fixed deployments provide safety/security assurance along the original routes and corridors, which can then be supplemented by dual-use resources. Figure 25 depicts changes in sensitivity and selectivity of present inspections that can be "tuned up" on the basis of intelligence reports and threat advisories. Regional agreements are needed to coordination these efforts under Federal (e.g., like DOE RAPP teams, or response regions under EPA or NRC). Alignment of regions under the DOT model seems best, due to the dependence on the DOT transportation requirements and the need for the cooperation among state police and regulatory agencies. For example, Figure 26 depicts a Southeastern Region that is closely aligned with the DOT Southern Leadership States Conference.

Figure 25. Normal inspections (dash line) versus tuned inspections (solid line).

Figure 26. Suggestion for states in the southeastern region.
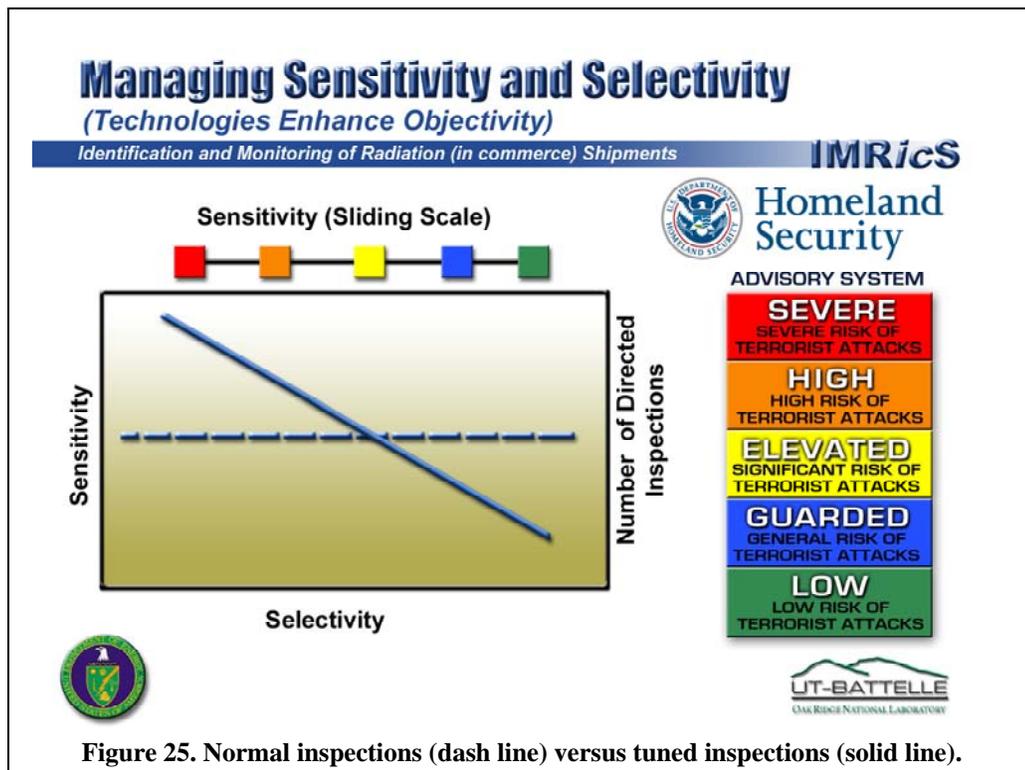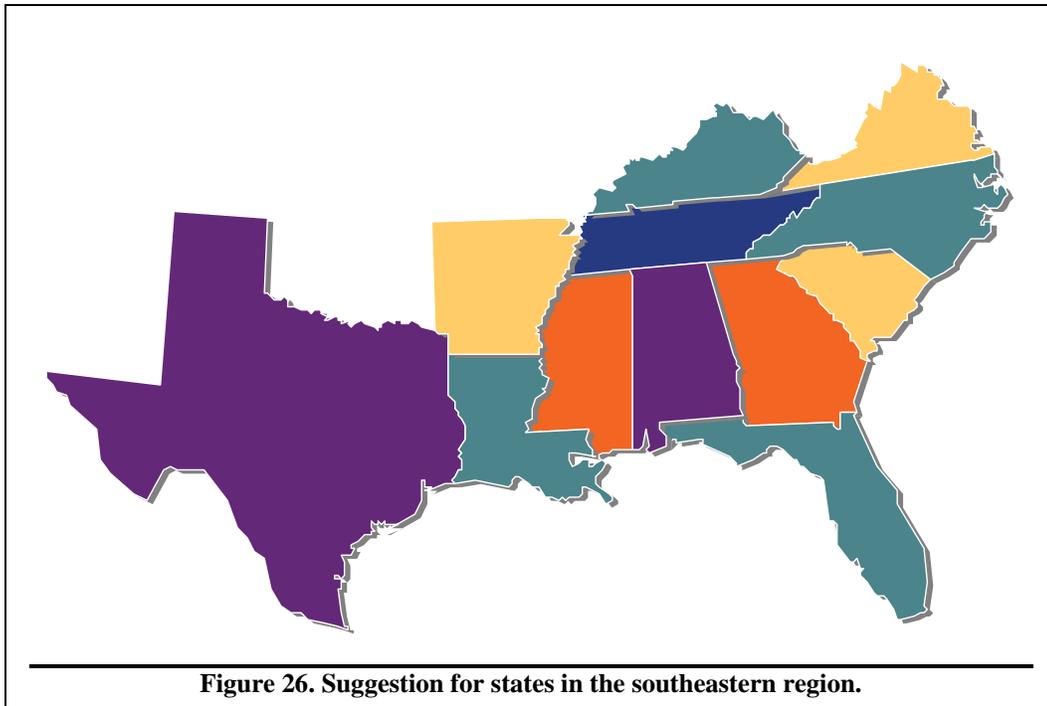
3.11. DETERRENCE AND SURVEILLANCE

Deterrence and surveillance are essential components of law enforcement ConOps, and should likewise be considered in the SETCP deployment. For example, RPM "dummies" can be placed at strategic locations to deter violations and/or to move suspicious vehicles into lanes where interdiction is easier. Moreover, vehicles or cargo can be identified at one location with better detection sensitivity for subsequent inspection at the next location with better interdiction capability. This approach to law enforcement officers is also used for interdiction for illegal drugs and drunken driving.

4. KNOWLEDGE DISCOVERY AND COMMUNICATIONS REQUIREMENTS

Information integration is a critical component for SETCP success. This component includes integration of the sensor information, maturation of the integrated technologies, and infrastructure to support a nationwide deployment. Figure 27 shows the variety of information, involving the acquisition of data from many sensors, and the use of rule- and knowledge-based applications for regulatory enforcement by state police. The functionality to enable these applications include:

- Identification of information for decisions;
- Selection of sensors to collect the information;
- Identification and access to databases for confirmatory comparison of critical information;
- GUI development;
- Data architecture plan for archival information from earlier SETCP deployments;
- Baseline data collection from deployments;
- Selection of data fusion candidates for "smarter" sensor integrations.

Figure 27. Need for data integration and knowledge discovery.
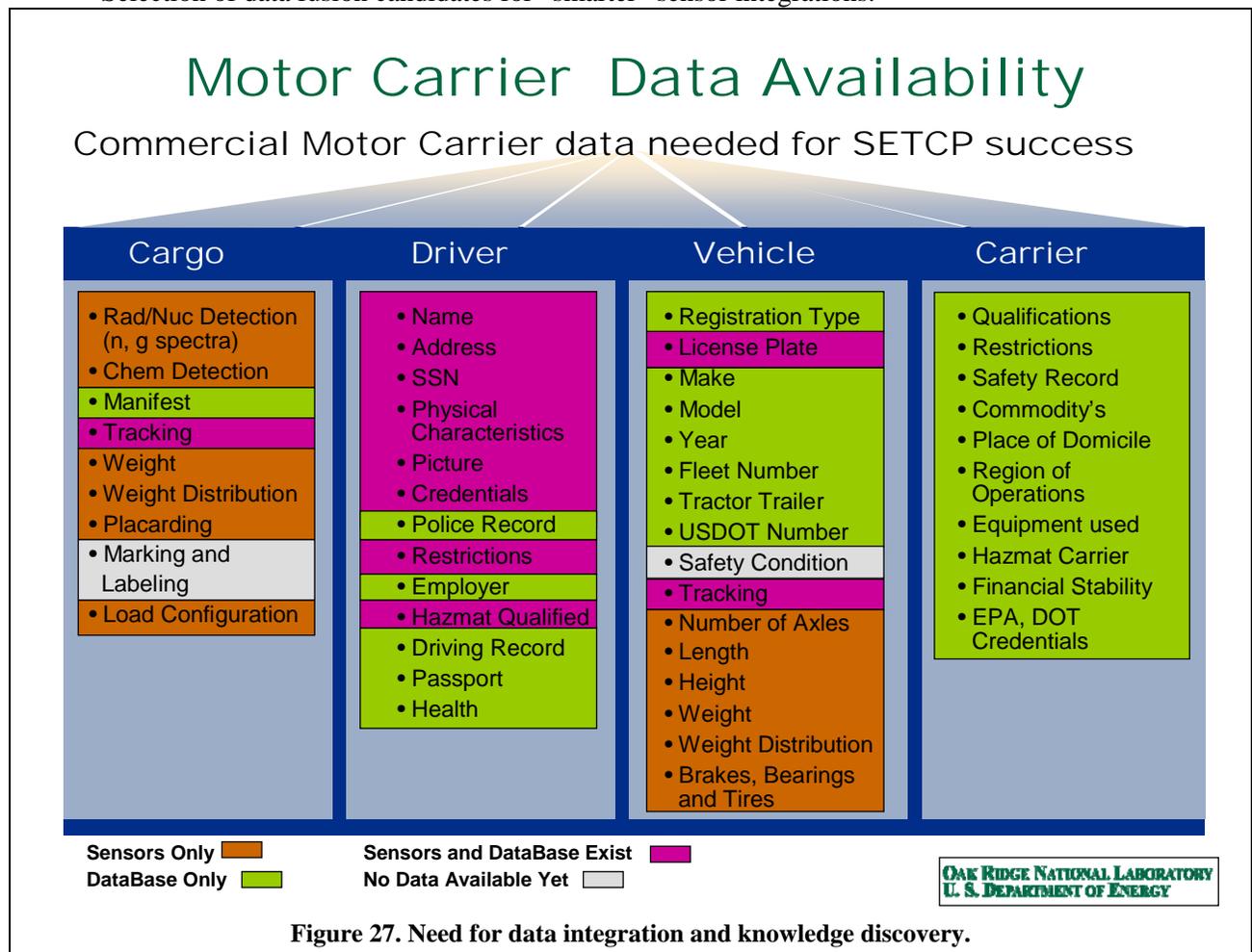
4.1. BASELINE DATA COLLECTION REQUIREMENTS

The first step in the knowledge discovery process is collection of baseline sensor data. ORNL has collected such data, in cooperation with SC, TN and KY. Moreover, ORNL has begun the integration

effort. Additional data is needed to develop rule- and knowledge-based applications. Requirements for the acquisition of sensor data are shown below:

- Durable, non-labor-intensive process for data acquisition;
- GUI presentation of sensor data to state police and reachback SMEs;
- Identification of database approaches for integration of sensor data;
- Beta-testing of less complex sensor integrations with participating vendors;
- Secure means for data sharing;
- Automatic identification of data anomalies through built-in diagnostics to assure data quality;
- Publicly available data standards for vendors and users.

Figures 28 and 29 show examples of integrated RPM output.
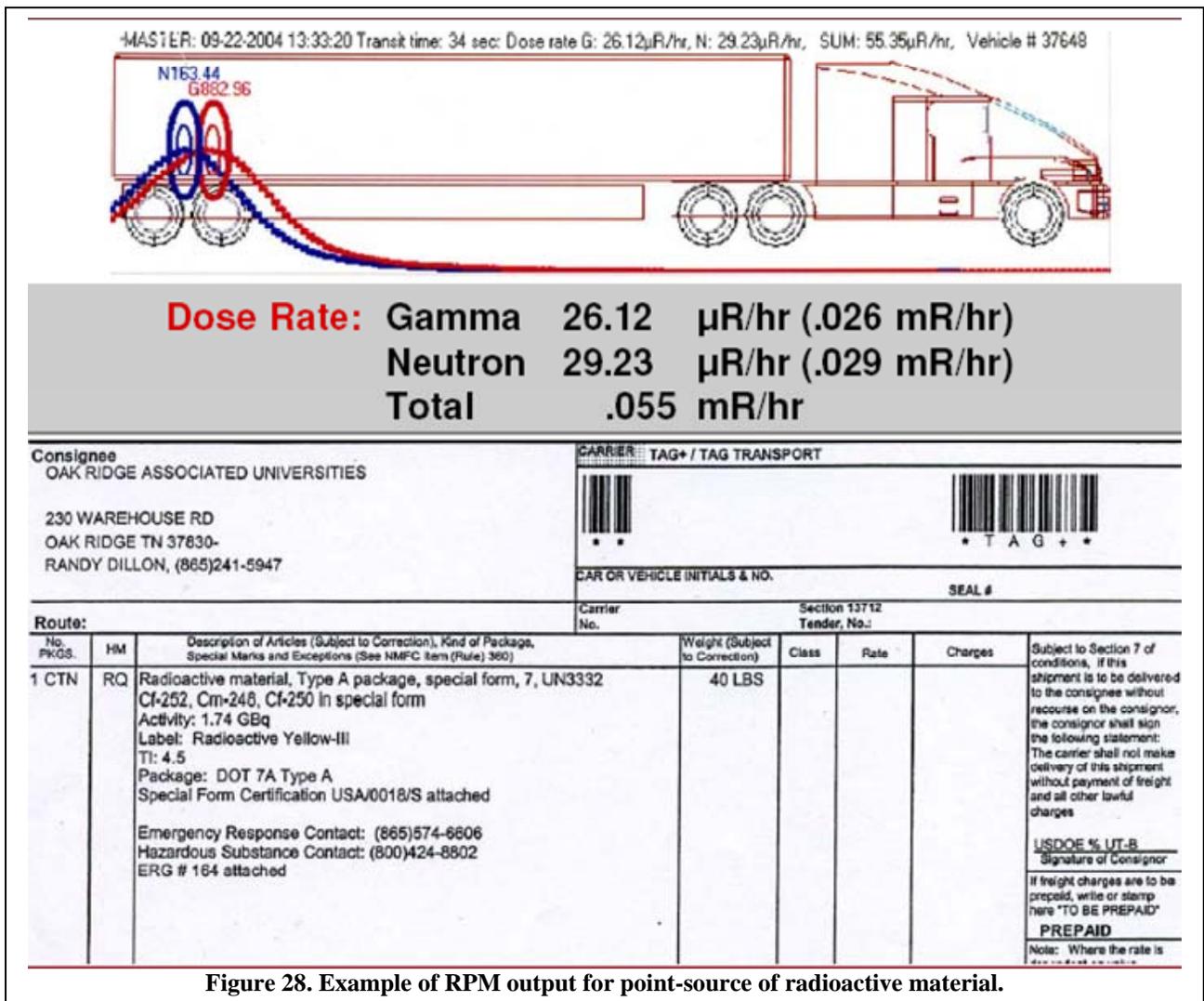
Figure 28. Example of RPM output for point-source of radioactive material.

REMOTE: 08-31-2004 08:53:07 Transit time: 11 sec: Dose rate G: 10.38µR/hr, N: .38µR/hr, SUM: 10.76µR/hr, Vehicle # 31746

G7.93

G7.93

☐ Original BOL ☒ Shipping Order ☐ Loading Order		PRICE CLASS 10	MILES 868	FROM	Golden Products Div. of Nestle' Purina PetCare Co
CARRIER PENM PENN'S BEST, INC	SUPPLY POINT BLOOMFIELD		MO 63825	LOADING ORDER NUMBER 3133783	
SHIP TO GOLDEN CAT - KING WILLIAM 931 DUNLUCE RD RALSTON PURINA COMPANY KING WILLIAM VA 23086	ROUTING Selling Party: Nestle' Purina PetCare Co.			SCH. SHIP 08/30/04	CRA DATE 09/01/04
				COMMENTS	

| ORDER NO. 3133783 | CUSTOMER P.O. NO./DATE 797-726065 | CUBIC FT. 1004 | PRODUCT WT. 44064 | TOTAL QTY. 1080 | UNIT LOADS 20 | CASES PICKED 0 | SEAL NO. 172755 |
| | DATE SHIPPED 08/30/04 | QTY. SHIPPED 1080 | CAR OR VEHICLE INITIAL & NO. 5446 | DATE LOADED 08/30/04 | FREIGHT TERMS Prepaid | | SEAL NO. |

Shipper hereby certifies that he is familiar with all the terms and conditions of the said bill of lading, including those on the back thereof, which govern the transportation of this shipment, and the said terms and conditions are hereby agreed to by shipper and accepted for himself and his assigns.

BILL OF LADING CLASSIFICATION CODES (SEE REVERSE SIDE)

IF CHARGES ARE TO BE PREPAID, WRITE OR STAMP ABOVE "PREPAID"

Figure 29. Example of RPM output for a distributed-source of radioactive material.

4.2. STANDARDS

Reporting standards are different across Federal agencies (e.g., DOT, DOE, DoD), states, and localities. Consequently, DNDO probably will have to use those existing standards, specifically the requirements under state DOTs, which comply with Federal DOT standards for reporting (IEEE 1512.3). Appendix A discusses this standard, which is intended for reporting HAZMAT incidents (e.g., chemical spills and releases) rather than safety compliance and routine inspections. Consequently, implementers will probably adapt this standard for local requirements with flexibility for local control and local decisions, since by definition all incidents are local. Related standards include ANSI N42.42 and WFS-T. The IEEE 1512.3 HAZMAT standard has versatility to adapt the recommended message to local conditions, although the basic structure of the messages is fixed. The locality manages the operational complexities, acquires and archives the data, makes queries to multiple databases for all of the relevant information, and shares the results as appropriate.

4.3. SYSTEM DIAGNOSTICS

Assurance of system reliability and quality requires well-documented and auditable diagnostics that are:
- Automatic;
- Properly calibrated to known standards, either locally or remotely;
- Appropriately maintained, either locally or remotely;
- Functional under standard operating procedure(s);
- Providing the state of system health during each occurrence;
- An integral part of the technical assistance program.

4.4. CYBER SECURITY REQUIREMENTS

A data security system needs to be designed that ensures multiple levels of user access (e.g., classified, restricted, OUO, and compartmentalized), including:
- Certificates controlled by central security point of contact;
- Detection of cyber attacks and identification of the attacker;
- Compliance with multiple federal and state agency requirements;
- User-transparent updates and changes;
- Detection and identification of system users;
- Acceptance and archival of data updates from multiple data sources.

4.5. DATA TRANSFER

SETCP success depends on acquiring data from disparate sources, saving the data at central locations, integrating the data for the technical reachback and law enforcement community, and alerting decision makers at different levels. The underlying network capabilities include the following linkage capabilities:
- Weigh station to weigh station;
- Car to car;
- Car to officer;
- Officer to officer;
- State law enforcement to state fusion center;
- State fusion center to regional technical assistance;
- Regional technical assistance to RAPP and/or technical reachback;
- Reachback to the Federal Bureau of Investigation (FBI);
- State to state law enforcement;
- State to local law enforcement;
- Federal law enforcement to all;
- Secure data transfers;
- Network redundancy;
- Data transfer rate of ≥42 kilobytes/s;
- Voice-conferencing capability to facilitate multi-party discussions about data and screens.

4.6. INFORMATION SHARING

Each SETCP location must also be able to obtain information that is locally pertinent, a timely item (e.g., vehicle driver, tag, red signature), and change alert status change, including:
- Law enforcement BOLOs;
- DHS alerts;
- Agricultural embargoes;
- Stolen vehicles;
- Illegal immigrant migrations;
- Safety issues (e.g., reckless driver or hijacked load);
- Tips about illicit drug movement;
- Intelligence information;
- Trusted corridor vehicle clearances and BOLOs.

5. DATA RESEARCH AND DEVELOPMENT

This effort requires a phased approach. We expect that initial R&D will focus on data integration of multiple sensor outputs for DHS detection needs (e.g., radiation dispersal device and WMD), as well as highway safety via anomaly detection. We anticipate that Phase II work will acquire baseline data to eliminate nuisance alarms for certain commodities with NORM. This work supports law enforcement and highway safety, including:

- Mock shipments with and without nuisance-alarm NORM in the load;
- Addition of spectroscopy to the RPM data;
- Addition of imaging (object video) technology (e.g., show numbers, configurations or patterns);
- Addition of metadata (e.g., weather, time, shipping patterns, engagement/threat analysis);
- Gap analysis (e.g., needs for sensors, data, operations, training, legal, procedures, political).
- Advanced R&D (e.g., multiple hypothesis tracking, learning- and rule-based systems);
- Requirements for specific to R&D applications.

5.1. IDENTIFICATION AND ACCESS TO EXISTING DATABASES

Since all data needed is not neatly available in existing national databases it will be necessary to identify data needed and where data currently resides, including:

- Development of data requirements (graded approach for acquisition);
- Identify data sources and source reliability;
- Architecture for access to and data acquisition from multiple, disparate databases;
- Removal of political/legal barriers to data access (perhaps the most difficult issue);
- Integration of databases;
- Identification of improvements for better access to disparate data sources.

5.2. NEW DATABASE DEVELOPMENT

Development of new databases will be required for several reasons. Necessary data may be unavailable, or available only from multiple disparate sources. New deployments may provide unique data that was previously non-existent. These databases must be easily accessible, secure, and reliable for integration into SETCP, including:

- Unique databases for advanced algorithm development by the R&D community;
- Access by the reachback community;
- Development of a data strategy for Trusted Corridors;
- Compartmentalization of data access to ensure proper security;
- Data integrity and network reliability for critical data streams;
- Adequate data storage.

5.3. ADVANCED ALGORITHM DEVELOPMENT FOR MULTIPLE SENSORS

DHS is supporting advanced algorithm development. However, the underlying data was not sufficiently comprehensive enough to make the originally-envisioned advances. Consequently, additional data and new sensors are needed to support ongoing advanced algorithm development. This work includes:

- Appropriate metadata (e.g., specific alarm, manifest, time, weather, vehicle characteristics);
- Controlled experiments with authentic materials, deployments, shippers, and carriers;
- Investment by sensor vendors in integrated "cookie cutter" products for immediate deployment;
- Use of sorting or targeting quotas to decrease inspections;

- Development of "easy" algorithms with placeholders for notional applications;
- Ongoing acquisition of baseline data;
- Anomaly detection on the basis of material, location, time, carrier container/vehicle, etc.
- Partnerships with industries and carriers that produce NORM or RAM near deployments

5.4. SMART DATA COLLECTION ANALYSIS AND SYSTEM UPGRADE FOR MOBILE/RELOCATABLE APPLICATIONS

Mobile and relocatable deployments require initial testing at fixed SETCP facilities. This work involves data collection and determination of anomalies. The goal is algorithm developments to make the system smarter over time (e.g., statistical expectation for N concrete trucks at Dorchester County SC weigh station between time T and $T+t$ on day D, versus no such vehicles). Such data can be used at mobile or relocatable deployments (e.g., sort or target POVs for inspection in an orderly manner), including:
- Software agent technology for analysis of data in disparate databases;
- "OnStar" type detection in remote patrol vehicles;
- Pattern recognition from multiple sensors;
- Multiple anomaly limits to enable a graded approach for inspections;
- Use of human-factors data in the decision-making process for inspections;
- Use of multiple applications for security, safety, and law enforcement.

5.5. INTEGRATED TRUSTED CORRIDOR WEB DEVELOPMENT

A key deliverable of the SETCP work is a prototype web-based application for data acquisition and storage, information analysis and distribution, and easy access for authorized users. We envision that initial prototype development would involve demonstration for the southeastern region with subsequent extension to nation-wide service. The prototype features include:
- Input to and approval by cognizant Federal, state, and local agencies;
- Complaint with privacy act requirements;
- Scalable, plug-and-play capable, and user friendly;
- Self diagnostic;
- Compartmentalized security;
- Redundant;
- Forensic capabilities;
- Easy integration with existing systems at the Federal, state and local levels.

6. PROCEDURES AND PROTOCOLS

No CFR-rulemaking procedure is in place now for DHS requirements. Consequently, confusion exists about promulgation of DHS requirements to the states and localities. Figure 30 shows the model that DHS presently uses. This confusion is compounded by multiple DHS requirements that are technology dependent and require modifications of existing regulations by DOT (49CFR), NRC (10CFR), the U.S. Department of Agriculture--USDA (7CFR), and EPA (40CFR). State agencies currently have responsibility for their own Homeland Security missions with the exception of WMDs, especially Rad/Nuc types.

Figure 30. Historical model for flow-down of DHS requirements.
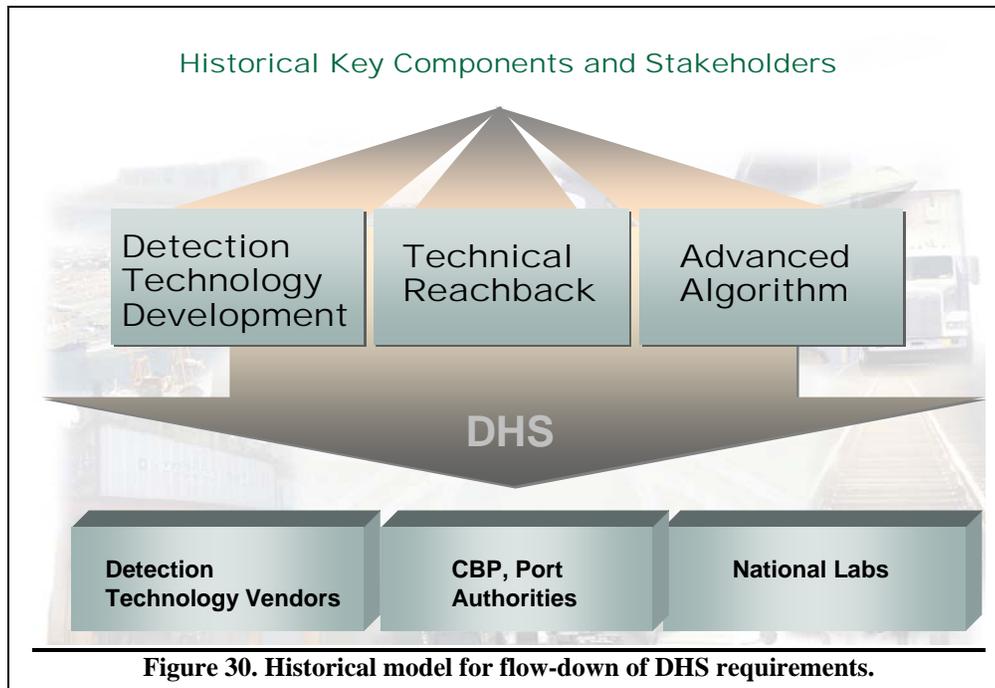
6.1. STATE/LOCAL ROLES VERSES FEDERAL ROLES FOR INTERDICTION AND ENFORCEMENT

State enforcement of Rad/Nuc requirements traditionally focuses on regulations, emergency preparedness, and safety. The states view Rad/Nuc interdiction as a Federal issue. Consequently, immediate steps are needed to define local, state, and Federal roles in Rad/Nuc interdiction, including:

- DHS' role in detection of Rad/Nuc material in transportation;
- State/local role in detection of Rad/Nuc material in transportation;
- Current regulatory requirements that drive DHS needs;
- Gaps in the current regulations that may inhibit DHS Trusted Corridor deployment;
- Compliance with existing safety/regulatory standards for deployment of DHS pilot technology;
- Identification of political barriers to success, versus legal or commercial barriers;
- Initial deployment in leadership states under corresponding policy and procedures;
- Deployments to meet DHS needs with proven technology under present administrative approval.

An example of the last item is RFID sorting and satellite tracking.

6.2. LEGAL ISSUES

Legal issues have confounded many DHS deployments. The issues are manifold: inhibition of research, confusion on interdiction and enforcement authorities, lack of guidance about liability responsibilities, enforcement personnel safety, privacy act limitations, and protection of proprietary information from the private sector. Moreover, potential security classification issues create real and perceived barriers to information sharing, due to ongoing evolution of DHS integrations, multiple agency participation, and emerging knowledge discovery applications. The issues for resolution involve DHS inspection technologies, concurrence among local/state/Federal agencies and private partners, include:

- Interpretation of Price-Anderson legislation, regarding participation of private partners;
- Search-and-seizure restrictions for multiple-enforcement purposes at non-border deployments;
- Use of independent, secure DHS networks for data collection and sharing;
- Security-classification guidance (e.g., information/technology combinations);
- Safety guidelines (e.g., CBRNE training and personal dosimetry) and inspection procedures;
- Regional technical assistance centers for questions (e.g., technology, CBRNE, personnel safety);
- Protocols for vehicle/personnel detention with more formal analysis by reachback SMEs.

6.3. IDENTIFY AND ENGAGE KEY INDUSTRY PARTNERS

The restriction of "law enforcement only" creates large hurtles for establishing a SETCP surveillance network for interdiction and technology deployment within the current legal framework. Other agencies with public safety and security missions rely primarily on administrative controls with minimal reliance on technology advances over the past twenty years. These administrative controls were developed jointly by the regulators, the enforcement community, and the regulated industry. Regulatory modifications are needed to lower costs, increase productivity, and provide better enforcement via modern technologies. Technology developers and regulated industries are interested in pursuing regulatory changes. DHS is in a unique position to drive this paradigm shift in the national regulatory model. Key partnerships are needed with the industrial community, including:

- Transportation (e.g., carriers, shippers, packaging manufacturers, value-added-service providers, and intermodal facility operators);
- Manufacturers and users of NORM with consistent nuisance alarms;
- Medical- and industrial-radioisotope manufacturers and users;
- Commercial tracking industries (e.g., PrePass®, SpeedPass and Qualcom).
- Hazardous and solid waste industries;
- Information technology providers (e.g., data management, technology integrators).

6.4. ESTABLISH PILOT PROCEDURES THROUGH INTER-DEPENDENT STATE/LOCAL DEPLOYMENTS

DHS pilot deployments involve tight central control over procedures and protocols. Typical deployment locations are at ports, large cities, and borders under by Federal control. These deployments have required minimal relationships with other Federal and state agencies that promulgate and enforce safety and security requirements for interstate commerce. Consequently, DHS procedures and protocols at these deployments impose central control over enforcement, legal, and safety issues. In some cases, this central control is either too rigid for interstate deployments. In other instances, this control does not provide independent enforcement agencies with adequate guidance about the DHS security plan. State and local authorities have plans (e.g., inspection, enforcement, training, exercises) for industrial and transportation accidents. However, they are inadequately prepared for nuclear incidents. Figure 31 depicts the need for a highway/state police deployment strategy that includes:

- Fixed deployments at transportation inspection/interchange points for baselining;.

- Relocatable/mobile deployments to migrate the procedures and protocols to remote locations;
- Development of multi-functional operating procedures for exportable to similar entities;
- Harmonizing procedures across states and localities to minimize public/private impacts;
- Encouragement of "cookie-cutter" integration and technology products for state/local needs.

Figure 31. Procedural issues for phased SETCP deployment.
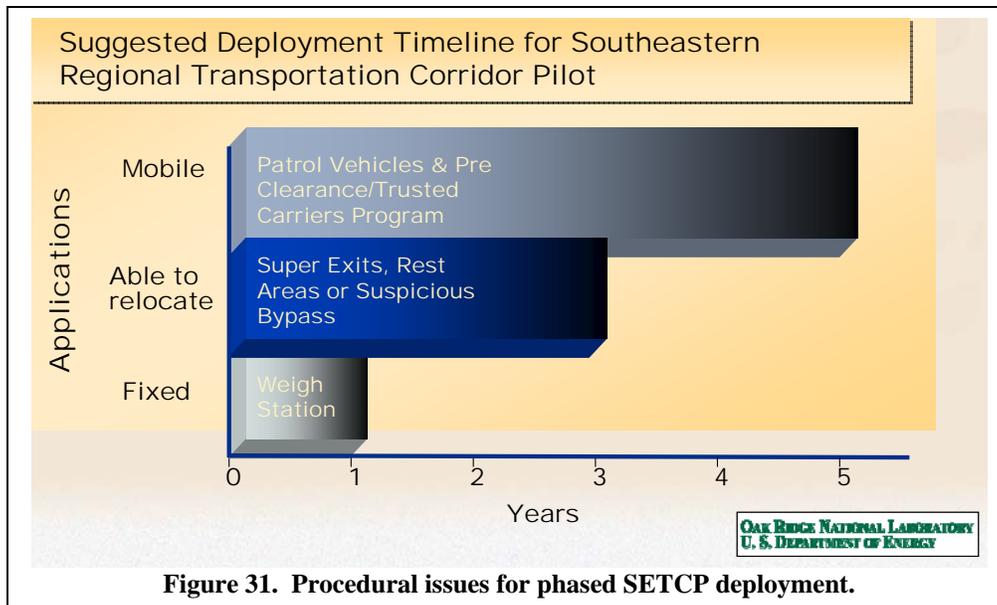
6.5. POLICY FOR DHS REGULATORY DEVELOPMENT

Four key players exist in the transportation arena that impact state enforcement and policy. These same players also regulate the private sector's use of state transportation resources. The specific agencies are DOT, NRC, EPA, and USDA, which have regulations that states must follow for compliance with interstate commerce laws. Compliance is a requirement for continued Federal funding for respective state programs. These agencies also have security requirements in their regulations. Although homeland security is a part of the state missions, Congress has assigned the primary homeland security role to DHS, which must now determine requirements where gaps exist. Rad/Nuc incidents are such area, as an excellent candidate to begin this policy development. All public and private stakeholders must have input in this promulgation process, including:

- Gaps in current regulations;
- State resources/expertise for the mission
- Impacts on the private sector;
- Impacts on interstate commerce;
- Impacts on public safety;
- Impacts on privacy issues;
- Technology advances;
- Deterrence;
- Cost.

6.6. INDUSTRY PARTICIPATION

Figure 32 depicts key stakeholders that will be affected by changes in DHS policy and procedures. Consequently, the promulgation of new regulatory requirements must have industry participation. Standardized security requirements are needed for state compliance, although DHS does not need to codify its own security regulations. Industry will push for this position, while seeking traditional regulatory models as a means of enforcement, including:

- Trusted carrier or shipper programs;

30

- Protection of proprietary data;
- Sensitivities associated with misuse of data;
- Reduction of transit time/delays with improvements in current safety/law enforcement;
- Integration with current tracking systems such as PrePass™, NORPASS and EZ Pass;
- State-driven enforcement standards.

Figure 32. Stakeholder interactions for promulgation of new regulations.
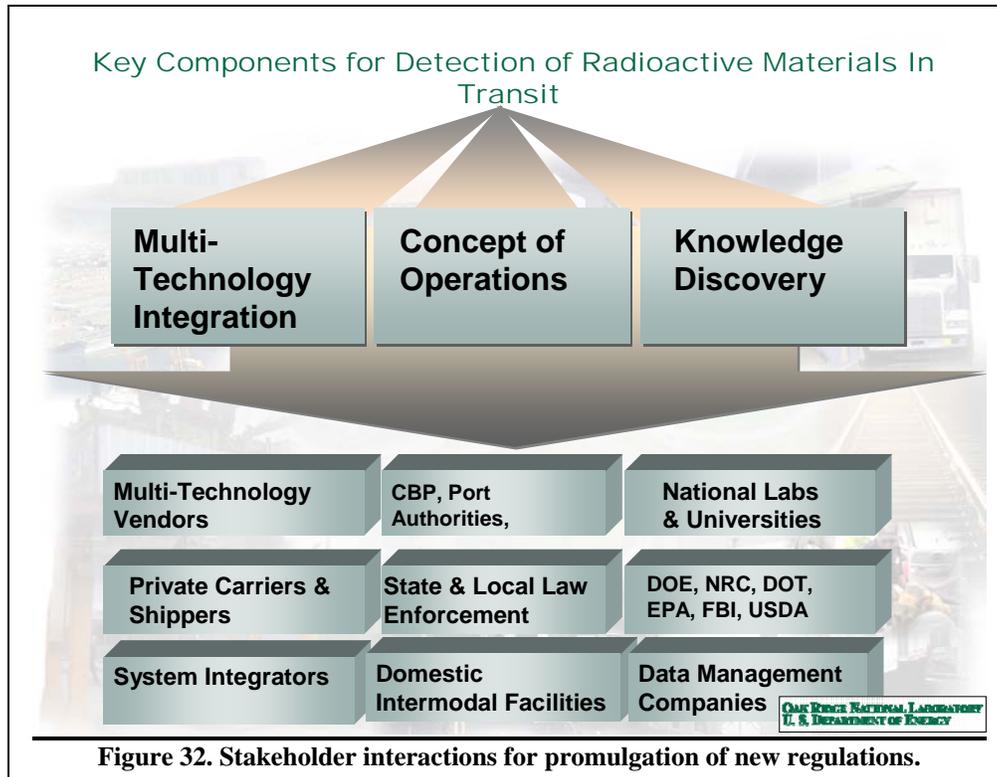
6.7. REGULATORY HARMONIZATION AMONG DOT, DHS, EPA, AND NRC

The primary cognizant agencies for regulation of interstate transport are DOT, EPA, NRC, and USDA, as discussed above. All of these agencies have regulations that have been harmonized with the others by incorporation in and references from 49CFR (DOT). This fusion of requirements typically takes place at the state level, due to strong needs for standard regulations for simplified enforcement, including:
- Common regulation from mutual requirement development;
- Data needs for common regulatory enforcement;
- Harmonization of long-range strategic plans with congressional feedback;
- Identification of gaps in DHS requirements for Homeland Security under current requirements.

6.8. IDENTIFICATION OF TECHNOLOGY CANDIDATES FOR CODIFICATION

New technologies have appeared, since the promulgation of the original transportation regulations. See Figure 33 for examples. These technologies are helpful to both the regulators and those regulated. Additional technologies need to be identified with sufficient maturity and acceptance to warrant regulatory changes for their use. Examples include:
- RFID technology;
- Satellite tracking technology;
- Integrated-scale/radiation-detection technology;

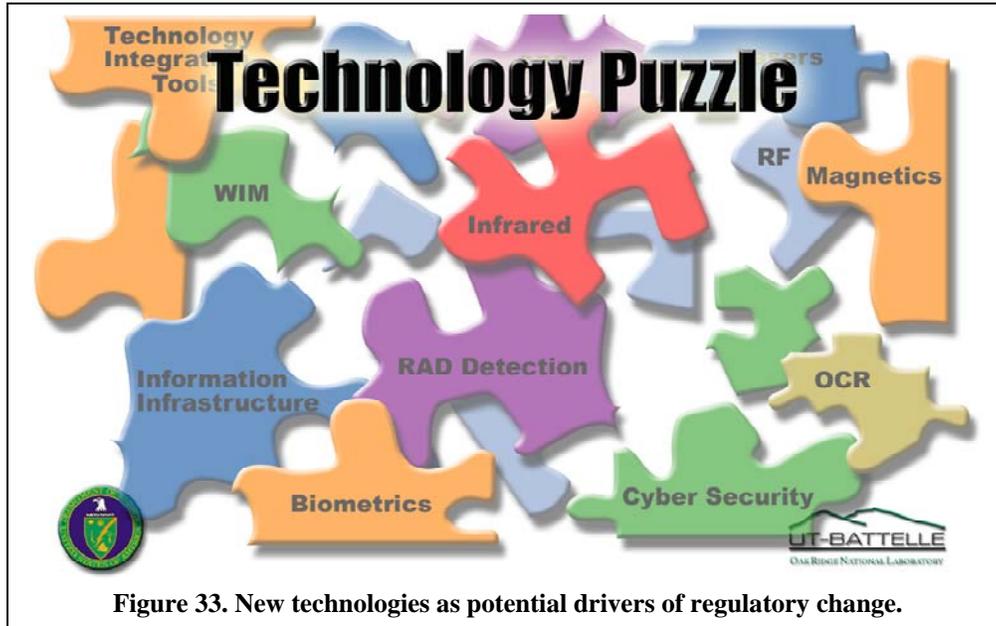- Information and knowledge management technology.

Figure 33. New technologies as potential drivers of regulatory change.

7. SUMMARY

Present work on the Trusted Corridor Project is driven by state police operations (KY, SC, TN) for safety compliance and law enforcement. These deployments involve multiple sensors for automated data acquisition (e.g., vehicle characterization and license number, driver's license, RF identification, radioactive and chemical emissions, overly hot truck components for safety). DHS is interested in this work as a prototype for detection of INDs and WMDs on interstate highways. The most important aspect of this dual-use effort is awareness and training among the affected local, state, and Federal agencies; this training is active and ongoing. The second component of this work is the concept of operations, which automatically characterizes the vehicle, cargo, driver, and carrier via the state-of-the-art sensors. An important issue in the light of DHS needs is frequent, nuisance alarms from naturally occurring radioactive materials (e.g., ceramic tile, tobacco, kitty litter). Consequently, ORNL has developed a draft protocol for response to radiation alarms that is now in use in TN. The third component of this effort is extraction of useful information from the deluge of data, involving comparison of new observations to baseline data for safety, law enforcement, anomalies, and follow-up. The fourth component of this effort is sharing of the local data with regional (and national) collaborators, involving database development, advanced software for analysis of data from many sensors, and network communications. The fifth component is harmonization of the regulations, procedures, and protocols among the local, state, and Federal partners (e.g., regulators, National Laboratories, DOE, DHS), together with commercial stakeholders (e.g., sensor vendors, shippers/carriers, truckers, radioisotope manufacturers). The use of modern sensors and data integration is the essential feature across all of these components.

APPENDIX A

SUMMARY OF IEEE (HAZMAT) STANDARD 1512.3-2002

APPENDIX A. SUMMARY OF IEEE (HAZMAT) STANDARD 1512.3 - 2002

IEEE Standard 1512.3-2002, "Hazardous Material Incident Management Message Sets for Use by Emergency Management Centers" describes a system of information exchange during transportation-related incidents that involve hazardous material (HAZMAT). A typical incident entails an unintentional HAZMAT release from a transport vehicle on or near a roadway. These messages are primarily for use among HAZMAT responders (on- and off-site) and any other supporting agencies (e.g., state and local police). This standard also provides the communication framework between responders at the incident site and off-site databases, including a method to coordinate the complex decision support process for incident response. These messages support communication of the (often incomplete) information to, from, and among off-site databases. This information can come from several sources, including shippers, carriers, on-site documentation and observations, and fleet/freight management centers. Typical information in these messages includes:

- Incident details (e.g., type, location, vehicle damage, injuries, releases, traffic condition);
- Verification of information;
- Specific cargo in the vehicle(s);
- Hazardous materials (e.g., chemicals/waste, radioactive material, physical form, amounts);
- Center for coordination of incident response (e.g., name, location, commander, points of contact);
- Plan for HAZMAT control/confinement/cleanup;
- Real-time inter-agency management of an incident;
- Support needs (e.g., traffic control, fire control, evacuation of injured personnel, detours);
- Termination of the incident response.

The messages in the HAZMAT Standard work in conjunction with the Base Standard; the two standards must be used together for useful exchanges of information. The HAZMAT Standard is compatible with the other standards in the IEEE-1512 family.

This standard supports the communication of information about a HAZMAT incident via structured messages, data frames and data elements. Two functions must be performed to satisfy this mission.

1. Retrieve further information about what the cargo and/or contents is, based on what are often quite partial cues available on site. That information is available in off-site databases managed by shippers, carriers, and Fleet and Freight Management centers.

2. Retrieve information about the characteristics of the cargo and/or contents that is important for incident management, such as toxicity, flammability, danger of explosion, size of a potential toxic plume, environmental damage, recommended set-back distances, and evacuation areas.

These functions lead to the following three requirements for the system of messages, data frames and data elements in this standard in concert with the Base Standard:

1. Messages or sets of messages about the cargo and/or contents from on-site cues and/or from a remote information source. Examples of on-site cues include: statements by the driver, vehicle placard(s), package label(s), and the shipping papers. Database information can be very general (e.g., mapping from package labels to contents types), or very specific (e.g., details from the shipper).

2. Messages or sets of messages that describe the cargo and/or contents to a remote hazard-management database, and retrieval of data on how to manage any cargo/content-related hazards. The cargo/contents information can range from quite cursory, such as the first on-site cues, to quite complete, such as the complete information from the shipping papers or from the shipper.

4. *Messages or sets of messages that are broadcast from the vehicle. Those messages may be broadcast automatically by the vehicle (e.g., triggered by on-board cues indicating an incident, including cues indicating leakage), or upon an action by the vehicle driver. In either case, the message can be transferred to some (or all) of the network of nodes that conform with the IEEE-1512 family of Standards.*

Table A-1 shows the seventeen functional requirements (FR) as an unambiguous basis for determining that the messages, data frames and data elements in this standard satisfy the above three requirements.

Table A-2 shows the ten required information types (RIT), much like the FRs, except limited to the information type required for each FR. The parts of the FR that extend beyond the RIT can be addressed by the way the message is labeled and defined. Tables A-3 through A-5 provide additional details.

Table A-1: Functional Requirements (FR) for IEEE Standard 1512.3-2002, "Hazardous Material Incident Management Message Sets for Use by Emergency Management Centers"

FR1: Vehicle/cargo information observable from outside the vehicle, or from external observation of cargo containers, but not shipping papers, to an external database for retrieval of more detailed information about the cargo. The message is a request for information from the external database.

FR2: Vehicle/cargo information available from any typical vehicle shipping papers, to an external database for the purpose of retrieving more detailed information about the cargo. As such, the message constitutes a request for information from the external database.

FR3: HAZMAT and other building contents information observable from outside the building, or by observing package units, not records, to an external database for the purpose of retrieving more detailed information about the contents of the building that may be of particular interest for incident management. As such, the message constitutes a request for information from the external database.

FR4: HAZMAT and other building contents from records inside the building to an external database for the purpose of retrieving more detailed information about the contents of the building that may be of particular interest for incident management, such as SARA Title III Community Right-to-Know (CR2K) information. As such, the message constitutes a request for information from the external database.

FR5: Queries from off-site databases about on-site observable data, of the type specified in FR1 through FR4. An off-site cargo database system may want to query on-site personnel about observable data.

FR6: Responses (of the type in FR1 through FR4) to queries specified in FR5 about observable data.

FR7: Requests for detailed hazmat or non-hazmat cargo information, while providing information of the type specified in FR1 through FR4 or a more detailed level based on a database lookup. These requests differ from the requests specified in FR1 through FR4, in that they may come from another database rather than on-site. That is, on-site data could be communicated to one off-site database for one level of information, via communication specified in FR1 through FR4; then the results of that database lookup could be used to query a more detailed database via communication specified in FR7. This FR is included to cover the situation where the information sequence may start with data available on site (FR1 to FR4), then go to one database to be supplemented, and then go to a second database for further information.

FR8: Vehicle/cargo or building contents information from a database look-up in response to queries of the type specified in FR1 through FR4 and FR7. This information is at a more detailed level than the information carried in FR1 through FR4 and FR7. For example, the querying information might be at the level of types of mixtures, while this more detailed information might include actual concentrations.

FR9: Requests for hazard management information, including data of the type in FR1 through FR4, FR7 and FR8 as a basis for that. Not keyed to the actual leak/spill situation (for that, see FR11 to FR12).

FR10: Hazard management information from a database look-up in response to queries specified in FR9.

FR11: Requests for hazard management information specific to the actual situation, while providing data of the type specified in FR1 through FR4, FR7, and FR8.

FR12: Hazard management information for the actual situation of hazardous materials, leaks, spill pool sizes, and potential/actual hazards that is provided in response to queries specified in FR11.

FR13: Requests for current status information on the incident particular to cargo/content.

FR14: Current status of the incident about cargo/content, that is provided in response to FR13 queries.

FR15: Requests for static document information, such as the Emergency Response Guide Book.

FR16: Static document information in response to requests as specified in FR17.

FR17: Mayday-like messages (e.g., transmitted automatically from a vehicle, or by the driver command.

Table A-2: Required Information Types (RIT) for IEEE Standard 1512.3-2002, "Hazardous Material Incident Management Message Sets for Use by Emergency Management Centers"

RIT1: Vehicle/cargo information observable from outside the vehicle, or from external observation of cargo containers, but not shipping papers.

RIT2: Vehicle/cargo information available from any typical vehicle shipping papers.

RIT3: Building HAZMAT and other contents information observable from outside the building, or by observing package units, not records.

RIT4: Building hazmat information obtainable from records inside the building.

RIT5: Vehicle/cargo or building contents information retrieved from a database look-up in response to queries based on information types RIT1 through RIT4. This information is at a more detailed than RIT1 through RIT4. For example, the querying information (RIT1-4) might be at the level of types of mixtures, while this more detailed information (RIT5) might include actual concentrations.

RIT6: Hazard management information, keyed to the types of materials but not keyed to the actual situation (for that, see RIT7).

RIT7: Hazard management information specific to the actual incident leak/spill situation.

RIT8: Current status information of the incident particular to cargo/content.

RIT9: Static document information.

RIT10: Mayday-like (telematic) messages, i.e., telematics messages automatically transmitted from an involved vehicle, or transmitted upon a command action by the driver. This is intended for special telematics messages particular to HM carriers, as opposed to "civilian" telematics.

Table A-3: Base Standard for Message Sets under IEEE Standard 1512-2000, "Common Incident Management Message Sets for Use by Emergency Management Centers"

Status Message Set	Acronym	Subclause
Incident Description	IDX	5.1.1
Public Incident Description	PID	5.1.2
Request Information	RIN	5.1.3
Incident Management Message Set		
New Incident Event	NIE	5.2.1
Split Incident Event	SIE	5.2.2
Merge Incident Event	MIE	5.2.3
Close Incident Event	CIE	5.2.4
Poll for Hand Off	PHO	5.2.5
Available for Hand Off	AHO	5.2.6
Request Hand Off	RHO	5.2.7
Grant Hand Off	GHO	5.2.8
Request Verified Incidents	RVI	5.2.9
Request Unverified Incidents	RUI	5.2.10
Center Management Message Set		
Establish Center On-Line	ECO	5.3.1
Disable Center On-Line	DCO	5.3.2
Establish Center Properties	ECP	5.3.3
Change Center Properties	CCP	5.3.4
Request Center Plans	RCP	5.3.5

Table A-4: Public Safety Message Sets for IEEE Standard 1512.2-2004, "Public Safety Incident Management Message Sets for Use by Emergency Management Centers"

	Acronym	Subclause
Warning Information		4.4
Advise All Personnel: Immediate Site Evacuation	ISE	4.4.1
Request Immediate Emergency Assistance	RIA	4.4.2
Publish Cautions for Responders	CFR	4.4.3
"Watch For" Cycle		4.4.4
Publish "Watch For" Message	WCH	4.4.4.1
Respond to a "Watch For" Message	RWF	4.4.4.2
Situation Awareness		4.5
Inform of Need For . . .		4.5.1
Law Enforcement	INL	4.5.1.1
Emergency Medical Services	INM	4.5.1.2
Rescue	INR	4.5.1.3
Fire Suppression	INF	4.5.1.4
Other Response	INO	4.5.1.5
Track Persons and Vehicles		4.5.2
Track Involved Persons	TIP	4.5.2.1
Track Response Personnel in Special Circumstances	TSC	4.5.2.2
Track Response Personnel On Site	TRP	4.5.2.3
Track Witnesses	TWT	4.5.2.4
Track Involved Vehicles	TIV	4.5.2.5
Publish Differential GPS Information	DGC	4.5.3
Plan Dissemination		4.6
Publish Zone Information	ZON	4.6.1
Publish Incident Action Plan, Mgmt Command Structure	MCS	4.6.2
Inter-Agency Asset Mgmt: Inventory Location, Status	UAI	4.7
Asset Linking		4.8

Table A-5: Traffic Management Standard Message Sets for IEEE Standard 1512.1-2002, "Traffic Incident Management Message Sets for Use by Emergency Management Centers"

	Acronym	Subclause
Request and Share Information about Work Zones		4.2
Request Work Zone Description	RZD	4.2.1
Work Zone Description	WZD	4.2.2
Request Local Traffic Control	RTC	4.3
Describe Local Traffic Control Plan	DTC	4.4
Share Information about Ingress/Egress Routes, and Route Services		4.5
Request Route Advice/Services	RRA	4.5.1
Offer Route Advice/Services	ORA	4.5.2
Share Location/Priority/Preemption Information on a Response Vehicle		4.6
Request Location/Priority/Preemption	RLP	4.6.1
Share Location/Priority/Preemption	SLP	4.6.2
Information on Clean Up/Infrastructure Repair: Need/Plans		4.7
Need for Clean Up/Infrastructure Repair	NCI	4.7.1
Clean Up/Infrastructure Repair Plan	CRP	4.7.2
Request Network Conditions/Route Status	RNC	4.8
Share Information on Asset Management		4.9
Ask for Assets	AFA	4.9.1
Respond to Request for Assets	RAA	4.9.2
Request Asset Status	RAS	4.9.3
Asset Status	AST	4.9.4

INTERNAL DISTRIBUTION

1. R. K. Abercrombie
2. F. A. Denap
3. B. L. Gorman
4. I. G. Gross
5. D. E. Hill
6. L. M. Hively

7. C. M. Smith
8. R. M. Walker
9. J. D. White
10. Central Research Library
11. ORNL Laboratory Records - RC
12. ORNL Laboratory Records - OSTI