

Development of a Common Data Highway for Comprehensive Incident Management

**James J. Kulesz
Oak Ridge National Laboratory**

April 29, 2003

Abstract

There is an escalating potential that chemical, biological, or radiological events could occur on the continental United States (CONUS) or outside the continental United States (OCONUS). For this reason, Oak Ridge National Laboratory proposes to develop the SensorNet system. The objective of this effort is to build an information technology and communications infrastructure that can serve as a common data highway for comprehensive incident management. With proper design, the SensorNet backbone can be used as a consequence management system to rapidly respond to a chemical, biological, or radiological event. By strategically locating and connect remote sensors on existing commercial and government infrastructures, critical information can be sent to a command center within minutes of an event. The ultimate goal of the system is real-time, reliable, and secure transmission and processing of data and information for the accurate prediction of the event location, identification of the threat, its directional path over time, and the number of people that could be affected. By receiving this information on an almost real-time basis, the command center can immediately dispatch first responders to the event area. Provided with detailed information from the SensorNet system, the effectiveness of the first responders will be greatly enhanced. They will know the exact agent involved and immediately execute the appropriate treatment. Also, areas in the projected path of the release can be evacuated in advance. To meet the objectives of this effort, ORNL has developed strategic partnerships with the National Oceanic and Atmospheric Administration (NOAA), the commercial telecommunications and data processing industries, and government and commercial sensor developers.

I. Introduction

In the wake of the events of September 11, 2001, the issue of homeland security has arisen to the forefront of the nation's consciousness. There is an acknowledged need to protect military installations, government facilities, business enterprises, and private citizens from the occurrence and effects of terrorist related incidents. In order to provide this protection, the acquisition, assimilation, correlation, fusion, and presentation of tremendous amounts of information must be accomplished in a timely and expeditious manner for the appropriate authorities.

Shortly after September 11, 2001, ORNL developed the SensorNet concept. When fully developed, SensorNet will be the Information Technology (IT) infrastructure of a national system for comprehensive incident management in cooperation with state and local governments. This IT infrastructure will provide a common data highway for a comprehensive set of homeland-security sensors that includes, but is not limited to,

Chemical-Biological-Radiation-Nuclear-Explosive (CBRNE) sensors, meteorological instruments, and other sensors (i.e. video cameras, air quality, environmental, etc.). The SensorNet infrastructure architecture will allow distributed access with multi-level security, information fusion, and a common operational picture. Also, the system must be designed to assure an ultra-high level of reliability, survivability and security, and must be scalable across state, local, and federal governments.

To meet the objectives of this effort, ORNL has developed strategic partnerships with the NOAA, the commercial telecommunications industry, and government and commercial sensor developers. A key to the architecture of this system will be the use of commercial standards to provide interoperability, maintainability, controllability, and upgradeability over a complete range of sensors. SensorNet will leverage the investments and operational expertise of the telecommunications industry.

Figure 1 provides a summary of SensorNet from the perspective of a first responder.

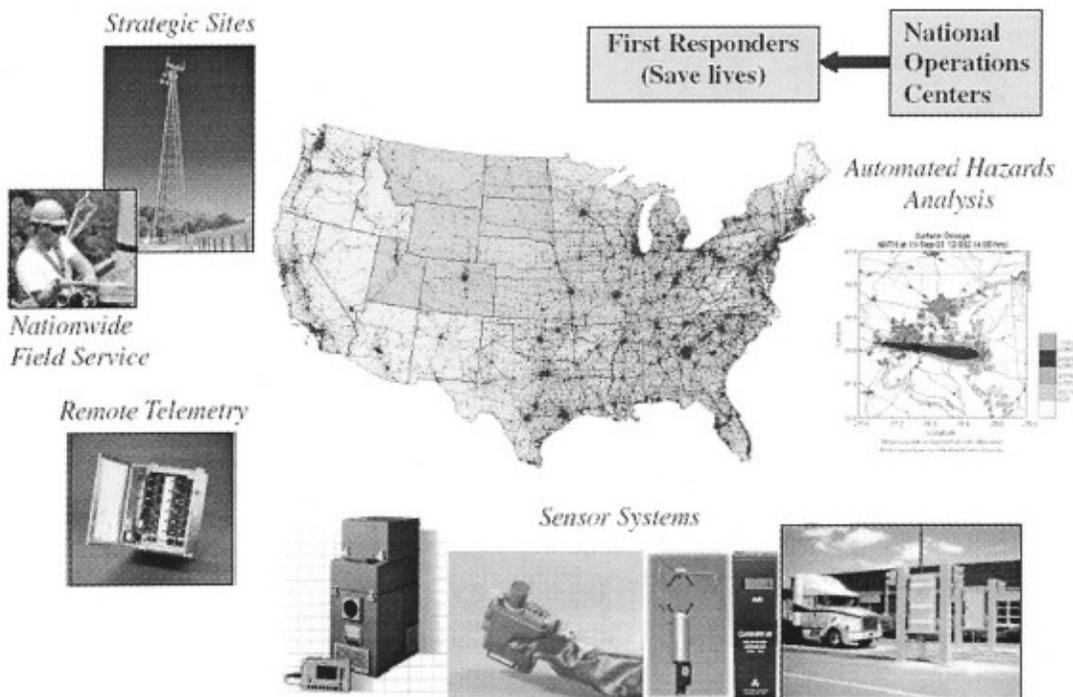


Figure 1. SensorNet – Nationwide Real-Time Detection and Assessment System for Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Threats

Various types of sensors that can measure releases of potentially harmful chemical, biological, and radiological materials are strategically placed on commercial and government infrastructures such as cell towers, roof tops, light poles, police cars, etc. at locations based upon a threat assessment. The sensors include video cameras and meteorological instruments. Robust communications systems can be located at existing structures, such as cell towers and roof tops, that are strategically located to service the population. Coincidentally, the density of telecommunications infrastructure elements, such as cell towers, follows the density in population that one wishes to protect. Also, the

telecommunications industry already has a system for 24/7 monitoring of the functionality of its equipment and the industry can quickly repair the equipment as needed. This existing service is useful for maintenance of SensorNet's distributed sensor network. This frees the end-user from the burden of maintaining the system and assuring its performance. All other components, such as remote telemetry and predictive plume modeling codes also already exist. Thus, one can rapidly install a functioning system that can help first responders and improve the system over time as technology improves. The objective is to be able to detect, identify, and quantify the constituents of harmful releases, convey the information to a location where a predictive plume model can be run, and provide accurate, user-friendly information to a command center for first responders within five minutes of an event.

II. Technical Description

The ultimate goal for SensorNet is to develop a common data highway for comprehensive incident management that provides the following benefits:

- Real-time information direct to the decision-maker
- Immediate identification of the threat
- Immediate predictive assessment of the event over time
- Redundant encrypted communication
- Common operational picture for multiple command centers
- Decision support tools
- Automatic reach-back for national asset response
- Assurance of system operational integrity – 24/7 monitoring
- Data archiving for operational and forensic assessments
- Sensor sites selection based on modeling studies
- Capability to seamlessly upgrade sensors to best in class
- Platform for realistic training

Great care must be taken to develop the appropriate architecture necessary to deploy SensorNet throughout the nation. Such large-scale deployments require a standards-based, open and modular architecture that maximizes participation by the government and private sectors and can seamlessly include new, best-in-class technologies as they are developed. Successful development will alleviate interoperability issues that have plagued many proprietary systems. The primary goals of the currently planned effort are to begin the design and development of this robust architecture and perform small-scale tests to evaluate performance.

A limited timing-test test was performed in March 2002 that successfully demonstrated that, using remotely distributed sensors, one can detect, identify, and quantify release constituents, convey pertinent information to a command center and perform predictive plume modeling within five minutes of interaction of the sensors and release agents. Figure 2 pictorially summarizes the fielded timing-test and Figure 3 gives the results.

SensorNet Timing Test – March 12, 2002

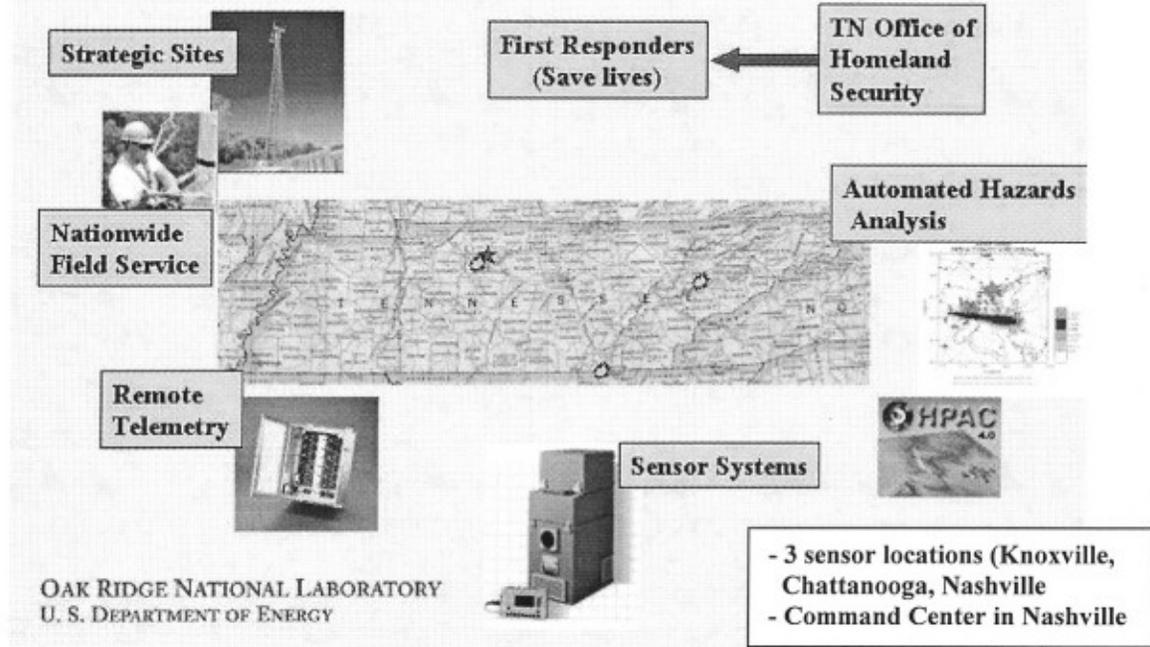


Figure 2. SensorNet Timing Test

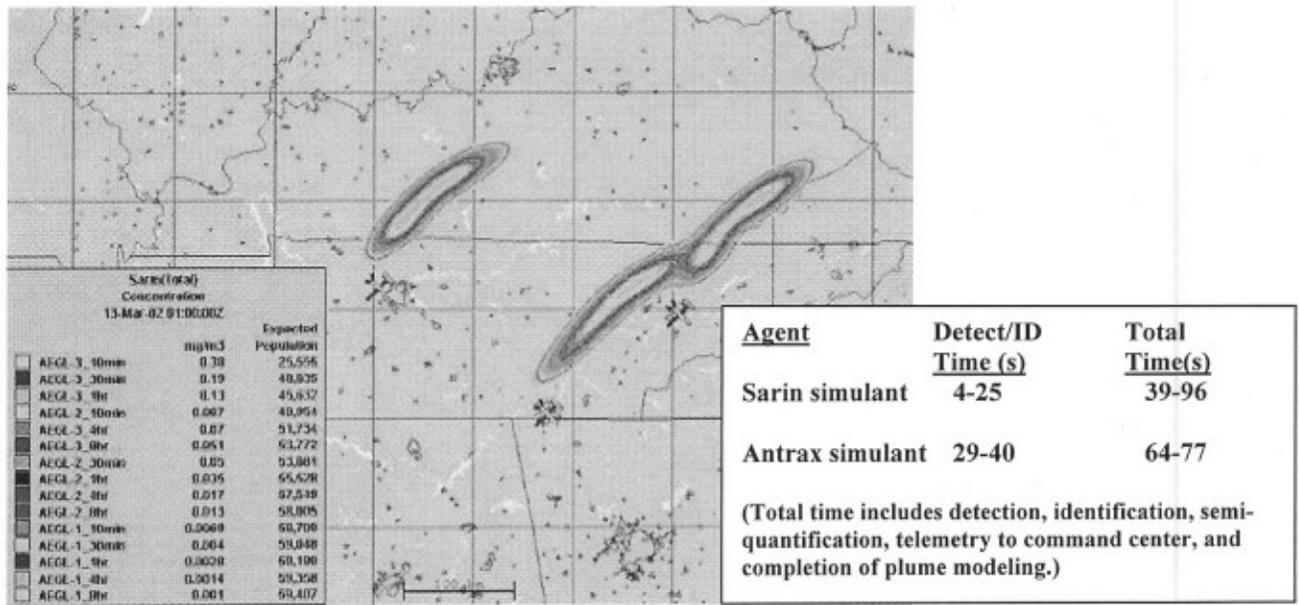


Figure 3. Timing Test Results

Encouraged by these favorable results, the SensorNet team conceptualized a robust, standards-based architecture to enhance system performance and maximize participation by

the private sector. During the summer of 2002, ORNL teamed with NOAA to collocate sensors and enhance the communication and information architecture at NOAA's existing urban test bed in Washington DC. Then, in November 2002, ORNL teamed with a DOE/ORNL team working on the Intelligent Transportation System initiative and created a SensorNet node at the Watt Road Truck Weigh Station on I40 near Knoxville, TN. The next operational test bed will include a broader deployment of SensorNet in East Tennessee.

To meet the overall objectives of SensorNet, ORNL is currently developing the data structures to allow for fusion of information from multiple sources (Figure 4) so that the "system" can proactively respond to changing threat levels and alerts. For instance, using the figure, one can envision that an alert from a law enforcement network to interdict particular trucks and conduct more detailed inspections for transport of radioactive materials can be quickly conveyed to weigh stations and/or other choke points using the SensorNet common data highway.

SensorNet Vision – Providing Knowledge For Action

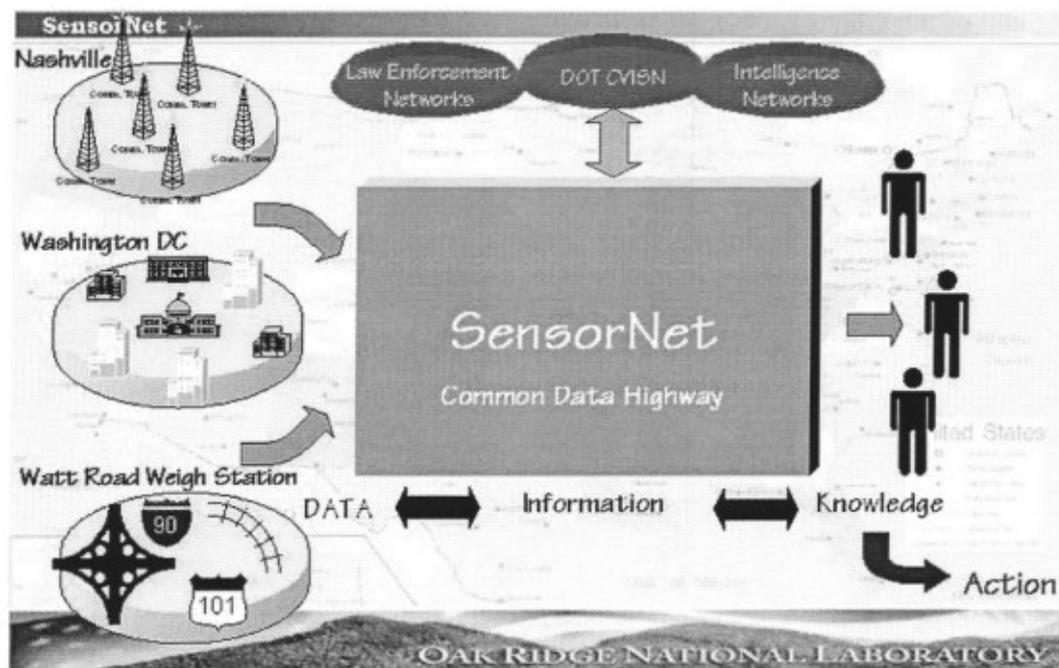


Figure 4. Common Data Highway for Comprehensive Incident Management

III. Developmental Approach

Recent funding from the DoD will allow the SensorNet team to develop the information technology infrastructure and communications architecture for a common data highway to support comprehensive incident management. Initially, we will target communications, secure information flow, information fusion, and data archiving. The design will require a highly adaptable, reliable, and survivable communication system that leverages wireless,

satellite, and fiber commercial and government telecommunications infrastructures. The design must also assure secure information flow. This will include a multi-level cyber security and access control system that can be upgraded as cyber security processes improve. To satisfy the requirements for all concepts of operations, we will design the data management system to accommodate fusion of information from multiple sources. As part of this task, we will also design and implement a distributed data archiving structure for both local and central data archiving necessary to provide reliability and survivability in accordance with the concepts of operation. Some rudimentary activities will also include methods for direct interface to plume modeling software and command/communication center interfaces. Finally, a mechanism for remotely monitoring performance of the system, independent of data feeds to an emergency response command center, will be included in the design and architecture to assure 24/7 system and component maintainability and rapid maintenance.

Specifically, the following will be included:

- **Design Standards Selection**
This will involve personnel who have had experience, especially through participation in standards committees, with recommendation and use of standards.
- **Sensor Interfaces**
The architecture must accommodate preferred sensor standards, such as IEEE 1451, as well as legacy interfaces, such as RS-232. The preferred architecture will revolve around sensor standards that accommodate the treatment of connected sensors as software object. This greatly increases the versatility of the system for sensor monitoring and reconfiguration.
- **Communications**
To assure the integrity of communications, the architecture design will include multiple, redundant means of communication. Communications can include a combination of wireless communications (IEEE 802.11b), ad hoc routing, multiple fiber connections, and satellite communications.
- **Data Processing**
Standards-based protocols and both distributed and centralized processing.
- **Data Storage**
Includes standards-based protocols, distributed storage (at nodes and at collections of nodes), regional storage, and collective, highly centralized storage.
- **Security**
Includes physical, cyber, controlled access, communications, etc. security considerations.

- **Maintenance Monitoring**
Includes the capability to monitor system performance separate from observations at the command center for incident response. This capability is necessary for 24/7 operations during large deployments.
- **Plume Model Interface**
Preliminary efforts to seamlessly incorporate sensor data into plume models for automated plume analysis.
- **Command Center Interface**
Includes the design structure for the command center and the demonstration of the acquisition of key data, the presentation of fused information and the simultaneous dissemination of dynamically restricted information to first responders and key decision makers.

We also plan to develop laboratory and field test beds for this technology infrastructure and communications architecture to determine system performance and scalability. We will prototype hardware and develop interface software. We envision producing semi-portable SensorNet hardware that can be quickly assembled, disassembled, and relocated.

IV. Summary

The Department of Homeland Security and DoD are faced with unique challenges related to CBRNE threats against CONUS and OCONUS installations, as well as the expeditionary forces on land and sea. Rogue nations and terrorist organizations appear willing to wantonly use weapons of mass destruction (WMD) to satisfy ideological objectives. Countermeasures to effectively respond to these threats are limited to preemptive military engagements that can have negative political consequences. However, ORNL is developing a common data highway for interdiction technologies, information fusion, and comprehensive incident management that will incorporate best in class technologies for sensors, communications, data management, security, dynamic predictive plume modeling, and consequence management to allow rapid response and interoperability of military and civilian systems. CONUS and OCONUS facilities must operate within civilian environments. Effective communications and engagement of the emergency response organizations within these civilian jurisdictions, including use of civilian infrastructures, are force multipliers for military and civilian response actions to engage perpetrators and minimize casualties from a WMD event.