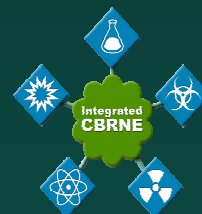


Integrated Chemical, Biological, Radiological, Nuclear and Explosive Program



[HOME](#) | [ABOUT ICBRNE](#) | [DOCUMENTATION](#) | [NEWS & EVENTS](#) | [ICBRNE TESTBED](#) | [CONTACT](#)



Maximizing Safety for First Responders

The ICBRNE program (Integrated Chemical, Biological, Radiological, Nuclear and Explosive Program) is the result of years of work between the [Department of Homeland Security](#) and local first responders and emergency managers to ensure the safety of our homeland. When operated completely, the ICBRNE program protects first responders, as well as the general public, in numerous types of disaster situations, as well as every day use:

◆ Terrorist threats ◆ Chemical releases ◆ Mine explosions ◆
Natural disasters ◆ And more

The Final Report

2010 ICBRNE Sensor Detection Demonstration Program



**Homeland
Security**



Contents

1	Executive Summary	5
2	ICBRNE Vision	5
3	ICBRNE Overview	6
3.1	ICBRNE Accomplishments	6
3.2	Program background: Los Angeles Initial Pilot Site.....	7
4	Concept of Operations and Policy Development	9
4.1	Sensor Instrumentation Overview	11
4.2	Incident Sensor Data:	12
4.3	Sensor Interoperability:	13
4.4	Utilization of the Common Alerting Protocol.....	13
4.4.1	ICBRNE use of CAP:.....	14
4.4.2	Sample CAP	15
4.4.3	CAP and Google Integration	16
4.5	Alerting and Notification	16
5	Tools & Services.....	21
5.1	Wireless.....	21
5.2	Network Devices	21
5.3	Sensor Views	21
5.4	SME Views.....	22
5.5	EM Views.....	24
5.6	Integration of maps.....	25
5.7	Integration with plumes.....	26
6	Regional Information System	27
7	Interoperable Test Virtual Laboratory.....	28
8	Program Solutions & Benefits	28
8.1	Equipment Diversity.....	29
8.2	Instrument Types	30
9	Standards Compliance & Interoperability	30
10	Training.....	31
10.1	Train the Trainer.....	31
10.2	Quick Start Guides.....	31
10.3	Drills/Exercises	31
11	First Responder Safety.....	32
12	Force Multipliers	33
13	Implementation Process.....	33
13.1	Identify Implementer(s)	34
13.2	Perform Instrumentation Inventory.....	34
13.3	Solicit Users to Input Inventory.....	34
13.4	Identify Communications Architecture	34
13.5	Create Budget.....	35
13.6	Identify Funding Source – Short/Long term.....	35
13.7	User/Manager Training	36
13.8	Training – Drills and Exercises	36
13.9	Standard Operating Practices.....	36
	Appendix A - Operation Golden Phoenix (Photos & Press)	38
	Appendix B - OGP After Action Report.....	39



Appendix C - Functional Specification.....	40
Definitions	43
1 General Specification.....	45
1.1 Overview	45
1.2 First Responders	45
1.3 Subject Matter Experts	45
1.4 Emergency Management & Command Operations	46
2 Information System Architecture.....	47
2.1 General Network Data Security Policy Requirement.	47
2.2 Encryption Standards Compatibility Policy Requirement	47
2.3 Standard Data Telecommunication Protocol Policy Requirement	47
2.4 Third-Party Applications & Systems Data Sharing Policy Requirement	47
2.5 Wireless Interoperability.....	47
2.6 Geographic Information Systems	48
2.7 Data Repository & System Logs	48
3 System Apparatus & Infrastructures	48
3.1 Mobile Transmission Appliances	48
3.1.1 User Interface & Operation	48
3.1.2 Meter Interface Options	49
3.1.3 Wireless Network Requirement Specification	49
3.1.4 GPS Receiver Requirement Specification.....	49
3.1.5 Power Source and Sustained Operation Requirement Specification.....	49
3.1.6 Meters May Be Modified	49
3.1.7 Physical Characteristics	50
3.1.8 Thermal Tolerance Requirement Specification.....	50
3.1.9 Meter Compatibility List.....	50
3.2 Gateways, Bridges, Routers, and Third-party Appliances	51
Appendix D - Testbed Frequently Asked Questions (FAQs)	52
1. What are the challenges of information sharing during an emergency?	52
2. What is interoperability?.....	52
3. How do we achieve interoperability?	52
4. What is the Interoperability Testbed?	52
5. How can I join the Interoperability Testbed?.....	53
6. What security features are available on the ICBRNE Testbed?	53
7. What types of information are important for Emergency Management?	53
8. Which open standards support Emergency Management?	53
9. What can I do to improve interoperability solutions in my city or organization?	53
10. When should I start addressing these needs?	54
11. What are “open” standards?	54
12. How do I participate in an open standards organization?	54
13. What is OASIS?	54
14. How do I participate in OASIS?.....	54
15. What is EDXL?.....	54
16. How do I use EDXL?.....	55
17. What is the Common Alert Protocol (CAP)?	55
18. How do I create a CAP message?	55
19. How do I put my sensor information into a CAP message?.....	55
20. How do I “GET” CAP messages from the ICBRNE sensors?.....	55



21.	How do I “POST” CAP messages to the ICBRNE Testbed?	55
22.	What is “Representational State Transfer” (REST) and how is it used on the ICBRNE Testbed? 56	
23.	What other data formats are available on the ICBRNE testbed?	56
24.	What do I do to send my message once I've created it?	56
25.	What is the EDXL Distribution Element (DE)?	57
26.	How do I package my CAP message in a DE?	57
27.	How do I post to OPEN?	57
28.	How do I post to Solace router?.....	57
29.	What is the National Information Exchange Model (NIEM)?.....	57
30.	What is the CBRN IEPD?	57
Appendix E - Testbed Templates (SPAWAR Forms)		58
Executive Summary		59
Example Template Forms		60
Question: How to convert Common Alerting Protocol v1.2 (CAP) message to Emergency Data Exchange Language (EDXL) Distribution Element (DE) format?.....		60
QUESTION: How to Post Messages to (and Get Messages from) DM OPEN?.....		65
QUESTION: How do you develop a Testbed for ICBRNE?		74
QUESTION: How do you create an “Energy Gradient” overlay using ICBRNE sensor data?		76
QUESTION: How do you “get” alerts (using the RESTful interface)?.....		80
ANSWER IN BRIEF:		80
QUESTION: How do you use the Safe Environment Engineering GET Realtime data feed?		81
14	Appendix F - Current Software Participants	106
Instrumentation Participants		108
15	Appendix G - Instrumentation Interfaces.....	110
Appendix H - Virtual Golden Phoenix Overview		114
(1) Sensor Management System		115
(2) DE Routing Test.....		116
(3) EDXL Standards		117
(4) N25 (CBRN IEPD) & DE Routing.....		118
(5) Integrated Chemical Biological Radiological Nuclear and Explosive Detection Demonstration Program (ICBRNE)		119
(6) Disaster Management (DM) Open Platform for Emergency Networks (OPEN)		120
(7) Integrated Public Alert & Warning System.....		121
(8) C4ISuite		122
(9) SAVIEW		122
(10) IC.NET.....		123
(11) Interoperable Wireless Hazmat Sensors.....		124
(12) EDXL DE & Geospatial Routing.....		125
(13) Virtual Interoperability Testbed		126
(14) Virtual USA.....		127
(15) SAGE.....		128
(16) Command Responder		128
16	Appendix I – Training Materials.....	130
16.1	ICBRNE Alert Quick Start Guide.....	130
16.2	Testbed Demo Training	131
16.3	MultiMeterViewer Quick Start Guide	136
16.4	Lifeline Gateway and LINC Operation	141



1 Executive Summary

The goal of the Integrated Chemical Biological Radiological Nuclear Explosive (ICBRNE) detection demonstration program is to educate, explore, test and develop improved interoperability of emergency information using standards. The ICBRNE process enables multiple organizations from various jurisdictions, each using their own chosen tools and standards, to work together to manage emergencies more effectively and save lives.

This report provides in its short 15 page introduction the primary lessons learned and guidance for other cities or organizations who may wish to understand the essence of the project and how to replicate this information sharing process to achieve similar benefits in their own region. The report details the merits of the program both from the perspective of increased safety as well as cost/time savings. The Program's architecture will be explained including how CBRNE data is integrated with appropriate policy, alert notifications, scalable visualizations and associated contextual information within a standards-based framework. In addition, the introduction references a full suite of Appendices for drill-down information and points of contact, including links to information and software sufficient to replicate and standup the entire ICBRNE process as needed. Cities also have the option to participate, with no additional effort, in the ongoing ICBRNE capability established in the Los Angeles region. Please read this introduction and if you are interested, you are welcome to join the ongoing DHS and Los Angeles initiatives, including the Interoperability Test Virtual Laboratory (ITvL) at <http://www.icbrne.org>. Here you will find an online version of the report, with all of the live links to materials and points of contact from the Appendices. Any fixes or corrections or updates to these materials will be found there. The ITvL mission begins with ICBRNE sensors and extends the capability throughout the entire family of Emergency Data Exchange Language (EDXL) data sets, including Hospital Availability (HAVE), Alerting (Common Alert Protocol), Resource Messaging (RM), Situation Reporting (Sitrep) and Patient Tracking (TEP). The ICBRNE Project is a proven process for sharing sensor readings, detections and detection-based information across local, regional, state, tribal and federal organizations for more efficient and effective emergency management.

The operational pilot in Los Angeles, California demonstrated that readings from over 500 sensor devices could be shared in near real-time with more than 40 regional partners in the Los Angeles area, across a multitude of commercial, government, local, and web-based visualizations and emergency management toolsets. See Table 1. These sensor readings were used in the Golden Phoenix and Virtual Golden Phoenix exercises in July of 2010 to provide a significantly enhanced level of capability for emergency managers. More than a demonstration, the lessons learned and capabilities are operational in Los Angeles today. In the words of Kathleen Kaufman, Director of Los Angeles County Radiation Management, "The ICBRNE capability is a major advance in information sharing for our region. Now that we have it, we can't live without it."

2 ICBRNE Vision

The ICBRNE vision is represented by three major components:

- (a) Sensors integrated through standards (format & communications);
- (b) Aggregated policies (local, regional, state, tribal and federal) governing exchange of CBRNE (sensor) information; and
- (c) Systems integrated for CBRNE Situational Awareness

Together, these components form an overall vision where emergency management is more efficient and effective because we can all share the same sensor information and the resulting common operational picture in near real-time. Before the ICBRNE Program, the vision was frustrated by the multitude of systems, sensors, and federated governmental entities involved in a large-scale



emergency. The ICBRNE Program overcame these challenges not by trying to eliminate the diversity but by enabling interoperability across the diversity, by establishing an infrastructure supporting and encouraging open standard data formats, open standard communication formats, and conversion as needed between different standards.

3 ICBRNE Overview

3.1 ICBRNE Accomplishments

To appreciate the ICBRNE accomplishments, consider these numbers. The ICBRNE Program enabled access to over 500 integrated instruments, including 170 radiation sensors, 200 chemical, 60 chemical warfare agents, 25 particulate, and 60 GPS instruments. Over 40 agencies in the Los Angeles area were active participants, along with over 14 national entities. The primary participants are shown below in Listing 1.

Los Angeles ICBRNE Participants

- Los Angeles City Fire Department
- Los Angeles County Fire Department
- Los Angeles County Department of Coroner
- Los Angeles World Airport
- Glendale Fire Department
- Long Beach Fire Department
- Port of Los Angeles
- Ontario Fire Department
- Riverside Fire Department
- Los Angeles City Police Department
- Los Angeles County Sheriff Department
- Los Angeles County Health Department
- Burbank Fire Department
- Santa Fe Springs Fire Department
- 9th Civil Support Team

Los Angeles Emergency Management Participants

- Area E Disaster Management Area Coordinator
- Los Angeles County Department of Mental Health
- Los Angeles Department of Health Services
- California Emergency Management Agency
- Los Angeles County Department of Public Works
- Area F Disaster Management Area Coordinator
- US Air Force/Los Angeles AFB
- City of Los Angeles Building and Safety
- Los Angeles County Department of Water and Power
- Pasadena Public Health Department
- LA County Office of Emergency Management
- LA County Public Library
- City of LA Department of Transportation
- Area D Disaster Management Area Coordinator
- Area C Disaster Management Area Coordinator
- Ventura County Public Health
- City of Pasadena
- LAPD - Emergency Operations Division
- Area H Disaster Management Area Coordinator
- Area G Disaster Management Area Coordinator
- InfraGard - Los Angeles
- Los Angeles Internal Services Department
- City of Long Beach
- Getty Foundation
- LA County Probation
- Joint Regional Inelegance Center
- Real-Time Analysis & Critical Response Division

National ICBRNE Participants

- Seattle – East Side, WA
- South King, WA
- Kent, WA
- Port of Seattle
- Renton, WA
- Tuckwila, WA
- 10th CST
- San Francisco
- New York City
- Boston
- State of MA HazMat
- Cambridge, MA
- San Luis Obispo, CA
- US EPA

Primary ICBRNE Participants



The ICBRNE Program participated in 25 exercises and drills and integrated capability across 8 partnering cities including New York, Los Angeles, Glendale, Burbank, Long Beach, Seattle, San Francisco, Boston, and soon to be in San Diego and Washington DC. The ICBRNE Program integrated comprehensive alerts and notification tools with embedded policies for dissemination based on specific instrumentation detections. ICBRNE provided web tools for instrumentation viewing and information sharing collecting and disseminating instrumentation, and a website and interactive wiki that enabled over 15,000 detection readings during the Golden Phoenix exercise. ICBRNE participants led the way in the promotion and development of OASIS Emergency Data Exchange Language (EDXL) standards, specifically utilizing Common Alert Protocol (CAP) as a core standard format. ICBRNE components were tested for interoperability through the FEMA NIMS program. ICBRNE collaborated with the DHS Domestic Nuclear Detection Office (DNDO) in the enhancement and pilot testing of the CBRN IEPD. The IEPD is a National Information Exchange Model (NIEM) standard message set utilized in the Mission Critical Messaging (MCM) pilot enabling geospatial and policy-oriented routing of sensor information. In short, the accomplishments of the ICBRNE program are numerous and the ICBRNE Program reshaped the sensor-driven emergency management landscape in the Los Angeles region.

3.2 Program background: Los Angeles Initial Pilot Site

The Los Angeles region was selected as the primary site for the ICBRNE pilot due to the many unique and important characteristics of the region, including its importance as a major population center, its world prominence as a commercial and transportation hub, its established sensor infrastructure, and its leadership and proactive approach to information sharing. The ultimate decision was based on a series of selection criteria, which included existing sensor deployment, infrastructure, time and resource availability, and regional impact resulting from a successful deployment.

Los Angeles is a large urban area that supports a population of approximately 10 million people. See Figure 1. The adjacent ports of Los Angeles and Long Beach are the largest seaports in the U.S. handling more than half of the containerized cargo entering the US. The ports also support a large rail and truck transport network, national and international tourism via cruise lines, a large contingent of pleasure craft, and a major Naval installation. The extended Los Angeles area has an international coastal marine border that receives container cargo from many countries including Chile, Colombia, Peru, Ecuador, Mexico, Canada, Japan, China, and Russia.

Los Angeles is a key hub in the transcontinental rail system and is characterized by three primary rail lines which include both freight and passenger rail services. Burlington Northern Santa Fe (BNSF), Union Pacific, and Pacific Harbor Line, Inc., provide the majority of these services. The largest component of rail traffic in the Los Angeles area is associated with the Port of Los Angeles seaport. The cornerstone of the Port's intermodal train traffic network is the 20 mile long Alameda Corridor which serves as the primary connection for cargo-carrying train traffic moving between the ports of Los Angeles and Long Beach and the transcontinental rail network based near downtown Los Angeles. Rail traffic along this corridor in 2007 included 17,824 trains. The Los Angeles area also maintains other rail facilities as part of major industrial complexes. One example includes the Carson Oil Refineries. Los Angeles also supports an extensive commuter rail system which includes both above ground and underground facilities.

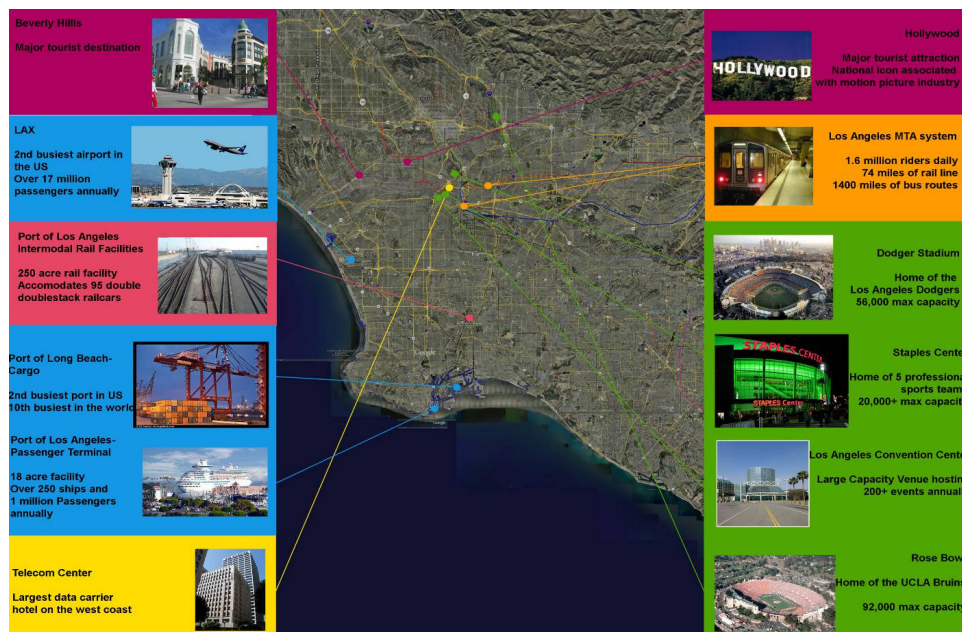


Figure 1: The Los Angeles /Long Beach area highlighting major venues.

Los Angeles has many key public facilities including the LAX Airport, Hollywood and Beverly Hills, Staples Center, Los Angeles Convention Center, Dodger Stadium, and the Rose Bowl. Los Angeles also has many key business and production facilities including the Telecom Center.

The Los Angeles region, through its own initiative and pilot efforts, has established significant network connectivity of its hazardous materials sensor systems. Every agency with a hazmat responsibility has been involved. Through key enablers a significant wireless sensor capability was already present in the region. The Los Angeles Fire Department information management team, led by CPT Yo Gikas, was already advocating for and enabling this expanded sensor capability. Along with leadership and guidance from Ms. Kathleen (Cass) Kaufman and Dr. Jeff Day of Los Angeles County Health, the Los Angeles region had begun to consider and explore the enhanced information management provided through sensor interoperability. The transfer and presentation of sensor readings and detections is only the beginning. As people are able, through the enhanced information sharing and situational awareness technology, to become more involved in the decision making process, a transformation and maturation of the raw data or information will occur which organizes and formats that information into “knowledge.” That knowledge can then be leveraged into informed decisions and actions. The maturation process can be delineated as follows:

Data Acquisition – Raw data via sensors or other automated or manual inputs is collected.

Information Management – Data from detectors are interpreted together with other contextual information. An example of this transition is the use of dispersion models to convert raw detections from multiple individual sensors into a graphical depiction of a chemical dispersion plume or radiological dosage contours.

Knowledge Management – Application of business rules or processes (usually) established by subject matter experts. One example would be combining the distance and dosage calculations of a dispersion model to calculate individual impact times and dose estimates for specific facilities or response zones.

Situation Awareness – Often defined as the user-oriented integration and display of multiple sets of information and knowledge, this requires the “fusion” of relevant information from mutually



independent non-redundant sources into actionable awareness. An example of situational awareness application for a first responder might well be the map displays and spreadsheets of the status of individual radiological and/or chemical detectors. Another example would be the dispersion plume or dosage contours used for emergency management, traffic control, or shelter activation.

Protective Action Decisions and Execution – The transition of knowledge into action. Execution of protective actions should be specific to communications and operational procedures driven by user need as defined in a Concept of Operations (ConOps). An example would be a responder with a specified role. A decision maker for the Red Cross may only want to see the list, locations, and status of the specific shelters to be opened and managed. In contrast, Police may need policies and checklists to execute a decision by the Health Department to provide prophylactic inoculations as part of a bio event response. Additional fused data could include the locations of inoculation sites as well as the procedures and checklists for all agencies needed to execute the decision.

This then was the start of the ICBRNE program. The region of Los Angeles, with its impressive resources and capabilities, would undertake the challenge of extending its use of sensors and standards to significantly enhance sharing of sensor and sensor detection-based information across local, regional, state and federal partners.

4 Concept of Operations and Policy Development

The ICBRNE Program concept of operations is based upon widespread, accessible and standardized sensor readings and alerts. There are two categories of alerts that Emergency Responders deal with: “Tactical” and “Strategic.” A Tactical alert is by far most common, and refers to alerts that pertain to information used to expediently resolve a situation or to temporarily gain an advantage while additional resources are brought to muster. See Figure 3a below. Strategic alerts are issued only in connection with planning and directing coordinated responses in larger operations.

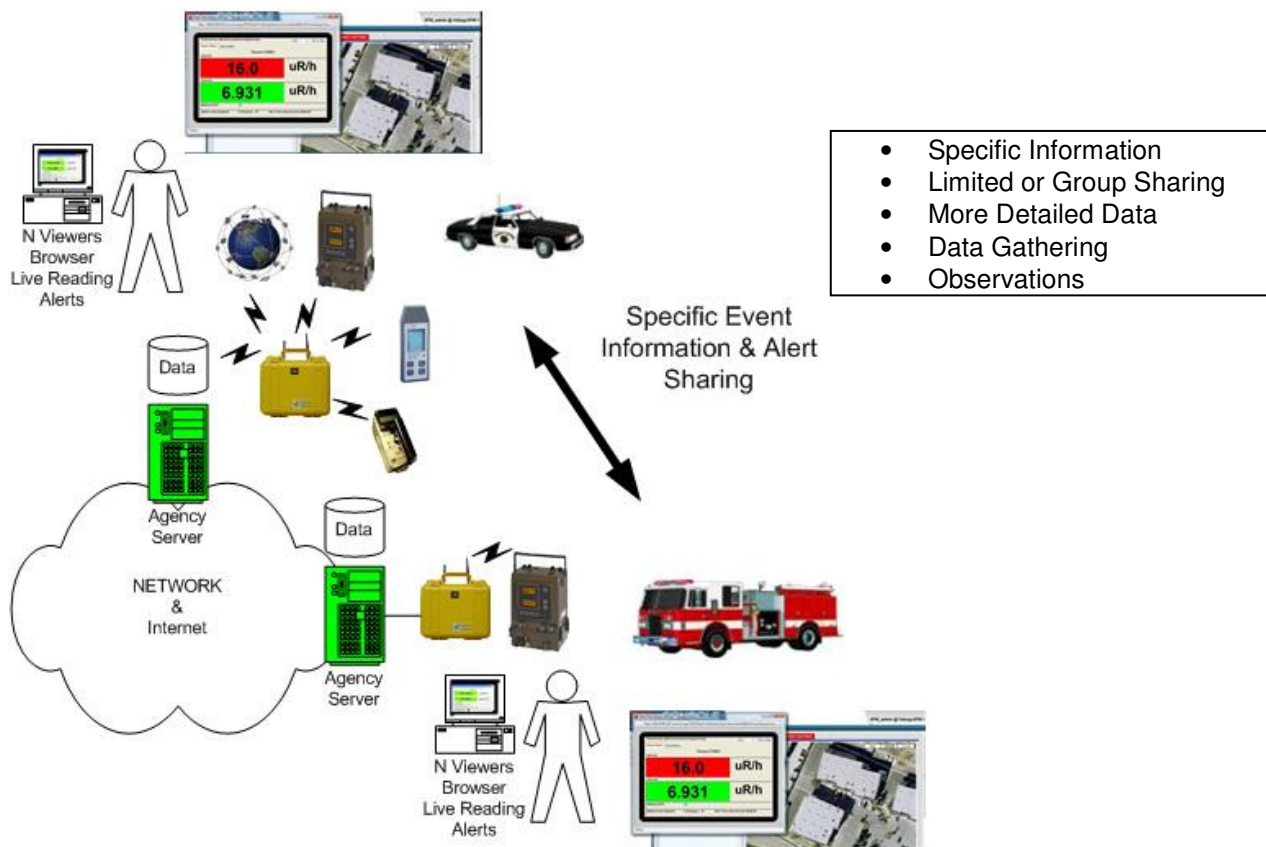


Figure 3a. ICBRNE Tactical Alerts

Sensors currently deployed in the Los Angeles Region are utilized primarily for tactical alert and notification processes. The Tactical Conops followed by the local public safety community has established 4 trigger points to automate notifications after initial information is vetted by the owner of the subject sensors. The notification trigger points are as follows:

Meter On
 Meter Off
 Meter in Alarm
 Meter out of Alarm

Numerous methods to deliver sensor data and alarm notifications message brokers are in place. These include TCP/IP, Web Services, E-Mail and pushed HTML. All data, messages, and notifications are delivered in initially DHS' Common Alerting Protocol (CAP) format, although conversion into other standard formats is enabled as needed for interoperability with diverse systems. Message/alert brokering is performed through a variety of commercial companies and federal services such as the Open Platform for Emergency Networks (DM-OPEN).

In the world of the strategic alerts there is no formal "play book." Strategies differ depending on the nature of an incident; however, chemical, radiological or biological events for the most part follow National Incident Management System (NIMS) protocols. The best documented series of alerts are in radiation detection. A simple Concept of Operations (ConOps) would involve four steps: (1) initial detection and alerting; (2) investigation and secondary screening; (3) technical reachback & ancillary confirmation; and (4) deployment of additional assets. See Figure 3b.

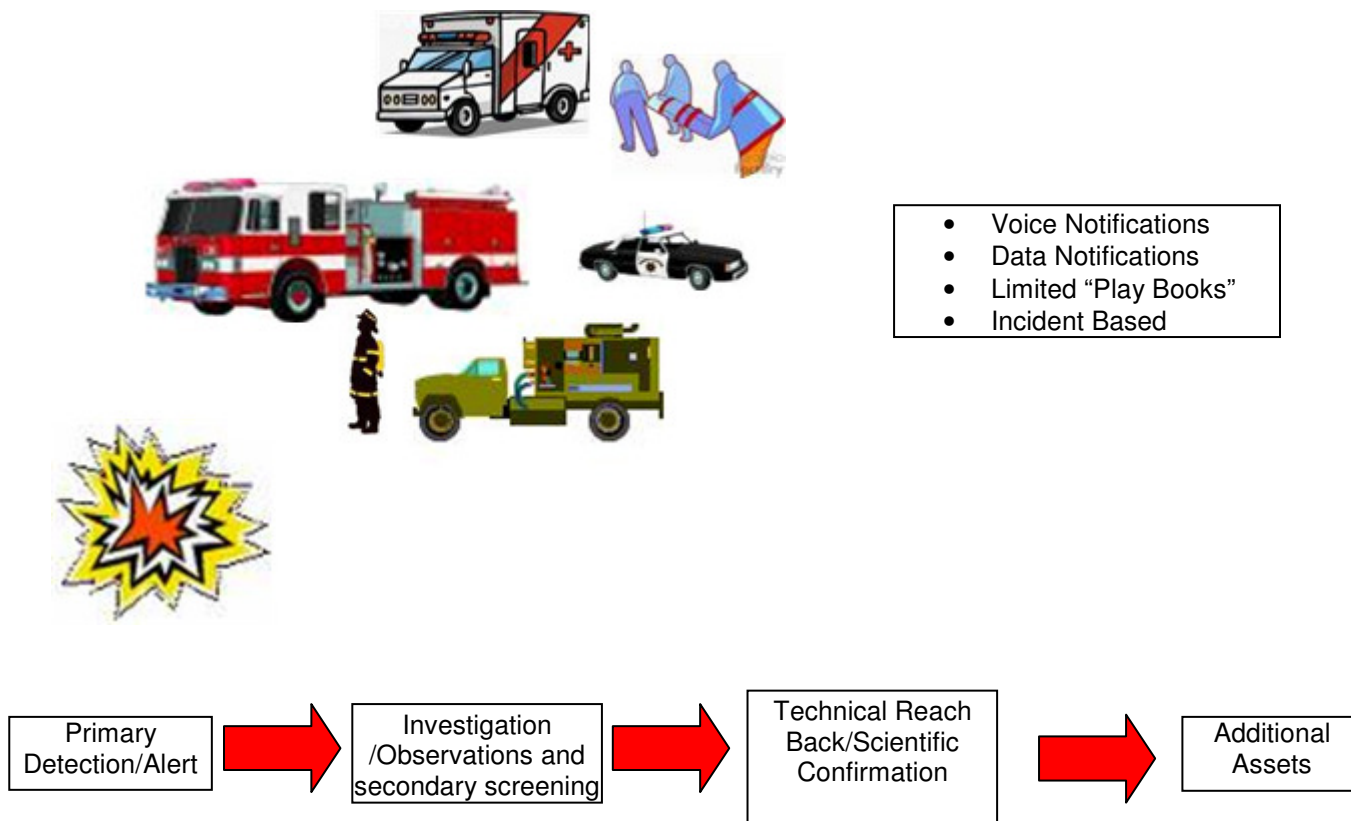


Figure 3b. ICBRNE Strategic Alerts & CONOPS

Although the arrows in Figure 3b point to the right, it's important to note that shared information for this conops must flow in both directions. The key is to utilize shared information across the organizations and federated levels in both directions to reachout to extended resources, expertise and decision-contributors and then funnel the resulting assessments, resources, and advice back down to the incident managers and decision-makers. The Domestic Nuclear Detection Office (DNDO) has developed this conops in its Mission Critical Messaging (MCM) program. The ICBRNE community participates in this program and supports and converts into the CBRN Information Exchange Package Document (IEPD) which supports this conops.

4.1 Sensor Instrumentation Overview

Public Safety utilization of sensors is fairly extensive but focused in several key areas for the primary purpose of environmental monitoring. Two sub categories cover most of the sensor use and fall into fields for chemical and radiological. Weather sensors also play a big roll, however, for the purposes of this report discussions will be limited to handheld equipment.

Typically sensors are combined in instruments to test for a variety of hazards. A combination of sensors often is called a meter or instrument. Within these two fields a distinction is typically made as result of cost and complexity.

In the radiation detection category there are three basic types of wearable or hand-held sensors: (a) a simple dose or count rate pager; (b) a survey tool; and (c) a detailed analysis instrument. We'll take a quick look at each of these types of instruments.



For a simple dose pager, the sensor typically provides information as to the presence of radiation (mostly Gama). This type of device tells the user that there is a source nearby and a display of 1 to 10 might be the only indication of the intensity of the source. Currently this type of device is not connected to any telemetry or information sharing system because they are subject to false positives, are deployed in large quantities, and are typically used just to catch someone's attention. The cost to add external monitoring to this type of a device is currently prohibitive given the nature of use of such devices.

The next type of radiation detection device is a survey tool which is a handheld device that can have interchangeable probes for performing area sweeps for more specific radiation types, and providing more refined information on the radiological properties. These devices are being used for telemetric data acquisition to insure the safety of survey personnel by a remote attendant or for data analysis by a subject matter expert in a remote location. Whereas the amount of data from these devices is relatively small, the rate at which they deliver data can be quite rapid; on the order of several readings per second. Many of the devices work in a constant delivery mode. The moment there is new data available it is sent to the output port of the device.

The third category of handheld radiation detection devices are isotope indemnification tools, providing a more detailed analysis. These devices can analyze and identify the radiation source, and in many cases produce information on the energy spectrum being detected. Spectrum data is typically treated separately from the raw sensor reading and stored in separate files on the device. The spectral data is available for acquisition from the device but is typically a much larger block of data.

For handheld chemical sensors, there are similar types of instruments with the major difference being a larger type for multi-gas meters. Telemetric data acquisition with multi-gas meters can monitor a wider range of a specific substance or a variety of sensors packaged together that can monitor several categories of substances. Since some of these devices contain several sensors and the data produced can be more extensive.

4.2 Incident Sensor Data:

In many circumstances the data acquired from Public Safety sensors is vetted by either on-scene Hazardous Material specialists or directly sent to remote subject matter experts. At this stage of the process the data is in its raw format (looking the same as the readings on the face plate of the meter) because it is being viewed by specialists familiar with the instrument. If a condition warrants the involvement of other experts or should it be appropriate that an alert be sent out, the local specialist has the option of either forwarding the raw reading with other alert information to others or just sending alarm and alert conditions.

Sensor analysis is performed using several factors:

1. Remote display of raw sensor readings
2. Filtering of raw data to only show alarm conditions
3. Trend analysis showing sensor values over time (depending on the sensor this can also be a trigger for alarm conditions when weighted averages need to be considered such as Short Term Exposure Limits [STEL] or Time Weighed Averages [TWA])
4. Sensor readings integrated as part of a Geographic Information System (GIS)



4.3 Sensor Interoperability:

There is a significant need for interoperable sensor data in the Public Safety community. Without wireless telemetric data transmission, sensor users face numerous challenges. One of the foremost problems is reading sensor values from an instrument's faceplate through several layers of fogged up facemasks. Another is the distraction of trying to read the instrument data while mitigating the hazard. Voice transmission of sensor values can also cause problems. Users may hold the transmit key down, inadvertently blocking instructions, and may misspeak vital data readings. There is also a risk of interception of sensitive information by an eavesdropper.

Further challenging the need for remote sensor data acquisition is the limited use of a standard data format, protocol, or connector associated with the instrument. In general no two manufactures handle data acquisition the same way. This problem can even be found across similar models of the same manufacture.

To overcome this problem in the short term, the ICBRNE program utilized the Common Alert Protocol (CAP) to enable reliable sensor information sharing. The Common Alerting Protocol (CAP) is one of the most useful, familiar and supported emergency management standards. This Federally approved Standard gave the Public Safety community confidence that the information flowing from sensors and to sensor utilization applications was in a non-propriety format. Utilizing CAP and other Emergency Data Exchange Language (EDXL) standards, such as the Distribution Element, the sensor data can be packaged with other information representing the associated hazards of the incident and routed to the appropriate users based on policies and geospatial coordinates.

CAP was carefully studied to determine what was minimally needed to maintain the standard knowing that bandwidth would be a consideration in any wireless deployment. Initially the "Headline" was picked as the most data efficient element within CAP to transport sensor information. As working knowledge of vendor adoption of CAP matured, so has the utilization of sensor data in CAP which now utilizes the "Parameter" fields.

Through the continued work of the ICBRNE Program and OASIS, there will likely be further refinement of sensor messaging protocols. In the long run, sensor manufacturers will likely adapt sensor-specific standards for the exchange of their data, such as IEEE 42.42 (a radiological sensor standard) or the Open Geospatial Consortium's (OGC) Observations & Measures standard. These standards will be integrated into suitable message exchange formats developed by government agencies under the National Information Exchange Model, such as those represented in the CBRN IEPD. This continuing maturation will contribute to the effectiveness of Public Safety sensor data and alert notification applications.

4.4 Utilization of the Common Alerting Protocol

Alert messaging standards for the public safety sector are rapidly converging around the OASIS OPEN CAP v1. The judicious use of this CAP message can provide a convenient alert and messaging mechanism for sensor data.

The CAP used for ICBRNE is an extended message that contains the actual summary data and alert status of the sensor(s). The data is contained in the <Parameter> tag in a comma delimited text string. The sensor data is therefore not readable by users unacquainted with the data string. However for the community of users that require the data, it is easily read by specific applications attached to their situational awareness tools. The message is relatively short and fits easily into small dedicated applications on handheld devices.



4.4.1 ICBRNE use of CAP:

The use of the parameter fields bundles single or multiple probes or detectors from a single instrument into a single parameter where the value name, value pair for each probe/detector contains all pertinent non-common information in a comma delimited text string. It is effective for passing data to a predetermined display formats. An example for a rad device with 3 probes would have 6 <parameter> tags (three common tags (sensorStatus, sourceDataURL, batteryLevel) and three Sensor tags, one per probe). The sensor data for each tag is then expressed as

```
<parameter>
  <valueName>Sensor</valueName>
  <value>deviceType, detectionType, probeType, probeModel, reading, units,
  alertColor </value>
</parameter>
```

An example of one Radiation Detector with 3 probes with additional data available would be:

```
<parameter>
  <valueName>sensorStatus</valueName>
  <value>Normal</value>
</parameter>
<parameter>
  <valueName>sensorDataURL</valueName>
  <value>128.156.12.34</value>
</parameter><parameter>
  <valueName>batteryLevel</valueName>
  <value>14%</value>
</parameter>
<parameter>
  <valueName> sensor</valueName>
  <value>Rad, Alpha, HCZ, Type4, 14.4, uR/hr, Green</value>
</parameter>
<parameter>
  <valueName> sensor</valueName>
  <value>Rad, Beta, GMT, Type2, 124, Counts/sec, Yellow, </value>
</parameter>
<parameter>
  <valueName>sensor</valueName>
  <value>Rad, Neutron, LIG, Type305, 2024, Counts/sec, Red
  </value>
</parameter>
```




4.4.2 Sample CAP

```
<?xml version="1.0" ?>
<alert xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:emergency:cap:1.1">
  <identifier>LAFD131A20080519075513</identifier>
  <sender>CAP@Safeenv.com</sender>
  <sent>2008-05-19T07:55;13-07:00</sent>
  <status>Test</status>
  <msgType>Update</msgType>
  <source>Ludlum Model 2241, SEE Ludlum.xml, 000B280218C4, 192.168.1.18</source>
  <scope>Restricted</scope>
  <restriction>HAZMAT list only</restriction>
  <note> This is only a test, no suspicious activity present </note>
  <info>
    <category>Other</category>
    <event>unknown explosion</event>
    <urgency>Immediate</urgency>
    <severity>Unknown</severity>
    <certainty>Observed</certainty>
    <senderName>LAFD</senderName>
    <web>http://64.160.7.213/common/jsp/SPM/RealTimeDisplayGen2/sensorAlertGISInfoFrameSet.jsp?sensorInfoFrame=realTimeThermoFH40SensorDataFrameSet.htmlhttp://Server URL</web>
    <contact>LAFD Station10, Engine 10, Capt. Lesinski</contact>
    <parameter>
      <valueName>sensorStatus</valueName>
      <value>Normal</value>
    </parameter>
    <parameter>
      <valueName>sensorDataURL</valueName>
      <value>128.156.12.34</value>
    </parameter>
    <parameter>
      <valueName>batteryLevel</valueName>
      <value>14%</value>
    </parameter>
    <parameter>
      <valueName> sensor</valueName>
      <value>Rad, Alpha, HCZ, Type4, 14.4, uR/hr, Green</value>
    </parameter>
    <parameter>
      <valueName> sensor</valueName>
      <value>Rad, Beta, GMT, Type2, 124, Counts/sec, Yellow</value>
    </parameter>
  </info>
</alert>
```



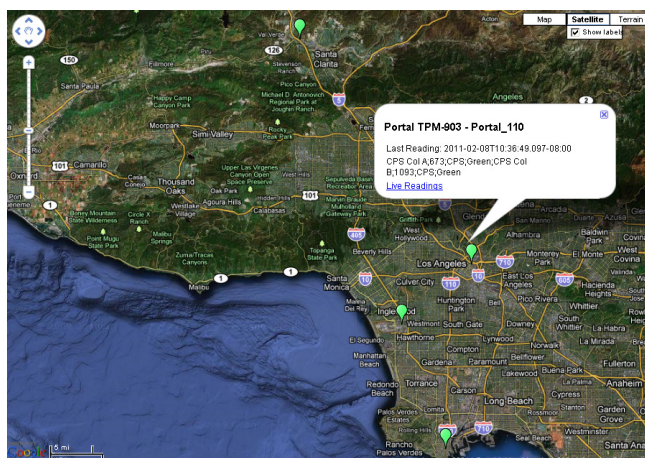
```

</parameter>
<parameter>
  <valueName>sensor</valueName>
  <value>Rad, Neutron, LIG, Type305, 2024, Counts/sec, Red</value>
</parameter>
<area>
  <areaDesc>1335 South Olive Street, Los Angeles, CA</areaDesc>
  <circle>34.0501, -118.2511</circle>
</area>
</info>
</alert>

```

4.4.3 CAP and Google Integration

The ICBRNE Pilot often uses the location component with the CAP message to indicate a location on a map. A common tool for displaying map data is either GoogleEarth or GoogleMap. The data format to express a location in either of these tools is the use of special Extendable Markup Language (XML) called Keyhole Markup Language (KML). Within the ICBRNE Testbed is a translator that takes CAP data and embeds into KML (<https://icbrne.info/icbrne/detections/?form=kml>).



4.5 Alerting and Notification

A component of the ICBRNE project is the ability to alert and notify in relation to CBRNE events. This process utilizes developed policies to filter automated messages generated from detection instrumentation. Once filtered these messages are broadcasted to a subscription list of emergency responders. Manual operation of this system is also provided. Delivery options include SMS, E-mail, test-to-speech or Fax.

The Los Angeles component also integrated a “man in the middle” concept through the use of Real-Time Analysis and Critical Response Division (RACR). The RACR Division is LAPD's first 24/7 fusion/information processing center. RACR operates as a 24/7 emergency operations center where resources, situation status of the city and developing tactical incidents are tracked. RACR also monitors and follows through on CBRNE alerts to insure that the alert message was received and responded to.



All data exchanged with the ICBRNE program follows strict adherence to federally endorsed open standards. Alert messaging specifically utilizes the Common Alerting Protocol (CAP) standard which defines the minimal necessary data elements to clearly define an alert. For CBRNE based alerts it is necessary that the message also contain information about substance detected. In addition to required minimal fields four additional items were added to the alert message including detection type, reading, units and alert color.

- **Detection Type** – designates the substance being detected such as radiation, ammonia or nerve/blister.
- **Reading** – Is the alphanumeric amount of the substance being monitored.
- **Units** – Represents the quantity of what is being measured.
- **Alert color**- Indicates the severity of the combination of the substance monitored and its readings and units. Typically Red indicates an alarm condition, Yellow a warning (radiation only) and Green indicates a safe condition. These trigger points are typically provided by Subject Matter Experts for radiation values and industry exposure limits as established by the National Institute for Occupational Safety and Health (NIOSH) for chemicals. These threshold values exist within an administrative password protected window and are typically configured at the time a new instrument is brought online.

Position	Model	Warn	Alarm	Test Unit
Position 1	Model 43-92-100 cm ² Alpha Scintillator	200	1000	Counts
Position 2	Model 44-9 Pancake G-M Detector	200	1000	Counts
Position 3	Model 133-2 G-M Detector	.000030	.000100	Dose (Rem)
Position 4	Model 44-9 Pancake G-M Detector	200	1000	Counts

Radiation Alarm Threshold Setting

Sensor	Label	Low Limit	High Limit
Sensor 1	LEL		10
Sensor 2	O2	18.5	23.5
Sensor 3	NONE		35
Sensor 4	SO2		2
Sensor 5	CO		35
Sensor 6	H2S		10

Chemical Alarm Threshold Setting

Policies were created to determine who got what alert/notification and under what circumstances. Whereas these policies can be extensive and diverse the ICBRNE program focused primarily on CBRNE conditions.

Alerts/notifications are generated by creating policy for one or more of the rules listed below.

1. **No Filter** - all data available. All information received from server will be pushed out to subscribers of this group. No special filtering will be applied. This is a pass through service.
2. **Pre Filter** – Provides for the creation of sub groups based on the CAP “incident” field
3. **In Test Filter** – The CAP field “Status” is monitored. Data with this field set to test is disregarded.



4. Extreme Alert Filter – All data is disregarded except if the CAP field of “Severity” is set to Extreme.
5. Geographical Alert Filter – Associated with the Test filter all registered users in a geographical area defined by a polygon wherein an alert is occurring receive notification.
6. Agent Alert Filter - Specific sensor types will trigger alert grouping as defined in number 4.
7. Multiple Detection Filter - Multiple instrument alarms coming from the same location (if not “incident” then Gateway) will trigger alert grouping as defined in number 4.

Using data acquired from CBRNE CAP message the rules are summarized as follows:

Safe ENV Sensor Groups	
Everything:	<input type="checkbox"/>
Single Green:	<input type="checkbox"/>
Single Red:	<input checked="" type="checkbox"/>
Multiple Red:	<input type="checkbox"/>
Test:	<input type="checkbox"/>
Extreme:	<input type="checkbox"/>
Exercise:	<input type="checkbox"/>

Safe ENV Instrument Types	
Radiation:	<input type="checkbox"/>
Radiation Alpha:	<input type="checkbox"/>
Radiation Beta:	<input type="checkbox"/>
Radiation Gamma:	<input type="checkbox"/>
Radiation Neutron:	<input type="checkbox"/>
Radiation Isotope:	<input type="checkbox"/>
Chemical Warfare Agent:	<input type="checkbox"/>
Combustible Gas:	<input type="checkbox"/>
5 Gas:	<input type="checkbox"/>
4 Gas:	<input type="checkbox"/>
Particulate:	<input type="checkbox"/>



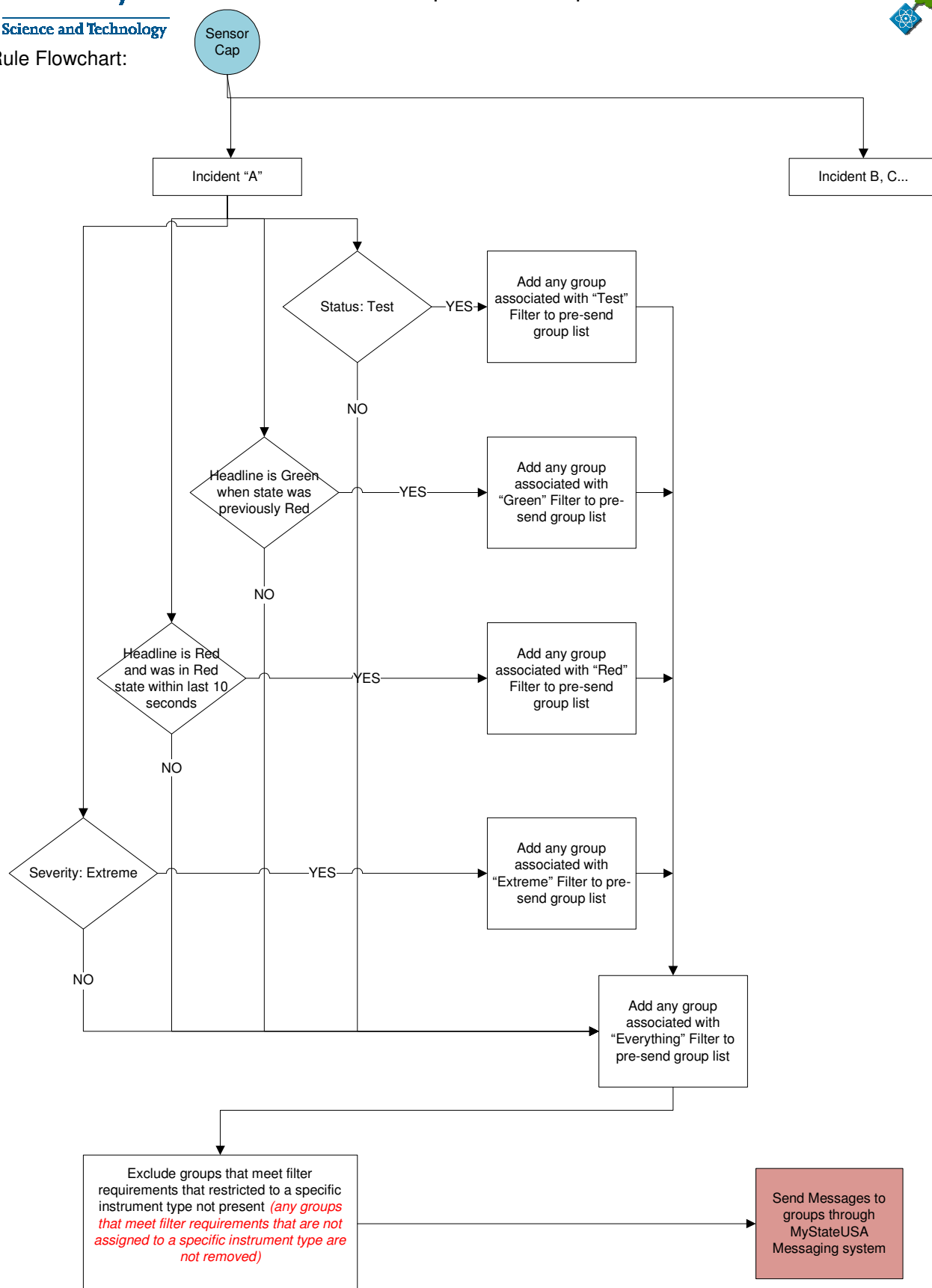
Specific instruments with their categories include:

Name	Selected
Bruker Daltonik RAID-M	<input type="checkbox"/>
Bruker Daltonik RAID-XP	<input type="checkbox"/>
Drager X-am 7000	<input type="checkbox"/>
Fluke 451	<input checked="" type="checkbox"/>
Industrial Scientific iTX	<input type="checkbox"/>
Industrial Scientific VX500	<input type="checkbox"/>
Ludlum Measurements Model 2241	<input checked="" type="checkbox"/>
Portal Monitor TPM-903	<input checked="" type="checkbox"/>
RAE Systems PGM-2000	<input type="checkbox"/>
Thermo DataRam 4000	<input type="checkbox"/>
Thermo FH 40 G	<input checked="" type="checkbox"/>
Thermo IdentiFinder	<input checked="" type="checkbox"/>
Thermo MDS	<input checked="" type="checkbox"/>

Name	Count
Radiation	6
Radiation Alpha	2
Radiation Beta	2
Radiation Gamma	6
Radiation Neutron	
Radiation Isotope	1
Chemical Warfare Agent	2
Combustible Gas	4
5 Gas	3
4 Gas	1
Particulate	1



ICBRNE Operational Report



Note: In addition to the Headline field separate Parameter fields are provided



5 Tools & Services

5.1 Wireless

There are 2 common ways of sending wireless sensor data from point A to point B, one being telemetry and the other through a network. The telemetry typically involves a process wherein each point sequentially interrogates each other point for the exchange of data. A network connection can almost be considered a continuous exchange of data between all devices on the network. Also important is the fact that a network connection can be routed across other network devices to extend the range which includes utilization of tools such as the Internet. For these reasons a network approach was chosen for ICBRNE.

5.2 Network Devices

A network device arbitrates data as it passes through it. For ICBRNE these devices are routers, switches, cellular modems, access points, gateways, serial servers and satellite terminals. The data sharing requirements of ICBRNE require data to be routed through the internet. To accomplish this most end points utilize a cellular connection. Cellular has the benefit of being the most pervasive cost effective network available but does not offer the same level of a guarantee of service as a private proprietary wireless network.

Example of ICBRNE communication

PowerPoint animation:

<http://www.icbrne.org/Presentation.htm>

5.3 Sensor Views

Two primary views of the sensor data worked best for the majority of users in the ICBRNE program: the Subject Matter Expert (SME) View and the Emergency Manager (EM) View. The SME view recreated an exact replica of the meter displays on the computer screen. This design has many benefits. SMEs are trained with their meters, so there is no extra training required to understand the computer displays. The sensor manufacturers' meter displays become de facto standards of their own and the reuse of the designs reuses their lessons learned. The meter views display specific sensor data for specific sensors which is what SMEs need. The meter displays can be viewed individually or multiple meters can be displayed on one screen as needed. The second primary view is the Emergency Manager (EM) View. Emergency managers have a more holistic and broader perspective than the SMEs, so they need a map of the region with highlighted areas and points that describe the sensor readings from a region-wide perspective. The goal is situational awareness derived from multiple sensor detections to guide management of the entire region.

Both views, SME or EM, can be delivered to any location in near real-time, whether the back of a fire truck, a mobile PDA, a desktop anywhere in the region or around the world. The views are accessible through a variety of installed commercial software viewers as well as through a user's browser without any additional



installation of software. Although we won't discuss the technical details here, it's important to understand that the flexibility of these visualizations and the implied interoperability with a variety of commercial tools is enabled by utilizing open standards and open architectures that allow for conversion of sensor information into a variety of standard formats. Let's look at examples of both kinds of views to better understand the ICBRNE program.

5.4 SME Views

The basic SME View is the meter shown in Figure 1. On the left is the actual meter faceplate and on the right is the SME View as shown on the remote computer display. Note that both displays are formatted in the same manner with three columns, the first being the chemical label, the second being the values and the third column being the units.



Instrument Display

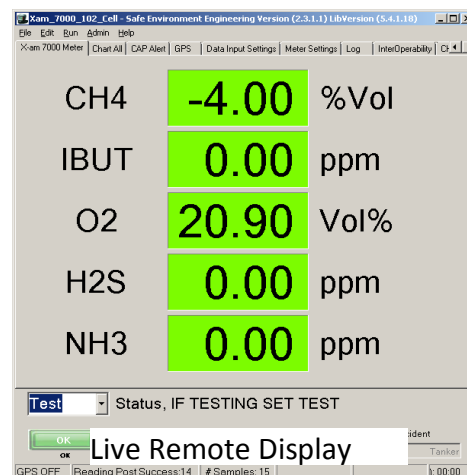


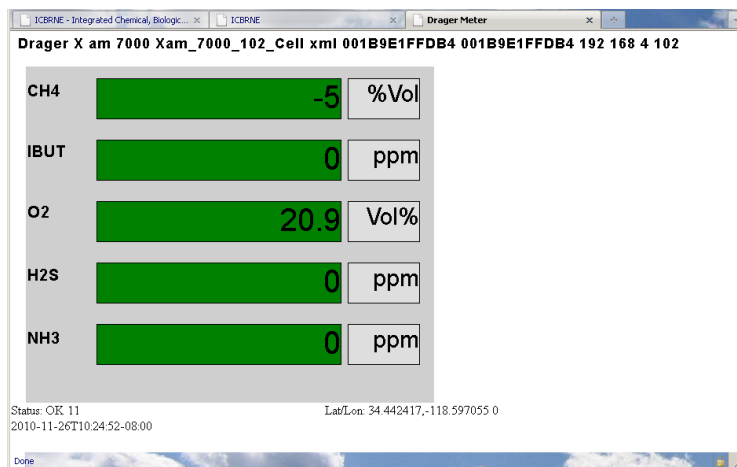
Figure 2. Basic SME View

A Multi-Meter SME View is shown in Figure 3. This view is available for SMEs who want to view numerous instruments that are operational at any one time. This Multi-Meter SME view is automated and dynamic. In this view, meters appear and disappear as they go on and off-line, and the meters shrink in size as needed to fit the overall display size. Filters can be selected to view meters by Incident, user or instrument type.

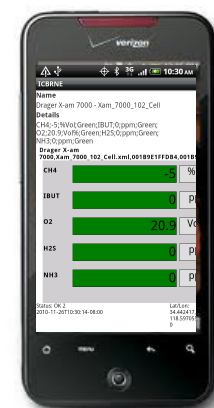


Figure 3. Multi-Meter SME View

The Basic SME Web view is another form of viewing the meter emulations in a web browser on a desktop display or on a cell phone or PDA. See Figure 4. The browser view is available in either a desktop component or in a mobile environment.



Desktop Web View



Mobile Web View

Figure 4. Basic SME Web View

The browser view was important for ICBRNE users that did not have local applications directly supporting ICBRNE data. In this format with approval, a user simply logs on to the ICBRNE testbed with appropriate



credentials wherein they are directed to a list of currently logged on meters. At this point the user can select which meter they want to view “live” and/or open up multiple windows for multiple concurrent views.

5.5 EM Views

The basic Emergency Manager (EM) View is the regional map display as shown in various forms in Figure 5. The characteristics of these views include a regional map, sensor-derived situational awareness, sensor readings in context, and at a glance situational awareness.

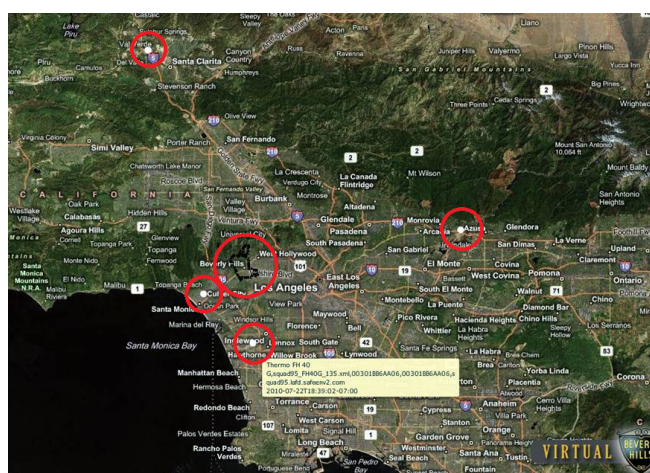
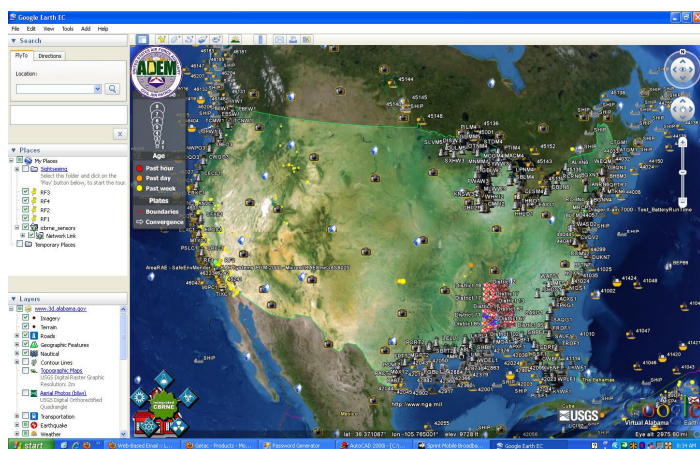
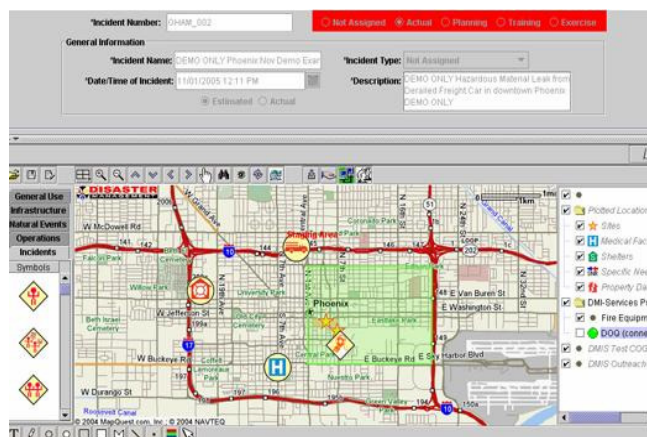
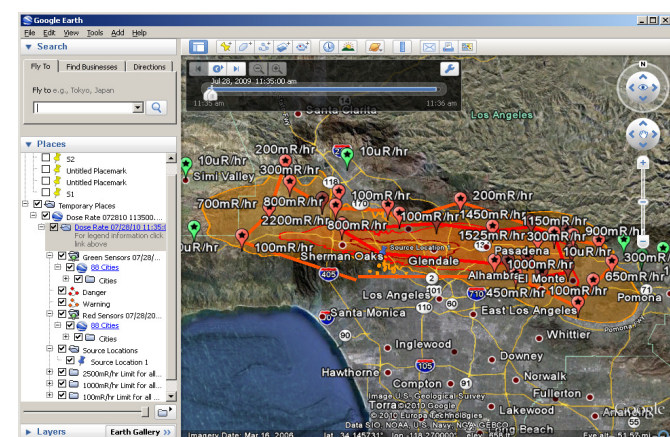


Figure 5 Emergency Manager (EM) Views

Operation Golden Phoenix provided insight into the viewing tools available for Emergency Managers. The conclusion yielded a need for data flexibility due to the lack of consistent tools. ICBRNE helped coordinate and integrate data across several tools including GoogleEarth, Disaster Management Interoperability Service (DMIS), Virtual Beverly Hills, Virtual Alabama and others.



As with the SME Views, these EM Views are available in installable commercial software as well as web browser-based displays. The same flexibility and interoperability is enabled through the use of open standards and open architectures.

5.6 Integration of maps

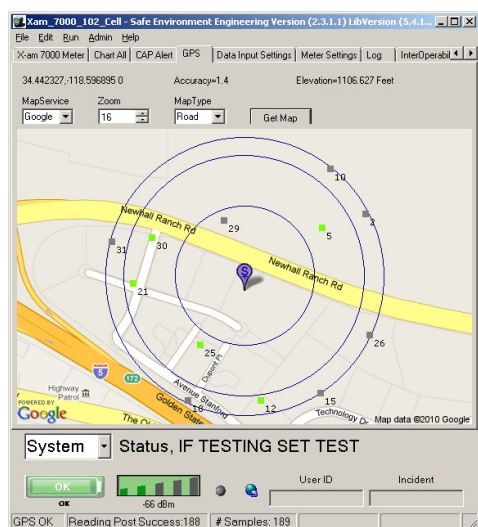
As the ICBRNE Project grows, the evolution of contextual information becomes more important. Today users want the ability of knowing where their sensor information is coming from so they can start correlating data about the incident.

To accomplish the location component, GPS receivers have been added to the wireless telemetry feeds coming from most of the instrumentation. This GPS feed is specific for the instrument which has matured from a grouped based GPS location which was originally provided the same GPS feed for the instrumentation at a specific location. With independent GPS feeds, specific users and/or specific instruments can be tracked as independent sources.

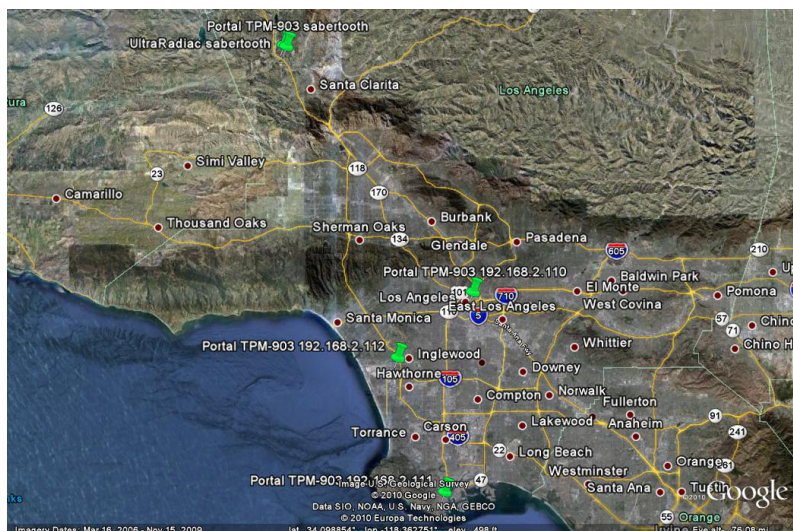
With the use of map based data, consideration of the origin of the maps is a very important component. Currently there are two map sources, the first being a live internet based map such as Google or Bing. The second is the more permanently affixed maps that are a component of the software on the PC viewing the data such as ESRI or MapPoint.

The importance of the consideration of where the map comes from is largely due to the availability of an internet connection. Users that could potentially go off-line or that want to use the system in a completely local network should consider local permanent maps. Users that have the ability of going to the Internet to acquire data and feel that this connection will be appropriately robust should consider live map feeds. For the map component, data is available in a variety protocols including a direct KML or GeoRSS feed.

Two types of maps were considered for ICBRNE, one being an instrument specific map and the other being a regional map, shown in Figure 6. The instrument specific map (as shown below) provides a view of specifically where the instrument is located. This is particularly useful with the MultiMeterViewer to identify where an instrument is as opposed to needing to see the complete group view of all instruments. In the regional or group view, all instruments can be viewed concurrently on one map; however, since sensor instruments can be located all over a city, region, state or nation, the zoom-level and perspective of the map must be considered in relation to where the sensors are located.



Instrument Specific Map View

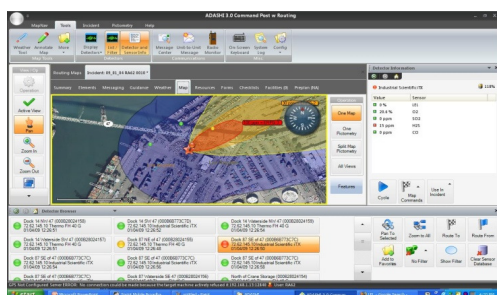


Regional Map View

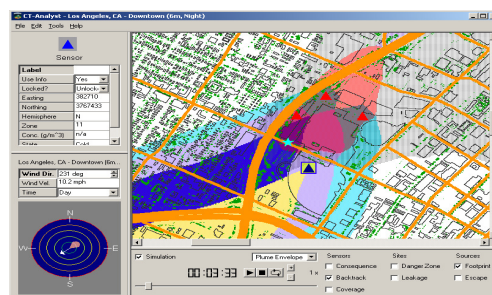
Figure 6. Two Types of Map Views: Instrument & Regional

5.7 Integration with plumes

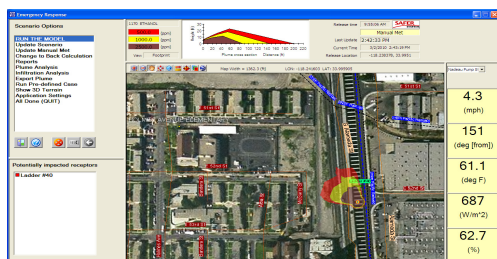
Often the CBRNE instrumentation is used as part of a plume tool. These tools are used to model the direction and magnitude of the agent, as shown in Figure 7. ICBRNE has interfaced with several different plume tools, including one that is created as a result of a detection, another that uses the sensor readings as part of its plume algorithm, and another that integrates sensor detections into its model.



Creation due to detection



Integration of detection data into the model



Integration of sensor data into the model

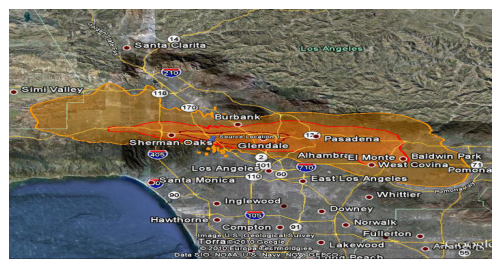


Figure 7. Integrating Sensor Data with Plume Displays

6 Regional Information System

ICBRNE enables a regional information system with the sensor information needed to manage an emergency, as shown in Figure 8.



1. Incident occurred, resources tasked, sharing information with enroute responders.
2. Additional responders preparing to assist with environmental knowledge of conditions.
3. Remote technical assistance provided, on seen assistance hindered by traffic.
4. (coming) Remote State and Federal subject matter expert assistance

Figure 8. Regional Information System Enabled with ICBRNE

The maps in Figure 8 illustrate the conops applied from a regional perspective and the importance of placing the sensor information in context with other relevant regional information, such as traffic and hospital locations. First, the incident occurs. Local resources are tasked. Key information is shared with in-route responders. Second, additional responders in the region prepare to assist with environmental knowledge and assessment of conditions. Third, remote technical assistance is provided since the sensor information is accessible in near real-time from any location. On-seen assistance is being hindered by traffic congestion. Fourth, remote state and federal subject matter expert assistance and resource support is activated and deployed.



7 Interoperable Test Virtual Laboratory

The **Interoperability Test Virtual Laboratory (ITvL)** is a virtual interconnection of computers with supporting infrastructure to enable testing and exploration of interoperability solutions. The testbed was utilized throughout the ICBRNE program, providing a sensor data repository, a set of conversion routines into a variety of standard formats, browser-based map displays, service-oriented access to data feeds, gradient displays in Google Earth, and a wiki of documentation for learning more about ICBRNE, standards and interoperability. In support of the ICBRNE Program, the testbed allows users from different backgrounds to come together, discuss and to explore interchange of information across organizations, sensor systems, and standards. You will find more information at <http://www.icbrne.org>.

The software components and lessons learned from the ITvL activities are available for your consideration and reuse. To provide an easy-to-understand overview of these components, a set of Frequently Asked Questions (FAQs) is provided in Appendix H. The questions cover a broad scope, from the general but significant definitions such as “What is Interoperability?” and “What are open standards?”, to the specific how-to questions, such as “How do I create a CAP message?” or “How do I post to the DHS OPEN messaging backbone”. The how-to questions reference template forms provided in Appendix I. The forms provide a structured reference providing point-of-contact information, links to examples, and links to the software itself. Together, this document with its Appendices H and I, and the software/style sheets linked from there, provide a comprehensive overview and accessible drill-down into the full ICBRNE program.

8 Program Solutions & Benefits

One way to measure the benefits provided by the ICBRNE program is to consider cost savings. As ICBRNE improves the effectiveness of sensor-based emergency management, a variety of examples of cost savings come to mind. In the current climate of limited resources, any significant cost savings is important and contributes to the overall effectiveness of the mission. Formal cost measures remain to be developed; however, examples of cost savings are readily available. We'll see by looking at the examples below, that the ICBRNE program can save time, resources and dollars.

Most incidents, especially hazardous material incidents, require the participation and guidance of subject matter experts. Often, these subject matter experts are a limited resource supporting multiple incidents and located remotely from the incidents. Before ICBRNE, the SME would be required to attend the incident or significant resources would be consumed communicating to and from the SME and the incident. With ICBRNE's distributed sensor readings, interoperability and situational awareness, SMEs can now collaborate remotely on an incident with much less verbal communication overhead. Not having to require the SME to be on scene can be significant and the time necessary to get the person appropriate data is dramatically reduced.

The same cost savings applies to federal resources. There are significant federal resources that could be “on-line” to help during an incident, if the federal participants could share sensor information in a real-time manner. The current model suggests that the resources must be deployed, get to the incident, and assess the situation on scene before providing expertise. Giving the federal resources data remotely and live would allow their expertise to contribute at the time of the incident as opposed to after the event occurred.

As one example, there is often a need during an incident for a first responder to support lookup on various chemicals from a library of information. Currently, a first responder may be tasked with this assignment and co-located at the incident, perhaps even in the back of the truck, looking up data. This effort may take considerable time because the responder must explore a variety of potential chemicals that *may* have been released or radiological conditions that *may* exist. This does not have to be done at the incident and, utilizing ICBRNE capability, can be performed remotely with real-time readings for guidance saving both time and the cost of deploying that resource to the incident just to service this library function.

Another ICBRNE benefit and significant cost savings is enabled by ensuring accurate data is provided to the incident command so that the response scales appropriately. At times during the stress of an event and also as a result of the environmental conditions, instrumentation readings may be misread which can cause



a chain of events to occur based on the misinformation. In the past, the wrong decimal point or the wrong units communicated over the radio could create a cascade of events that did not really need to occur. ICBRNE sends an exact replica of the instrument readings, through the telemetry interface that it provides to incident command so that appropriate decisions can be made, thus keeping the incident in check.

ICBRNE offers the use of predefined policy based notification to ensure that the data from a potentially significant event gets to the appropriate people to enable the optimum use of resources. This is another instance of getting the right data to the right people who can provide the correct level of response, either scaling up or scaling down based on real-time accurate sensor information. Appropriate use of resources improves response and lowers cost.

Collectively, all these balances of time, people and money based on live integrated ICBRNE data and equipment plays a very significant role in cost and time savings. As more opportunities are explored, the result of data integration, cost and time saving is a significant offset to the investment necessary to integrate the equipment.

8.1 Equipment Diversity

A wide variety of equipment is enabled by ICBRNE to support field activities. The equipment comes in different types (chemical, radiological, biological, etc.) with different communication formats.

Appendix L Instrumentation Interfaces includes a table providing a nice listing of the types of sensors supported, including communication format (protocol), data format, and a picture of the connector itself. The federated environment and the innovation in the commercial sensor industry result in a large diversity of equipment being used to support incidents.



8.2 Instrument Types

Ludlum <ul style="list-style-type: none"> 2241 2242 2360 	Brucker Detection <ul style="list-style-type: none"> RAID-M RAID-XP HAWK 
iCX <ul style="list-style-type: none"> Stride Radier 	Berkeley Nucleonics <ul style="list-style-type: none"> SAM 940 
Draeger Safety <ul style="list-style-type: none"> Xam-7000 Xam-5000 IMS 	Industrial Scientific Corp. <ul style="list-style-type: none"> iTX VX500 MX4/MX6 
Rae Systems <ul style="list-style-type: none"> QRea MultiRae MiniRae PPBRae UltraRae AreaRae ChemRae 	ThermoFisher <ul style="list-style-type: none"> MDS FH40G DataRam IdentiFinder RADEYE Interceptor TPM903 
Met One Instruments <ul style="list-style-type: none"> EBAM 	Radiation Solutions Inc. <ul style="list-style-type: none"> RadAssist 
Ortec <ul style="list-style-type: none"> Detective 	EnviroNics <ul style="list-style-type: none"> ChemPro 100 
Trimble 	Fluke 
Canberra <ul style="list-style-type: none"> PDR-77 UltraRadiac 	MSA <ul style="list-style-type: none"> Sirius Altair 

9 Standards Compliance & Interoperability

One significant component making the ICBRNE interoperability work is the use of open standards, which are listed in Appendix F. The instruments communicate in their native format to an intermediate software application that converts the raw unformatted sensor data into a structured standard format. Through the use of a standard, systems designed to this specification will work together. The principal standard used for ICBRNE systems communications is the Common Alerting Protocol (CAP). CAP has a large international presence and is used as a notification method by organizations such as the National Oceanic and Atmospheric Association (NOAA) for weather alerts, the US Geological Service (USGS) for seismic (earthquake) alerts, the Federal Communications Commission for emergencies and a large variety of commercial, federal and defense systems. The ICBRNE Testbed provided a platform to integrate CAP with other standards including Universal Core (UCore), Cursor on Target (CoT), Sensor Web Enablement (SWE), Emergency Data Exchange Language – Distribution Element (EDXL-DE), Hospital AVailability Exchange (HAVE), Emergency Data Exchange Language – Resource Messaging (EDXL-RM) and Situation Reporting (SitRep). More information on CAP can be found in Appendix F of this report.



10 Training

Training is a significant and ongoing component of ICBRNE's deployment. For a regional deployment there can be a significant number of users that will require training on the various software and hardware additions. The training should contemplate that there will, in all likelihood, be multiple shifts of users and that these users could rotate through the job positions that interact with the ICBRNE program. Additional training requirements could result from normal job promotion and/or attrition. The net result of this section is to encourage the ICBRNE facilitator to make training a significant component of the program implementation.

10.1 Train the Trainer

An effective tool for long term training is a Train-the-Trainer program wherein the ICBRNE facilitator trains specific ICBRNE users who will in turn train field users. Given the quantity of ICBRNE users the Train-the-Trainer program can be a longer term tool to insure optimum program participation.

10.2 Quick Start Guides

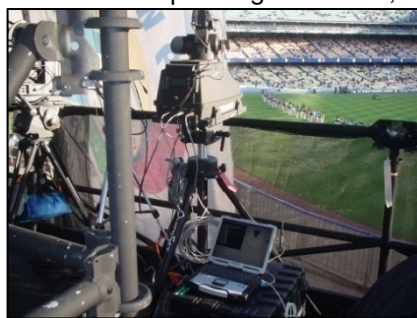
Utilization of quick start guides or cheat sheets are essential for field deployments. These guides outline a step-by-step process for software and/or hardware use so that a user can rapidly utilize the various system components without much process memorization. Appendix X provides examples of several quick start guides.

10.3 Drills/Exercises

One of the valuable tools utilized to explore the various components of the ICBRNE program are drills and exercises. These events quickly and conveniently allowed multiple agencies and/or teams the ability to share information and utilize this information to complement their activities. The ICBRNE program is an active participant in many of these activities spanning from local, state and federal level.



Rose Parades/Game



World Baseball Classic



Emmy Awards 2008-2010



USC/Ohio State & BCS



Long Beach Grand Prix
2009-2010



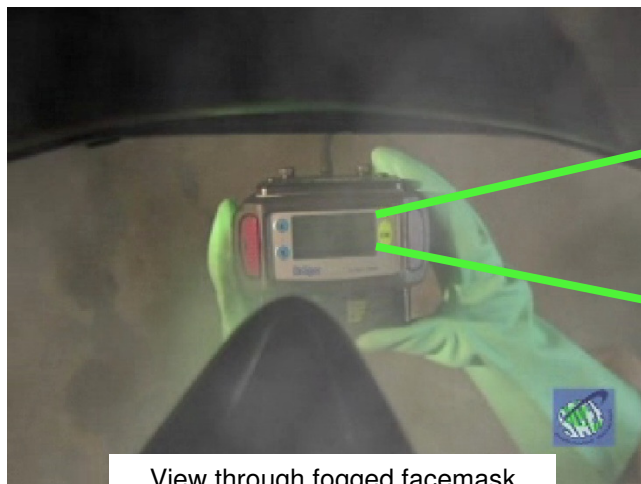
Los Angeles Regional WMD



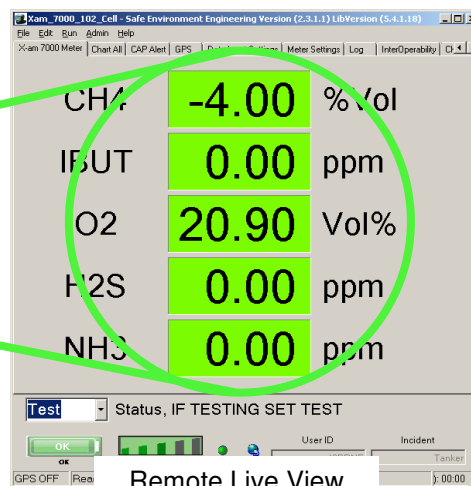
On large scale the ICBRNE program was tested in the 2010 Operation Golden Phoenix (OGP-10). OGP-10 was conducted as a series of training and exercise events that included participation by almost 800 personnel from 133 separate agencies. OGP-10 was an integrated training and exercise program that provided more than 130 local, state, and federal public safety agencies, private sector, non-governmental organizations, and military units with the opportunity to evaluate and develop their response to the detonation of an improvised nuclear device (IND). See Appendix X for the complete After Action Report. In addition to the on-site Golden Phoenix, there was a “Virtual” Golden Phoenix (VGP) where interoperability was enabled among a number of remote systems. The concept was that those who could not attend due to the geographic and time constraints might participate before, during or after the event to explore improved interoperability solutions. A report summarizing these VGP activities is available in Appendix M.

11 First Responder Safety

An attribute of the ICBRNE programs ability to move and share information are several significant safety enhancements. CBRNE responders have significant challenges trying to see instrumentation readings through layers of face masks. High humidity levels typically fog up the lenses making the small readings from the faceplates even more difficult to read. The ICBRNE program captures the instrument's readings in real-time and displays them remotely as a replica of the instrument's display. This data is monitored by trained CBRNE technical representatives who can assist.



View through fogged facemask



CBRNE instrumentation users can also have difficulty accurately reporting the correct data wherein it is easy to misreport units or decimal points. Care should also be taken when verbally reporting incident sensor data over potentially open or easily monitored radio communications. The ICBRNE architecture transmits live digital data eliminating the potential of changing a unit or decimal place such as 0.10 ppm as 0.01 ppm.



12 Force Multipliers

The ICBRNE program, as demonstrated during the Golden Phoenix exercise tabletop and simulated during the subsequent Functional Exercise, is a significant force multiplier in support of a regional response to an emergency, such as the Golden Phoenix potential nuclear incident, allowing remotely-located personnel and subject matter experts to access and utilize visualizations of live sensor data. As a tool it provided field data directly to Emergency Management to allow them to better assist and guide.

The ICBRNE system has been tested extensively at the field responder level and has proven very effective in generation of an integrated sensor picture. At the same time, it has been demonstrated as a significant force multiplier in the integration and dissemination of critical incident data, to enhance situational awareness and validate predictive models with real-time real-world information about the operational environment.

13 Implementation Process

The implementation process section is provided to bring the reader through a step-by-step guide to define what worked for the Los Angeles ICBRNE pilot program. This section identifies personnel, meetings, budgets, grants, long term and short term funding requirements, the utilization of equipment and software, training, program sustainment as well as, the augmentation of existing policies or the creation of new ones to support the ICBRNE effort. It is hoped that, through the Los Angeles ICBRNE pilot program efforts, many of the gaps and challenges have been brought forward within this document. However, with any new program gaps will be identified and remedied. This guide and the subsequent material in this report should help the facilitator expedite implementation of ICBRNE-like system and allow for a reasonably easy transition offset by significant safety and time enhancements.

An early stage method for the introduction of the ICBRNE program into a region is the identification of existing meetings wherein the foundation of the ICBRNE program can be discussed. Within this presentation it is recommended to discuss the overall concepts of ICBRNE followed by its benefits, costs associated with implementation, the time necessary both for implementation and participants followed by a discussion of what gaps ICBRNE currently fills.

In the opening discussion an overview of ICBRNE represents the project in its simplest terms. Thus far, the basic approach is to show ICBRNE as a “Universal Translator” from CBRNE instrumentation through implementation processes and procedures for Subject Matter Experts and Emergency Managers as well as the responders.

The discussion typically introduces and provides overview to the participants on the various CBRNE equipment, the challenges faced by trying to get all the dissimilar equipment to work together, followed by a discussion of the benefits created by integration of the data. This benefits section identifies the safety and time merits of ICBRNE as well as the enriched data set now acquired from the instrumentation and its subsequent utilization.

The costs component identifies the amount of time typically taken by responders and facilitators for implementation of the ICBRNE program. These costs include the time necessary for policy meetings, training, facilitation and administration.

The time component needs to expose the necessity for field testing and sustainment activities as well as the facilitation time necessary to explore the regional policies and their augmentation now that additional data are available for evaluation and action.

Throughout the process of implementation, gaps will be identified and subsequently filled. These gaps can include elements such as policy, notification, visualization and administration. Some of the significant rewards of the implementation of the ICBRNE program are the bridging of these gaps and the effectiveness the results have with the programs users and overseers.



13.1 Identify Implementer(s)

Identifying implementers is an early and important task in the ICBRNE effort. An implementer is a person or persons that facilitate the management of the ICBRNE program. This work includes coordination meetings, integration into drills/exercises, coordination of training, performing field performance audits, overseeing support documentation, media relation and management of acquired data.

This is a very rewarding and necessary job with ICBRNE because of the significance the program has as enumerated throughout this report.

13.2 Perform Instrumentation Inventory

A necessary process in the ICBRNE program implementation is creating an inventory of CBRNE assets to determine what instruments can be integrated. Typically this means a meeting with end user response organizations and facilitating an inventory audit of their instrument assets. Dispatching an inventory form to the participating agencies is an effective and efficient way of collecting this data. Information included in this inventory should include instrumentation type, manufacturer, model number, serial number, sensor configuration, probes, last calibration date, next calibration date, consumables and a short description of how the instrument is used.

13.3 Solicit Users to Input Inventory

The inventory process is not a onetime occurrence. In order to keep the inventory up to date equipment should be reviewed periodically and/or when new equipment is added and older assets taken out of service. The ICBRNE program is developing an integrated database and form tool for simple inventory asset management.

13.4 Identify Communications Architecture

The information sharing component of ICBRNE requires a network to work. The requirement of this network is that it supports Transmission Control Protocol (TCP) and Internet Protocol (IP) namely TCP/IP. Transport of this network information can occur through a variety of modalities including WiFi, cellular, Ethernet, and satellite among many others. An investigation as to the best communications medium should be performed which should include the following criteria:

- Geographical coverage distance
- Network robustness
- Network redundancy
- Penetration and propagation (indoors and outdoors)
- Bandwidth Licensed, unlicensed, Family Radio Service (FRS), standards based (IEEE)
- Network broadcast locations (towers, buildings, mobile)

Additionally important is an understanding of the end users use. Many of the current ICBRNE users are mobile and require portable networks that follow them and are used when and where needed. Others may be in a fixed location requiring network connectivity that may need to be shared with other network based services.



13.5 Create Budget

The ICBRNE program supports integration with many other systems (software & hardware). Whereas in many cases these can be existing systems, other external factors should be considered in system budgeting.

- What equipment needs telemetry?
- Do the computers need to be upgraded (is there enough RAM)?
- Are local hotspots needed for communication (vehicle/portable)?
- Is decision support software needed?
- Are network services needed (cellular)?
- What are training/installation needs?
- What are maintenance requirements?

Addressing the above issues at the onset of an integration project can save considerable time and will help ensure the project sustainment.

13.6 Identify Funding Source – Short/Long term

This funding section is to serve as a guide in revealing potential funding areas for consideration. The below list of grant options have proven to be sources throughout the history and growth of the ICBRNE Los Angeles Pilot as well as other complementary projects. Securing grant money can be a long arduous process, so the ICBRNE facilitator or others involved in the program should seek out grant managers for their region to help assist in the grant process. Consider the following sources:

- Leftover year end money
- Non encumbered funds
- Urban Area Security Initiative (UASI)
- Public Safety Interoperable Communications (PSIC)
- State Homeland Security Grant Program (SHSGP)
- Assistance to Firefighters Grant (AFG)

Once funding is secured the actual implementation process can be started. This includes the installation of software, hardware and Web services, and updating computer systems including security patches. Performing this can be a timely process depending on the state of the equipment on which systems will be installed. It is recommended that, if possible, relocating and upgrading computers to a high bandwidth Internet connection can save considerable time.

- Facilitate user/manager training
 - Multiple shifts
 - Hands on
 - Training materials (Very Important – Include Cheat Sheets)
 - Follow up training - quarterly
 - Develop/integrate smaller training exercises
- Establish reoccurring system test using participants
 - Ideal – weekly system tests in conjunction with equipment checks
 - Introduce scenarios into tests



13.7 User/Manager Training

Two levels of training should be addressed, one for users and the other for system administrators/managers. For the system administrator/manager, training primarily involves how to setup their system including network addressing, sensor firmware updates, alarm and threshold values and alert/notification program setup. User training is focused on the practical operational component of the various systems and how to perform routine tasks such as system startup, responding to alarm events, coordination with other software systems such as plume generation and guidance systems. Optimally, much of this training should be facilitated in a hands-on environment giving the users direct exposure to the systems they will be using.

For Responder training, typically three shifts are required to ensure sufficient training for all personnel.

Simple training materials are an enormously important component to longer term systems sustainment. Included in the Appendix of this report are various training materials that have been used in facilitating the ICBRNE program. One of the more important tools is the use of quick start guides. These documents summarize system operation down to the most basic steps and are typically accompanied by pictures or illustrations.

For systems sustainment, training becomes an integral force multiplier. Regular follow-on training can provide an opportunity to refresh users and administrators on systems operation and can also provide a platform to explore further integration options.

Another very positive result of systems interoperability is the ability to coordinate information sharing CBRNE scenarios. Here CBRNE events are shared between agencies wherein remote data is used to drive a multi-agency response without the formalities of a larger exercise. These smaller training events have also conveniently supported routine weekly equipment checks.

13.8 Training – Drills and Exercises

Integrated CBRNE information sharing continues to be an integral part of drills and exercises in the LA pilot. The information collected and shared has provided actionable situational data to stimulate many activities that have proven beneficial to the exercise participants. The level of available CBRNE information may need to be conveyed to exercise coordinators to ensure the capability is an active component of the planning process. Consideration of both the ICBRNE Responder and Emergency Manager role should also be factored into the design.

Briefing the ICBRNE exercise goals and objectives before the event helps maintain participant focus throughout the event. The results should then be reviewed during the “Hot Wash” to capture any lessons learned and identify areas for improvement.

13.9 Standard Operating Practices

As ICBRNE becomes part of operational procedures, amending standard operating procedures should also be addressed. By addressing these procedures in a document they are memorized and can be utilized as an operational guidance document. It is highly recommended that these additions be addressed early in development of ICBRNE throughout a region so as to give credibility to the program and instill in the users that there is backing from senior managers. The Los Angeles ICBRNE pilot program has also put in place a policy group that meets on a regular basis to review, critique, and develop policies which have been included as an appendix to this report. Examples of these policies include:

1. Participation in this program is completely voluntary and at no-cost to the participating agencies. However, each agency will have to incur its own cost to make their existing and future CBRNE sensors compliant to the telemetry standards developed by the project group.

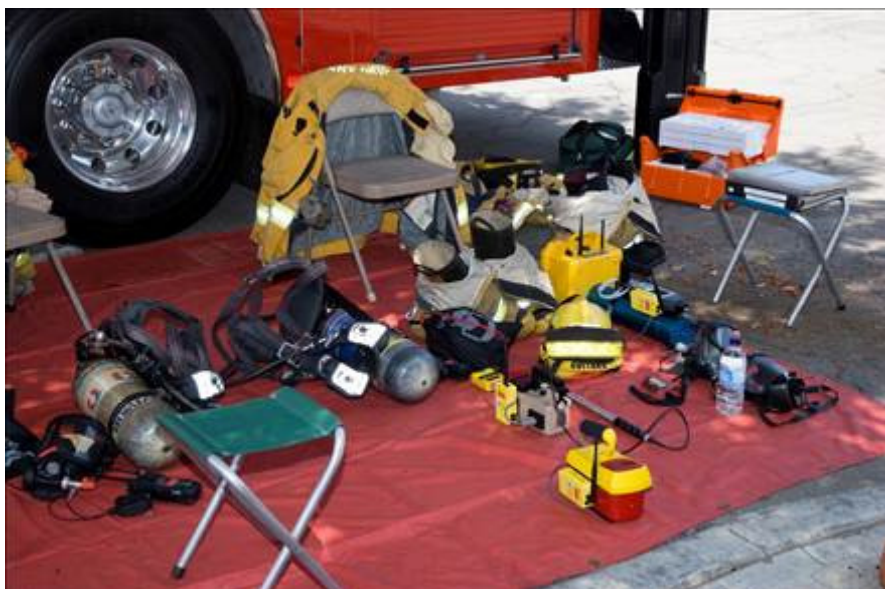


2. Alert/Notification or access to CBRNE sensor data should never to be treated as a request for resources. Request for resources will be done following existing processes.

Members addressing the SOP development should regularly perform internal audits to help identify policy gaps and address improvement opportunities.



Appendix A - Operation Golden Phoenix (Photos & Press)





Example OGP 2010 press information:

<http://www.icbrne.org/press/Operation%20Golden%20Phoenix%202010%20Information%20Guide%207-28-10.pdf>

<http://www.icbrne.org/press/Los-Angeles-Nuclear-Explo.pdf>

Appendix B - OGP After Action Report

Please request this report through the www.icbrne.org website. This information is for Official Use Only.



Appendix C - Functional Specification

Functional Requirement Specification

Real-time Interoperable CBRNE Data Telemetry Network and Information System

Summary:

This specification of a standards compliant regional wireless CBRNE data telemetry network and information system will enable coordination, collaboration, and information sharing between departments, agencies, and jurisdictions. The system will provide ground truth to emergency management operations; securely disseminate technical data and information to Subject Matter Experts located anywhere; improve the safety and effectiveness of First Responders; and provide real-time information to improve the safety and security of the general public.



(Intentionally Blank)



Table of Contents

Definitions	43
1 General Specification	45
1.1 Overview .	45
1.2 First Responders .	45
1.3 Subject Matter Experts .	45
1.4 Emergency Management & Command Operations .	46
2 Information System Architecture	47
2.1 General Network Data Security Policy Requirement.	47
2.2 Encryption Standards Compatibility Policy Requirement	47
2.3 Standard Data Telecommunication Protocol Policy Requirement .	47
2.4 Third-Party Applications & Systems Data Sharing Policy Requirement .	47
2.5 Wireless Interoperability	47
2.6 Geographic Information Systems .	48
2.7 Data Repository & System Logs	48
3 System Apparatus & Infrastructures	48
3.1 Mobile Transmission Appliances .	48
3.1.1 User Interface & Operation .	48
3.1.2 Meter Interface Options .	49
3.1.3 Wireless Network Requirement Specification.....	49
3.1.4 GPS Receiver Requirement Specification	49
3.1.5 Power Source and Sustained Operation Requirement Specification	49
3.1.6 Meters May Be Modified	49
3.1.7 Physical Characteristics.....	50
3.1.8 Thermal Tolerance Requirement Specification	50
3.1.9 Meter Compatibility List	50
3.2 Gateways, Bridges, Routers, and Third-party Appliances .	51



Definitions

The following constitute the definitions of the words, acronyms and terms used throughout this document and supersede any conflicts of meaning in general colloquial use or otherwise.

2.1	CAP:	“Common Alerting Protocol” is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks; allows a consistent warning message to be disseminated simultaneously over many different warning systems. CAP also facilitates the detection of emerging patterns in local warnings of various kinds. The CAP format is compatible with emerging techniques such as SAME used by the NWS, the EAS, and various Web services, OASIS
2.2	CBNRE:	Chemical, Biological, Nuclear, Radiological, and High Explosive
2.3	COTS:	Commercial-off-the-shelf equipment and software
2.4	DHS:	United States Department of Homeland Security
2.5	DMIS:	Disaster Management Interoperability Service (Now DM-OPEN)
2.6	DM-OPEN:	Disaster Management - Open Platform for Emergency Networks, FEMA (Formerly known as DMIS)
2.7	EAS:	Emergency Alert System - National public warning system to provide communications to inform the public during a national, state or local emergency. FEMA
2.8	EDXL-DE:	“Emergency Data Exchange Language” – “Distribution Element,” OASIS
2.9	FEMA:	Federal Emergency Management Agency
2.10	FIPS 140-2:	Federal Information Processing Standards publication 140-2, NIST
2.11	GIS:	A Geographic Information System (GIS) is a database with software that can analyze and display data using digitized maps and tables. A GIS can assemble, store, manipulate, and display geographically referenced data, tying this data to points, lines and areas on a map or in a table. For emergency managers, a GIS can facilitate critical decision-making before a disaster impacts an area in easy-to-understand formats
2.12	Interoperable:	Capable of exchange of alerts and notifications among all kinds of emergency information systems
2.13	IPAWS:	Integrated Public Alerts and Warning System
2.14	Meter:	Applicable chemical, biological, radiological, nuclear, and high explosive instruments, detectors, sensors, and identifiers, as well as human physiological sensors and various other types of sensors as may be specified
2.15	NAT:	Network Address Translation
2.16	NWS:	National Weather Service, NOAA
2.17	NOAA:	National Oceanic and Atmospheric Administration
2.18	OASIS:	Organization for the Advancement of Structured Information Standards
2.19	PC:	A desktop or notebook personal computer running Microsoft Windows XP or Microsoft Windows 7
2.20	Real-time:	Synchronization with real-world events with a latency not to exceed 1000 milliseconds (1 second) excluding network transmission latency which include variables beyond the scope of the System. (See Sample Rate)



- 2.21 SAME: Specific Area Message Encoding, NOAA
- 2.22 Sample Rate: Refers to the interval between new data samples. Data may be real-time (latency equal to or less than 1 second) and may have a sample rate of 30 seconds. This means that new data is acquired once every 30 seconds.
- 2.23 SME: Subject Matter Expert
- 2.24 System: Real-time interoperable data telemetry network and information system comprised of specialized COTS hardware and software, as well as architectural methodologies, policies, and practices.



1 General Specification

This is a Functional Requirement Specification for a real-time interoperable data telemetry network and information system comprised of specialized Commercial-Off-The-Shelf (COTS) hardware, software, and architectural methodologies, policies, and practices hereinafter referred to as the "System."

1.1 Overview

The System is to provide secure real-time actionable information in the form of remote real-time instrument console displays and shall incorporate, as needed, geographically delineated information as specified below. Remote user interfaces shall display data from a multiplicity of different COTS instruments and devices manufactured by the widest possible diversity of vendors. Such instruments and devices shall include applicable chemical, biological, radiological, nuclear, and high explosive detectors, sensors, and identifiers, as well as human physiological sensors and various other devices and sensors as may be specified (hereinafter collectively referred to as "Meters") and more particularly described below. The System is to provide the same functionality with legacy as well as new Meters.

As delivered in fulfillment of any order, the System shall acquire, parse, and format acquired data to standard data exchange protocols as herein defined. The System shall communicate such data in real-time and shall support sample rates as needed to assure network availability. The System shall also derive or synthesize information for use in each of the following modes and/or applications:

1.2 First Responders

User friendly PC software tools shall provide comprehensive remote real-time detailed data in a format suitable to enable safety supervision and technical support from a safe location. The System shall display data corresponding to the scope of all necessary data available at any user console of any Meter and the software tools shall closely resemble the display of any instrument being remotely examined. Meter data shall be represented as direct numeric readings or, as applicable, in a graphic chart that displays readings over time. Where feasible, such software shall display graphic representations of radiological spectrum suitable for analysis.

The alert status of all Meters shall be displayed using a color-coded schema, and audible alarms shall be supported at the user's option. Alert threshold parameters shall be adjustable by remote users. Wireless signal connection status, signal strength, battery charge level shall be displayed, and Meter user identification, and incident identification shall be software user configurable and displayed.

First Responder applications shall be capable of manually initiating and sending via either pre-designated or manually entered email addresses Common Alerting Protocol (CAP) messages. Such applications shall also, at the user's option, be capable of automatically initiating and sending CAP alerts that include, at a minimum: Meter Startup; Alarm State Start; Alarm State End; Error; and Meter Shutdown. Also at the user's option, the application shall send only the "Alarm Start" Message only once during any session. Such automatically initiated CAP messages may be sent as properly formatted DM-OPEN alert messages, posted to a web server, or posted to a variety of third-party message services.

The System shall have been proven in actual emergencies, and in large-scale regional exercises and interoperability trials to be suitable and valuable in First Responder safety management and technical support.

1.3 Subject Matter Experts

Comprehensive remote real-time detail shall be displayed in a readily understandable format suitable for use by technical specialists and/or Subject Matter Experts (hereinafter collectively



referred to as “SME(s).” Such real-time instrument displays shall closely resemble the numerical display of the instrument being remotely examined. The detail of the data displayed shall include the scope of all necessary and applicable readings from each and every Meter connected to the System. Readily understandable color-coded alarm indicators shall be present for each Meter, and audible alarm indication shall be optionally enabled by the user. In addition to each Meter’s numerical readings, the application shall display the wireless connection status and signal strength from each Meter’s communication device or appliance, as well as the battery level of each communication device, if any.

SMEs shall be enabled to access the System regardless of field of specialization or location providing only that there be suitable secure Internet access. They shall be enabled to access any Meter, regardless of the number of other users that may access the same Meter simultaneously.

The System shall incorporate a GIS display of the location of all Meters on a street map with satellite view if desired by the user. The make and model of each Meter shall be capable of being displayed on the map as well as each Meter’s real-time alarm status using a color-coded icon schema. Users shall be enabled to “click” on any icon to reveal Meters that may be in or near the same location (Meter clusters), as well as the GPS coordinates of each device. Navigational directions to and from the location of each Meter, as well as real-time graphical traffic congestion information, shall be available to each user.

In addition to comprehensive Meter status and readings displays, individual users shall be enabled to apply source data filters to limit the display of Meters by network nodes and by incident IDs. Each individual user shall also be enabled to apply an additional layer of source data filtration to select the specific make and model of desired Meters from a drop-down list. This Meter filtration by make and model shall apply to previously filtered as well as unfiltered data. Such data source filtration shall also automatically alter the GIS system such that Meters and nodes that are filtered shall not appear on the GIS display.

This application may incorporate similar or identical components to other elements of the System, and must have been proven in large-scale regional exercises and interoperability trials to be suitable and valuable for SMEs. To facilitate rapid deployment in the event of any emergency, application software must be freely downloadable via the Internet and easily installed by users with minimal or no technical support, and without prior distribution of any license keys or encryption dongles.

1.4 Emergency Management & Command Operations

User friendly and readily deployable PC software tools shall provide comprehensive remote real-time detailed Meter data in a format that closely resembles the display of each Meter console. The detail of the data displayed shall correspond to the scope of all necessary and applicable readings from each and every Meter connected to the System. Such tools shall have been proven in actual large-scale regional exercises and interoperability trials to be suitable and valuable in emergency operations management as well as tactical and strategic management operations.

Emergency Management personnel shall be enabled to access any Meter, regardless of the number of other simultaneous users that may access the same Meter simultaneously.

The System shall incorporate a GIS display of the location of all Meters on a street map with satellite view if desired by the user. The make and model of each Meter shall be capable of display as well as each Meter’s real-time alarm status using a color-coded icon schema. Users shall be enabled to “click” on any icon to reveal Meters that may be in or near the same location (Meter clusters), as well as the GPS coordinates of each device. Navigational directions to and from the location of each Meter, as well as real-time graphical traffic congestion information, shall be available to each user.



In addition to comprehensive Meter status and readings displays, individual users shall be enabled to apply source data filters to limit the display of Meters by network nodes and by incident IDs. Each individual user shall also be enabled to apply an additional layer of source data filtration to select the specific make and model of desired Meters from a drop-down list. This Meter filtration by make and model shall apply to previously filtered as well as unfiltered data. Such data source filtration shall also automatically alter the GIS system such that Meters and nodes that are filtered shall not appear on the GIS display.

This application may incorporate similar or identical components to other elements of the System, and must have been proven in large-scale regional exercises and interoperability trials to be suitable and valuable for Emergency Management Operations. To facilitate rapid deployment in the event of any emergency, application software must be freely downloadable via the Internet and easily installed by users with minimal or no technical support, and without prior distribution of any license keys or encryption dongles.

2 Information System Architecture

System architecture shall be consistent with generally accepted principals of data acquisition, and host/client architectures. Computing systems with human/machine interfaces shall in each instance utilize such computer Operating Systems as shall be familiar to users as well as network and desktop administrators.

2.1 General Network Data Security Policy Requirement

No sensitive or secure data or information including without limitation, Meter readings, personnel or equipment locations, or any alert or other message traffic whatsoever shall be shared by the System with any third-party Geographic Information Service provider, mapping service, or any other information service related to the delivery of location specific information by the System. All subsystems and appliances shall be protected by means of a configurable administration account including user identification and password.

2.2 Encryption Standards Compatibility Policy Requirement

All 802.11 b/g/n transmission systems shall at a minimum be 802.11i compliant and support WPA2 AES 128 bit encryption.

2.3 Standard Data Telecommunication Protocol Policy Requirement

The system shall be capable of using OASIS Common Alerting Protocol version 1.1 (CAP) and/or Emergency Data Exchange Language Distribution Element version 1.0 (EDXL-DE) data telecommunication protocols to communicate data streams, alerts, and message traffic to third-party applications. The System shall optionally support the transmission of multiple Meter datagrams formatted as CAP messages and aggregated into EDXL-DE messages by means of an additional aggregation component, as necessary

2.4 Third-Party Applications & Systems Data Sharing Policy Requirement

The System shall be capable of sharing and exchanging source telemetry data streams, alerts, and emergency notifications using appropriately conformed CAP and/or EDXL-DE protocol messages and/or streams for use by one or more third-party software applications as may from time to time be designated.

2.5 Wireless Interoperability

All data communication transport protocols shall be standard, and shall not be proprietary to any manufacturer or vendor. Wireless data communication devices in each instance shall be capable of communicating by means of third-party COTS equipment available from the widest



possible variety of different manufacturers and vendors. Wireless configuration settings shall be administered by means of a suitable Internet browser interface.

2.6 Geographic Information Systems

Geographic coordinate data and interfaces shall be compatible with a multiplicity of Graphic Information Systems (GIS) together with the data and information detail suitable for use as described in each of the above modes and/or applications as necessary or desired.

The System shall include provisions for one or more preferred GIS systems which shall, at a minimum, be compatible with typical desktop and notebook PCs running Microsoft Windows XP, Microsoft Windows 7 Operating Systems, and mobile devices including at least three types of mobile cellular telephone data sets made by different manufacturers and utilizing at least three different software operating systems. These mobile operating systems shall include, but not limited to, Apple iPhone; and, RIM Blackberry (V5 and later); and, Android (V2.1 and later).

The proposed System shall include a preferred GIS subsystem inclusive of such software and interfaces as shall be necessary to provide for integration of all of the features and services specified herein. The preferred integrated GIS subsystem may incorporate similar or identical components to other elements of the System. The preferred GIS system must have been proven in large-scale regional exercises and interoperability trials to have been suitable and valuable for the purpose to which the GIS subsystem is applied. To facilitate rapid deployment in the event of any emergency, application software must be freely downloadable via the Internet and easily installed by users with minimal or no technical support, and without prior distribution of any license keys or encryption dongles.

2.7 Data Repository & System Logs

The System shall support logging of all CAP message traffic in a central data repository. The repository shall be capable of maintaining a minimum of 500GB of discrete message traffic, or the equivalent of 30 days message traffic from a minimum of 100 concurrently connected Meters, whichever is less, for diagnostic and performance audit purposes.

3 System Apparatus & Infrastructures

User friendly and readily deployable equipment shall be provided as needed for use in combination with both new and legacy Meters. Such apparatus shall be uniform in size and function, and shall connect wirelessly to other element of the System utilizing standard 802.11b/g WiFi digital radio transceivers. Once installed, activation of such apparatus shall be by means of an "on/off" switch. No other human/machine interface shall be required to effectuate activation and use of any apparatus. Each device shall be equipped with a timer suitable to mitigate accidental activation or deactivation of the apparatus.

3.1 Mobile Transmission Appliances

To facilitate uniform accessibility and operation of the System, wireless data transmission appliances shall interface to a multiplicity of makes and models of new and legacy Meters. To the greatest extent possible, all such appliances shall be uniform in size, battery life, required user interfaces, and operational characteristics. The Mobile Transmission Appliance must have been proven in large-scale regional exercises and interoperability trials to be suitable and valuable for its designated purpose, and a minimum of fifty (50) units must now be in continuous service for a variety of Meters.

Such equipment shall conform in each and every respect with the follow requirements:

3.1.1 User Interface & Operation

Activation of Mobile Transmission Appliances shall:



- Be by means of sealed and water resistant “on/off” momentary button. No other human/machine interface shall be required to effectuate activation and use.
- Be equipped with a timer suitable to mitigate accidental activation or deactivation.
- Provide visual indicators of operational status, network connectivity, low battery condition, and GPS acquisition.

3.1.2 Meter Interface Options

Mobile wireless transmission appliances shall be optionally utilized to interface with the widest possible variety of new and legacy Meters manufactured by the widest possible variety of vendors. These appliances shall, at a minimum, provide the following data interfaces to acquire data from new and legacy Meters.

- IrDA (Infrared free space binary optical serial data)
- RS-232 (IEEE standard binary single-ended serial data)
- TTL (Transistor to Transistor Logic binary singles ended serial data)
- Ethernet (IEEE 802.3i statistical network standard)
- Bluetooth SPP (Serial Port Profile for short distance wireless data exchange)
- USB (Universal Serial Bus 1.1)

3.1.3 Wireless Network Requirement Specification

To contain costs and facilitate interoperability with the widest possible diversity of makes and models of third-party network appliances, System Mobile Transmission Appliances shall conform to the IEEE 802.11b and 802.11g license free wireless network standards.

- Each Mobile Transmission Appliance shall include a removable/replaceable 6dB gain antenna with SMA connector.
- Nominal indoor range shall be 150 feet (45.72m)
- Nominal outdoor range shall be 300 feet (91.44m)

3.1.4 GPS Receiver Requirement Specification

Each Mobile Transmission Appliance shall be equipped with a GPS (Global Positioning System) receiver with the following characteristics:

- 20 Channels
- 36 Second cold start acquisition @ -136 dBm
- Location Accuracy: 10 feet (3.05m) vertical, 15 feet (4.57) horizontal
- An external GPS SMA-RP Antenna shall be supplied

3.1.5 Power Source and Sustained Operation Requirement Specification

Mobile Transmission Appliances shall be equipped with a rechargeable and replaceable battery and shall provide at least ten (10) hours of continuous operation.

3.1.6 Meters May Be Modified

Meters may be modified by their manufacturers, as needed, provide for an appropriate data interface to a Mobile Transmission Appliance.



3.1.7 Physical Characteristics

- Mobile Transmission Appliances shall be sealed and water resistant
- The physical dimensions of the any Mobile Transmission Appliance (excluding antennas, cables, and interface connectors and modules) shall not exceed:
 - Height: 3.75" (95.25mm)
 - Width: 5.0" (127mm)
 - Thickness: 1.5" (38.1mm)
- The weight of any Mobile Transmission Appliance (excluding antennas, cables, and interface connectors and modules) shall not exceed 13 oz (368.54 grams)

3.1.8 Thermal Tolerance Requirement Specification

All Mobile Transmission Appliances shall have a nominal operating temperature range from -40°F to 185°F (-40°C to +85°C)

3.1.9 Meter Compatibility List

At a minimum, each of the following Meters shall presently be compatible:

1. Canberra PDR-77
2. Canberra Ultraradiac
3. Berkeley Nucleonics SAM940
4. Bruker Daltronics HAWK
5. Bruker Daltronics RAID-M
6. Bruker Daltronics RAID-XP
7. Draeger Safety X-am 7000
8. Draeger Safety X-am 5000
9. Draeger Safety X-am 2000
10. Drager Safety IMS
11. Environics ChemPro 100
12. Fluke 415B
13. Industrial Scientific iTX
14. Industrial Scientific MX6/4
15. Industrial Scientific VX500
16. iCX Stride
17. Ludlum 2241
18. Ludlum 2360
19. Met One Instruments EBAM
20. MSA Sirius
21. MSA Altair
22. Ortec Detective
23. Radiation Solutions RadAssist
24. Rae Systems AeraRae
25. Rae Systems ChemRae
26. Rae Systems MiniRae
27. Rae Systems MultiRae (+)
28. Rae Systems PPBRae
29. Rae Systems QRae
30. Thermo Fisher TPM-903A/B



31. Thermo Fisher DataRam
32. Thermo Fisher FH40G
33. Thermo Fisher IdentiFINDER
34. Thermo Fisher Interceptor
35. Thermo Fisher Raider
36. Thermo Fisher MDS

3.2 Gateways, Bridges, Routers, and Third-party Appliances

The System shall support and include wireless gateway bridging appliances (Gateway Appliance) for the purpose of providing aggregated access to one or more TCP/IP connections to the Internet and/or Virtual Private Network via Cellular Data Radio; Private Data Radio Network; MESH network; Satellite Transceiver; Ethernet interface (wired); and/or or local TCP/IP connection to stand-off mobile command operations in a safe location outside of a hazardous zone. The System shall be generally compatible with third-party TCP-IP network communication appliances, encryption supplicants, and other common network appliances.

The System's basic Bridge/Router Gateway shall include, as a minimum, an 802.11b/g transceiver that complies with 802.11i specifications, and a cellular transceiver for a suitable network, a router with NAT capabilities, a rechargeable Li-ion Battery, and an internal battery charger. The system is to be provided in a sealed, water resistant enclosure. It shall have a capacity to run continuously for at least 10 hours between charges.

The Gateway Appliance must have been proven in large-scale regional exercises and interoperability trials to be suitable and valuable for its designated purpose, and a minimum of fifty (50) units must now be in continuous service for a variety of Meters.



Appendix D - Testbed Frequently Asked Questions (FAQs)

These Frequently Asked Questions (FAQs) provide an easy-to-read concise set of questions and answers to explain components of the ICBRNE capability. Each pair of questions addresses a specific topic relevant for interoperability. The “What” question gives a quick overview of a capability useful for interoperability, such as “What is the DHS OPEN?” The companion “How” question explains how you use the capability, such as “How do I post my emergency message to OPEN?”. These quick answers to key interoperability questions are sufficient for a quick introduction. For those wanting more information, the “How” questions reference template forms are provided in Appendix I. Each template form provides basic drill-down information such as providing links to examples, a subject matter expert’s point of contact information, and a link to a piece of software or an XML stylesheet which enables the capability. This information is sufficient to get a better understanding and to talk to a person who has done it before. For those who want to go further, the links to the specific software examples or fill-in-the-blank stylesheets can be utilized as a convenient way to copy/paste and tryout the capability. With these appendices, the user is able to drill-down to whatever level is desired to explore the specific key components of interoperability explored as part of the ICBRNE program.

1. What are the challenges of information sharing during an emergency?

During an emergency, first responders and emergency managers from many jurisdictions (including local, regional, state, federal and sometimes international) must work together and share information. Many of these folks have not worked together on a regular basis, and each jurisdiction brings its own chosen tools and standards. There is little time to coordinate, resources are strapped, and time is of the essence. Sharing of information and interoperability of situational awareness tools and systems becomes a significant challenge.

2. What is interoperability?

Interoperability means first responders and emergency managers from many jurisdictions (including local, regional, state, federal and international) can work together toward a common goal: (a) with each using their own chosen tools and standards; (b) without requiring significant resources and (c) with each able to use their own preferred vendor solution.

3. How do we achieve interoperability?

Interoperability is achieved primarily through the use of open standards. An “open” standard is a standard developed by an organization which allows for broad membership and supports a structured, fair mechanism for accepting input and governing the development of the standard. Also important for enabling interoperability are open (non-proprietary) architectures, data converters, information publication/subscription and information networked access, documented information sharing policies and system support.

4. What is the Interoperability Testbed?

The Interoperability Test Virtual Laboratory (ITvL) is a virtual interconnection of computers with supporting infrastructure to support testing and exploration of interoperability solutions. The Department of Homeland Security (DHS) Chemical and Biological Research Division (CBRD) recently launched the ITvL with capabilities distributed across a diverse set of government and industry partners, including the Los Angeles Fire Department, the Naval Postgraduate School, the Homeland Security Systems Engineering Development Institute (HS SEDI), DHS Science and Technology (S&T) and SPAWAR Systems Center Pacific (SSC Pac). DHS created the ITvL to provide a collaborative environment for integration, testing and experimentation for information exchange between different devices, systems and applications that support



the first responder community and to foster the education, training, testing, and adoption of EDXL standards to improve interoperability of emergency systems.

The ITvL is used in support of the ICBRNE program where the testbed allows users from different backgrounds to come together, discuss and to explore the interchange of information across organizations, sensor systems, and standards. As the ICBRNE program demonstrated with the Golden Phoenix activities in the summer of FY10 ([Golden Phoenix News Video](#)), improved sharing of sensor and sensor detection-based information during an emergency can result in significant enhancements to the speed and effectiveness of a coordinated emergency response.

The focus is on widespread education and facilitation of interoperability efforts through the use of existing standards, tools, and architectures to allow all participants to improve interoperability without requiring new, proprietary, or costly additions to existing infrastructure.

The testbed is not intended to promote any specific vendor tool or capability, nor is it intended to "test" individual tools or capabilities; rather the testbed is intended to focus on the interconnections between tools and capabilities. From an interoperability perspective, members of multi-jurisdictional government agencies and organizations should be able to use their own chosen tools, vendors, and information standard formats, yet still able to share CBRNE information easily and rapidly and collaborate for effective prevention, detection, and response. The solutions needed to enable this level of interoperability can be explored in this Interoperability Testbed.

5. How can I join the Interoperability Testbed?

To join the ICBRNE please follow the instructions at:

[https://icbrne.info/icbrnewiki/index.php/Welcome to The Interoperability Testbed](https://icbrne.info/icbrnewiki/index.php/Welcome_to_The_Interoperability_Testbed)

Or send an email to edxl-help-list@lists.mitre.org; Additional information can be found at

<http://www.icbrne.org>

6. What security features are available on the ICBRNE Testbed?

Anybody can join the testbed as long as they have an appropriate local, regional, state or federal point of contact in the ICBRNE community. The data on the ICBRNE testbed is not classified, but is protected by user-authentication and SSL encryption. In the future, Single-Sign-On and PKI certificates may be added. Each agency is required to apply appropriate security features.

7. What types of information are important for Emergency Management?

Information important for emergency management includes sensor readings, alerting, patient tracking, hospital availability, resource management, situation reporting and information packaging and addressing.

8. Which open standards support Emergency Management?

The suite of emergency management standards known as the Emergency Data Exchange Language (EDXL) provide standardized formats for representing all of the major types of emergency information mentioned above. Other standards support related areas important for emergency management, such as Cursor on Target and Ucore for situational awareness, and Sensor Web Enablement for sensor information. Of special importance is the National Information Exchange Model (NIEM) which provides a process for integrating these standards into a set of message exchanges tailored for a given agency's concept of operations.

9. What can I do to participate in improving interoperability solutions in my city or organization?

Use Open Standards and Join Open Standards Organizations and Initiatives in your community, such as the Interoperability Testbed. If you are a program manager or grant author, consider putting language into your statements of work or other contract documentation stating "Open standards such as EDXL and the National Information Exchange Model (NIEM) shall be preferred and utilized for information inputs, outputs and exchanges wherever practicable. Participation in a community-supported interoperability testbed is preferred



and encouraged to ensure open standards are effectively utilized. ” The use of open standards is the key to interoperability but to learn and explore how to use those standards is what the interoperability testbed is all about. You can sign up for an account at <http://www.icbrne.org>.

10. When should I start addressing these needs?

Don't Wait! Join now and support your program or capability, get feedback from first responders, avoid costly transition costs down the road, and help prepare for the next emergency today.

11. What are “open” standards?

“Open” standards are standards produced by organizations which allow a wide diversity of organizations and/or individuals to join as members and whose processes and governance structure are visible to members and the general public and which encourage fair and reasonable contributions, feedback and approval by their members. Examples of “open” standards organizations are the Organization for the Advancement of Structured Information Systems (OASIS), the Open Geospatial Consortium (OGC), and the World Wide Web Consortium (W3C).

12. How do I participate in an open standards organization?

“Open” standards organizations are easy to join and they are extremely appreciative and supportive of their membership. Fees are usually quite reasonable, especially for non-profit, government or academic members. Most business is conducted via weekly or bi-weekly telecons of 1 hour in length. Once your organization joins, you select which member sections and committees in which you would like to participate, and then you call in and listen, learn, and contribute as desired to the ongoing discussions. Members can support various tasks in the standards development process, including editing the specifications, developing examples or other documentation, or supporting interoperability tests to advertise capabilities and benefits at selected conferences.

13. What is OASIS?

The Organization for the Advancement of Structured Information Systems (OASIS), see <http://www.oasis-open.org>, is an open standards organization which has a particular focus area on emergency management (EM). The EM Member Section is active in the development of the suite of standards known as the Emergency Data Exchange Language (EDXL). Members organize themselves into committees to collaborate on the development of standards.

14. How do I participate in OASIS?

You or your organization can join OASIS and participate in the development of these important emergency management standards. An hour every week or two is enough to participate. Your feedback and insights are not only valuable contributions to improving the standards, but they ensure that your company or organization can ensure that the standards to which industry products will be developed meet your needs as well. For more information on how to join, visit <http://www.oasis-open.org/join/membership-application.php> or simply send an email to join@oasis-open.org.

15. What is EDXL?

The Emergency Data Exchange Language (EDXL) is a suite of standards designed for efficient and effective sharing of emergency information. The EDXL standards are developed by OASIS based on requirements derived from members, including a practitioners' working group organized by the U.S. Department of Homeland Security. The EDXL standards include Common Alert Protocol (CAP), Hospital Availability (HAVE), Resource Messaging (RM), the Distribution Element (DE), and two emerging standards, Situation Reporting (Sitrep) and Tracking of Emergency Patients (TEP). To learn more about EDXL, see <http://en.wikipedia.org/wiki/EDXL>.



16. How do I use EDXL?

A good way to get started with EDXL is to learn to use the Common Alert Protocol (CAP) with the Distribution Element (DE). You can then post your information to the free messaging backbone provided by DHS known as OPEN. See Templates #1 and #2 in Appendix B to learn how to package your CAP message in a DE and how to post to OPEN. You will find free open-source parsers at http://en.wikipedia.org/wiki/EDXL_Sharp

17. What is the Common Alert Protocol (CAP)?

"The Common Alerting Protocol (CAP) standardizes the content of alerts and notifications across all hazards, including law enforcement and public safety as well as natural hazards such as severe weather, fires, earthquakes, and tsunami. Systems using CAP have shown that a single authoritative and secure alert message can quickly launch Internet messages, news feeds, television text captions, highway sign messages, and synthesized voice over automated telephone calls or radio broadcasts."

(http://www.incident.com/cookbook/index.php/CAP_Fact_Sheet)

18. How do I create a CAP message?

The simplest way to create a Common Alert Protocol (CAP) message, for exploration, is to take an existing sample message and modify it. A template is provided in Appendix B for this purpose. In addition, resources are available to assist you in this process. You can freely download open source software for reading/writing CAP messages at <http://edxlsharp.codeplex.com/>. There are online CAP validators where you can test your newly constructed CAP message to ensure it is valid on the interoperability testbed, for example at <http://209.242.167.100/validate/Message>.

19. How do I put my sensor information into a CAP message?

The ICBRNE program utilized CAP as a simple, first responder-friendly way to provide sensor alerts. The four basic components of a reading, namely the type of measurement, the value, the units of measure, and the state (red, yellow, green), can be provided in a few different locations depending on the need, including a short, condensed version in the title and/or a more modularized listing in the parameters fields. Examples of Sensor CAP messages are available on the interoperability testbed, and the format is described there at https://icbrne.info/icbrnewiki/images/3/38/CAP_Sensor_Profile_v6.doc

20. How do I "GET" CAP messages from the ICBRNE sensors?

There are several different methods to obtain sensor data from the ICBRNE testbed, but one easy way is a simple web URL. The ICBRNE Los Angeles lead, Safe Environment Engineering, has "URL" data-feeds and corresponding applications to process and view the data. In addition, SPAWAR Systems Center Pacific developed a "Representational State Transfer" (REST) implementation to allow for the posting and getting of sensor data. A detailed explanation regarding the REST implementation can be found at https://icbrne.info/icbrnewiki/index.php/ICBRNE_URL_Feeds_and_Early_Examples.

In addition, a variety of testbed partners have developed capabilities for delivering sensor data efficiently and effectively. Solace Systems has a real-time geospatial router with which you can interact, described below. And the DHS OPEN messaging backbone is available for your exploration.

21. How do I "POST" CAP messages to the ICBRNE Testbed?

Using the "Representational State Transfer" (REST) "Post", it is possible to add CAP XML messages to ICBRNE testbed. An example Java program can be found at:

https://icbrne.info/icbrnewiki/index.php/ICBRNE_URL_Feeds_and_Early_Examples. Other mechanisms are available, including posting to the Solace router or to OPEN. See Template Form #15 in Appendix B.



22. What is “Representational State Transfer” (REST) and how is it used on the ICBRNE Testbed?

REST is an approach that uses URLs and HTTP to provide access and sharing of information in a manner similar to the way you access web pages in your browser. A program specifies a URL and does an HTTP GET operation to get data. Similarly, data can be “posted” to a URL to send data. The REST approach has many advantages for learning: (a) it is easy-to-use; (b) you can test it yourself by putting the URL into your browser; (c) it is scalable; (d) it can be as secure as online-banking using web-based security mechanisms. The primary disadvantage is that the REST approach does not “push” data to you. For that purpose, you can use the Solace router or other publication/subscription mechanisms.

23. What other data formats are available on the ICBRNE testbed?

Many different information formats are utilized in the emergency management community. Several of these formats were explored as part of the ICBRNE effort, including:

- Common Alert Protocol (CAP) (For more on CAP, see http://www.incident.com/cookbook/index.php/CAP_Fact_Sheet)
- KML (a mapping standard utilized by Google Earth and others) (For more on KML, see http://code.google.com/apis/kml/documentation/kml_tut.html)
- CSV (an older style of representing data as comma separated values)
- HTML (for traditional web-based viewing of sensor information)
- Distribution Element (DE) (for addressing sensor information to a set of responders by role or by keywords) (For more on the DE, see <http://www.oasis-open.org/committees/download.php/34264/EDXL-DE-Basics-White%20Paper-18Aug09-r2.doc> and <http://en.wikipedia.org/wiki/EDXL>)
- NIEM CBRN IEPD (a flexible representation of sensor information messages utilizing multiple standards and managed by a CBRN community led by the Domestic Nuclear Detection Office (DNDO)) (For more on CBRN IEPD, see <http://www.niem.gov/CBRN.php>)
- Sensor Web Enablement (SWE, an open standard developed by the Open Geospatial Consortium, including the Observations and Measures standard which is offered as one way to view sensor readings in the testbed) (For more on SWE, see http://portal.opengeospatial.org/files/?artifact_id=25562)
- Universal Core (UCore, a standardized format for who, what, where, and when information) (For more on UCore, see <http://www.ucore.gov/>)
- Cursor-on-Target (CoT, a situational awareness format for representing the category of information and its location and time) (For more on CoT, see http://www.dodccrp.org/events/2006_CCRTS/html/papers/073.pdf)

24. What do I do to send my message once I've created it?

There are several options for posting your emergency information. First, you can use the freely available DHS messaging backbone known as OPEN. Second, you can use one of the DNDO messaging routers. Third, you can use one of the interoperability testbed partner's routing solutions, such as the MITRE IC.Net system. Fourth, you can use your own chosen commercial routing capability. Look for ones that are advertised as “EDXL-aware”. Fifth, you can make your xml messages accessible using traditional web-based techniques, such as a URL link to your XML feed. Although this latter suggestion is not a “push”



technology, it can be useful as a reference for those who weren't subscribed for the original alerts. Templates are provided in Appendix B for all of these solutions (forthcoming).

25. What is the EDXL Distribution Element (DE)?

The DE is designed to support “packaging” and addressing your emergency information. The DE carries a special importance for the EDXL family of standards because it is designed to support packing information from any of the other EDXL standards to enable effective policy-oriented access and routing. For an easy-to-read overview of the EDXL DE, see the white paper at <http://www.oasis-open.org/committees/download.php/34264/EDXL-DE-Basics-White%20Paper-18Aug09-r2.doc>.

26. How do I package my CAP message in a DE?

A template is provided to automatically package your CAP message into a DE, see Template #1 in Appendix B. In addition, you can utilize the [EDXLSharp](#) open source software for parsing and creating your CAP and DE messages. Then you can validate your message using the online [validators](#) available on the interoperability testbed.

27. How do I post to OPEN?

A template is provided to demonstrate how to post to OPEN, see Template #2 in Appendix B. The basic process, after acquiring an account, is to use a program to open a connection, post the alert to the specified group, then close the connection.

28. How do I post to Solace router?

A template is provided to demonstrate how to post to the DNDO pilot router from Solace Systems. The router is a high-speed EDXL-aware router that can support fast policy-oriented routing and fast geospatial routing. The basic process, after acquiring an account, is to use a program to post your message after wrapping it in a DE and specifying a keyword or role and a geographic location to enable smart routing. A description of the router capability and video are available on the Solace website at <http://www.solacesystems.com/solutions/content-networking/geospatial-routing>

29. What is the National Information Exchange Model (NIEM)?

The National Information Exchange Model (see <http://www.niem.gov/>) is both a set of reusable information elements and a process for how to go about integrating multiple open standards with additional information needed to support your own agency's information exchange needs. The NIEM program is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. The NIEM exchange development methodology results in a common understanding among participating organizations and data formatted in a consistent manner with a well-understood meaning. NIEM provides a support help-desk, documentation and training to help you and your agency partners to quickly develop and continue to evolve your message exchange formats. The overall goal is to help you do information exchanges without having to reinvent the wheel, by reusing the work and lessons learned of others, utilizing existing open standards, providing a process to generate your own message exchange format known as an Information Exchange Package Document (IEPD), and providing a community of support.

30. What is the CBRN IEPD?

The Chemical, Biological, Radiological and Nuclear (CBRN) Information Exchange Package Document (IEPD) is the message exchange format supporting CBRN applications. The CBRN IEPD was originally developed under the leadership of the Domestic Nuclear Detection Office (DNDO) and included the radiation and nuclear components. The DHS Science & Technology Chemical and Biological Directorate contributed components for representing chemical and biological information. The combined result is the CBRN IEPD. You can learn more and explore the use of these message exchanges by participating in the interoperability testbed and ongoing DNDO router pilot efforts.



Appendix E - Testbed Templates (SPAWAR Forms)

**Integrated Chemical Biological Nuclear Radiological
Information Sharing Templates**



Prepared for: Department Homeland Security

Prepared by: Space and Naval Warfare System Center Pacific



Executive Summary

The ICBRNE program enabled interoperability of sensor and sensor detection-based information with local, regional, state and federal systems through the use of standards. The main body of the ICBRNE Final Report provides the overview of how this was accomplished. In addition, these appendices provide an easy-to-use reference for drill-down information on specific topics of interest.

For those wanting more information, each template form provides basic drill-down information such as providing links to examples, a subject matter expert's point of contact information, and a link to a piece of software or an XML stylesheet which enables the capability. This information is sufficient to get a better understanding and to talk to a person who has done it before. For those who want to go further, the links to the specific software examples or fill-in-the-blank stylesheets can be utilized as a convenient way to copy/paste and tryout the capability. With these appendices, the user is able to drill-down to whatever level is desired to explore the specific key components of interoperability explored as part of the ICBRNE program.



Example Template Forms

Question: How to convert Common Alerting Protocol v1.2 (CAP) message to Emergency Data Exchange Language (EDXL) Distribution Element (DE) format?

Author: Jeff Waters, (619) 208-3018, jeff.waters@navy.mil

Answer In Brief: Use Extensible Stylesheet Language Transformations (XSLT) to transform the CAP XML document into a DE XML document. XSLT enables and empowers interoperability.

Template Link: See Example Template D-1 below for the XSL used for converting CAP to DE message.

How to use the template: There are two ways for using xslt to transform your XML documents, by programming or using a tool. Here is a sample Java code used for performing an XSLT transformation using the XSLT stylesheet "cap_to_de.xsl".

```
String sDEXml = XSLTransform.transformToString(sCAPXml.getBytes(), "xsl/cap_to_de.xsl", null);
```

Another way is to use a XSLT 2.0 processor like Altova to do the transformation. Sample command line:

```
altovaXML /xslt2 cap_to_de.xsl /in CAP.xml /out DE.xml
```

EXAMPLES: See Example D-2 below for a sample CAP message and Example D-3 for sample DE output after applying the XSL conversion.

BACKGROUND: "The Common Alerting Protocol (CAP) standardizes the content of alerts and notifications across all hazards, including law enforcement and public safety as well as natural hazards such as severe weather, fires, earthquakes, and tsunamis. Systems using CAP have shown that a single authoritative and secure alert message can quickly launch Internet messages, news feeds, television text captions, highway sign messages, and synthesized voice over automated telephone calls or radio broadcasts."

To Learn More:

For an overview of EDXL, see <http://en.wikipedia.org/wiki/EDXL>



For sample EDXL parsers, including CAP, see <http://edxlsharp.codeplex.com/>

A tutorial on XSLT can be found at: http://www.w3schools.com/xsl/xsl_intro.asp

The CAP 1.2 Specification: <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf>

The DE 1.0 Specification: http://docs.oasis-open.org/emergency/edxl-de/v1.0/EDXL-DE_Spec_v1.0.pdf

Intro to CAP: http://www.incident.com/cookbook/index.php/Welcome_to_the_CAP_Cookbook

XSLT Overview: <http://en.wikipedia.org/wiki/XSLT>

SME: Don McGarry, dmcgarry@mitre.org, <http://edxlsharp.codeplex.com/>

```
<?xml version="1.0" encoding="utf-8"?>
<xsl:stylesheet version="2.0"
    xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1">

    <xsl:output method="xml" indent="yes" encoding="UTF-8"/>
    <xsl:param name="DistributeID" />
    <xsl:param name="DateTimeSent" />
    <xsl:param name="DetectionType" />
    <xsl:param name="AlertType" />
    <xsl:template match="/">
        <EDXLDistribution xmlns="urn:oasis:names:tc:emergency:EDXL:DE:1.0">
            <distributionID><xsl:value-of select="$DistributeID"/></distributionID>
            <senderID>icbrne@icbrne.info</senderID>
            <dateTimeSent><xsl:value-of select="$DateTimeSent"/></dateTimeSent>
            <distributionStatus>Exercise</distributionStatus>
            <distributionType>Report</distributionType>
            <combinedConfidentiality>UNCLASSIFIED</combinedConfidentiality>
            <language>EN</language>
            <keyword>
                <valueListUrn>urn:myagency:gov:sensors:keywords</valueListUrn>
                <value><xsl:value-of select="$DetectionType"/></value>
            </keyword>
            <keyword>
                <valueListUrn>urn:myagency:gov:sensors:keywords</valueListUrn>
                <value><xsl:value-of select="$AlertType"/></value>
            </keyword>
            <targetArea>
                <xsl:copy-of select="cap:alert/cap:info/cap:area/cap:polygon"/>
            </targetArea>
            <contentObject>
                <contentDescription></contentDescription>
                <contentKeyword>
                    <valueListUrn>http://icnet.mitre.org/ValueLists/ContentKeywords</valueListUrn>
                    <value>EDXL-CAP</value>
                </contentKeyword>
            </contentObject>
        </EDXLDistribution>
    </template>
</xsl:stylesheet>
```



```

        </contentKeyword>
        <xmlContent>
            <embeddedXMLContent>
                <xsl:copy-of select="cap:alert"/>
            </embeddedXMLContent>
        </xmlContent>
    </contentObject>

    </EDXLDistribution>
</xsl:template>

</xsl:stylesheet>

```

Example Template D-1: XSL to Convert Sensor CAP to DE

```

<alert xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="urn:oasis:names:tc:emergency:cap:1.1" >
    <identifier>SEE__20100615100518_656</identifier>
    <sender>Squad X</sender>
    <sent>2010-07-07T10:05:18-07:00</sent>
    <status>System</status>
    <msgType>Alert</msgType>
    <source>Bruker Daltonik RAID-
M, Sample_RaidM14.xml, 000B5C77717F, 000D6CAE10E6, squadx.safeenv2.com</source>
    <scope>Restricted</scope>
    <note/>
    <incidents/>
    <info>
        <category>Other</category>
        <event>Meter Reading IS RED!</event>
        <urgency>Immediate</urgency>
        <severity>Severe</severity>
        <certainty>Observed</certainty>
        <audience>audience</audience>
        <expires>2010-07-08T10:05:18-07:00</expires>
        <headline>Nerve;B=0 C=0 L=0;mg/m3;Green;HSI;B=2 C=69 L=0;mg/m3;Red;Toxic;B=0
C=0 L=0;mg/m3;Green</headline>
        <description/>
        <instruction>Sensors:4,Battery:65%,SignalStrength:-10</instruction>
        <web/>
        <contact/>
        <parameter>
            <valueName>sensorStatus</valueName>
            <value>NORMAL</value>
        </parameter>
        <parameter>
            <valueName>sensorData</valueName>
            <value>empty web info section</value>
        </parameter>
        <parameter>
            <valueName>batteryLevel</valueName>

```



```

    <value>65</value>
  </parameter>
  <parameter>
    <valueName>Sensor</valueName>
    <value>Nerve ,Nerve,Bruker Daltonik RAID-M,Lib A,B=0
C=0,mg/m3,Green</value>
  </parameter>
  <parameter>
    <valueName>Sensor</valueName>
    <value>Blister ,HSI,Bruker Daltonik RAID-M,Lib A,B=2
C=69,mg/m3,Red</value>
  </parameter>
  <parameter>
    <valueName>Sensor</valueName>
    <value>Toxic ,Toxic,Bruker Daltonik RAID-M,Lib A,B=0
C=0,mg/m3,Green</value>
  </parameter>
  <area>
    <areaDesc>No Area Description</areaDesc>
    <circle>34.1626,-118.344 0</circle>
  </area>
</info>
</alert>

```

Example D-2: Sample Test Sensor Data in CAP

```

<?xml version="1.0" encoding="UTF-8"?>
<EDXLDistribution xmlns="urn:oasis:names:tc:emergency:EDXL:DE:1.0"
xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1">
  <distributionID></distributionID>
  <senderID>icbrne@icbrne.info</senderID>
  <dateTimeSent></dateTimeSent>
  <distributionStatus>Exercise</distributionStatus>
  <distributionType>Report</distributionType>
  <combinedConfidentiality>UNCLASSIFIED</combinedConfidentiality>
  <language>EN</language>
  <keyword>
    <valueListUrn>urn:myagency:gov:sensors:keywords</valueListUrn>
    <value></value>
  </keyword>
  <keyword>
    <valueListUrn>urn:myagency:gov:sensors:keywords</valueListUrn>
    <value></value>
  </keyword>
  <targetArea/>
  <contentObject>
    <contentDescription/>
    <contentKeyword>

<valueListUrn>http://icnet.mitre.org/ValueLists/ContentKeywords</valueListUrn>
    <value>EDXL-CAP</value>
  </contentKeyword>
  <xmlContent>
    <embeddedXMLContent>

```



```

<alert xmlns="urn:oasis:names:tc:emergency:cap:1.1"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <identifier> SEE__20100615100518_656</identifier>
  <sender>Squad X</sender>
  <sent>2010-07-07T10:05:18-07:00</sent>
  <status>System</status>
  <msgType>Alert</msgType>
  <source> Bruker Daltonik RAID-
M, Sample_RaidM14.xml, 000B5C77717F, 000D6CAE10E6, squadx.safeenv2.com </source>
  <scope>Restricted</scope>
  <note/>
  <incidents/>
  <info>
    <category>Other</category>
    <event>Meter Reading IS RED!</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Observed</certainty>
    <audience>audience</audience>
    <expires>2010-07-08T10:05:18-07:00</expires>
    <headline>Nerve;B=0 C=0 L=0;mg/m3;Green;HSI;B=2 C=69
L=0;mg/m3;Red;Toxic;B=0 C=0 L=0;mg/m3;Green</headline>
    <description/>
    <instruction>Sensors:4,Battery:65%,SignalStrength:-10</instruction>
    <web/>
    <contact/>
    <parameter>
      <valueName>sensorStatus</valueName>
      <value>NORMAL</value>
    </parameter>
    <parameter>
      <valueName>sensorData</valueName>
      <value>empty web info section</value>
    </parameter>
    <parameter>
      <valueName>batteryLevel</valueName>
      <value>65</value>
    </parameter>
    <parameter>
      <valueName>Sensor</valueName>
      <value>Nerve ,Nerve,Bruker Daltonik RAID-M,Lib A,B=0
C=0,mg/m3,Green</value>
    </parameter>
    <parameter>
      <valueName>Sensor</valueName>
      <value>Blister ,HSI,Bruker Daltonik RAID-M,Lib A,B=2
C=69,mg/m3,Red</value>
    </parameter>
    <parameter>
      <valueName>Sensor</valueName>
      <value>Toxic ,Toxic,Bruker Daltonik RAID-M,Lib A,B=0
C=0,mg/m3,Green</value>
    </parameter>
    <area>
      <areaDesc>No Area Description</areaDesc>
      <circle>34.1626,-118.344 0</circle>
  </info>
</alert>

```




```
</area>
</info>
</alert>
</embeddedXMLContent>
</xmlContent>
</contentObject>
</EDXLDistribution>
```

Example D-3: DE Output of Applying Template D-1 to Sensor CAP D-2

QUESTION: How to Post Messages to (and Get Messages from) DM OPEN?
AUTHOR: Jeff Waters, 619-208-3018, jeffrywaters@gmail.com
ANSWER IN BRIEF: Obtain an OPEN account by completing the Memorandum of Agreement and email to OPEN@eyestreet.com .
TEMPLATE LINK: See the Example Template D-4 and D-5 below.
HOW TO USE THE TEMPLATE: Replace any bracketed items with the specified information, for example [PUT_YOUR_DM_OPEN_PASSWORD_HERE], or [LOAD_YOUR_EDXL_FORMATTED_PAYLOAD_HERE]
EXAMPLES: Specific example code requires configuration information obtained under the Memorandum of Agreement and so is not included here.
BACKGROUND: DM OPEN is a federally-sponsored messaging backbone which is available to first responders in the United States as a solution for posting and retrieving emergency messages.
TO LEARN MORE: http://www.fema.gov/emergency/ipaws/aggregator.shtm#2 http://grandpaham.com/gpDM_OPEN.html
SME: Gary Ham, 703.899.6241, gary.ham@eyestreet.com



```
package sample;

import java.io.FileInputStream;
import java.io.IOException;
import java.io.StringWriter;
import java.io.ByteArrayInputStream;
import java.io.BufferedWriter;
import java.io.FileWriter;
import java.io.FileReader;
import java.io.BufferedReader;
import java.io.InputStream;
import java.util.Properties;
import javax.xml.soap.SOAPConnectionFactory;
import javax.xml.soap.SOAPConnection;
import javax.xml.soap.MessageFactory;
import javax.xml.soap.SOAPMessage;
import javax.xml.soap.SOAPPart;
import javax.xml.soap.SOAPEnvelope;
import javax.xml.soap.SOAPHeader;
import javax.xml.soap.Name;
import javax.xml.soap.SOAPHeaderElement;
import javax.xml.soap.SOAPElement;
import javax.xml.soap.SOAPBody;
import javax.xml.soap.SOAPBodyElement;
import javax.xml.transform.TransformerFactory;
import javax.xml.transform.Transformer;
import javax.xml.transform.Source;
import javax.xml.transform.stream.StreamResult;
import javax.xml.transform.stream.StreamSource;
import javax.xml.parsers.DocumentBuilderFactory;
import org.w3c.dom.Document;

public class ClientPostMessage {
    String m_sCAPServiceUrl = new String();
    String m_sLogonUser = new String();
    String m_sCogId = new String();

    public ClientPostMessage() {
        Properties properties = new Properties();
        try {
            FileInputStream fis = new FileInputStream("OPEN.properties");
            properties.load(fis);
            m_sCAPServiceUrl = properties.getProperty("open.capServiceUrl");
            m_sLogonUser = properties.getProperty("open.logonUser");
            m_sCogId = properties.getProperty("open.cogId");
            fis.close();

        } catch (IOException e) {
            System.err.println("Problem reading properties file, use default CAP
url.");
            m_sCAPServiceUrl =
"https://tdl.integration.fema.gov/DMOPEN_CAPService/DMOPEN_CAPService";
            m_sLogonUser = "dmopentester";
            m_sCogId = "999";
        }
    }
}
```



```
} // ClientPostMessage()

//-----
private String getXmlFromFile(String sFileName) {
    String sOut = "";
    try {
        FileReader fr = new FileReader(sFileName);
        BufferedReader br = new BufferedReader(fr);
        StringBuffer sb = new StringBuffer();
        String buffer;
        while ((buffer = br.readLine()) != null) {
            sb.append(buffer);
        }
        sOut = sb.toString();
        br.close();
        fr.close();
    }
    catch (Exception e) {
        System.err.println("An Exception Occurred: getXmlFromFile()");
        e.printStackTrace();
    }
    return(sOut);
} // getXmlFromFile()

//-----
private Document getDocument(String p_sCAPXml) {
    Document doc = null;
    try {
        // Load the XML text into a DOM Document
        DocumentBuilderFactory builderFactory =
DocumentBuilderFactory.newInstance();
        builderFactory.setNamespaceAware(true);
        InputStream stream = new ByteArrayInputStream(p_sCAPXml.getBytes());
        doc = builderFactory.newDocumentBuilder().parse(stream);
    }
    catch (Exception e) {
        System.err.println("Problem load CAP XML into DOM Document.");
    }
    return doc;
} // getDocument()

//-----
private void addDocumentToSOAPBody(SOAPBodyElement p_body, Document p_doc) {
    try {
        MessageFactory factory = MessageFactory.newInstance();
        SOAPMessage message = factory.createMessage();
        message = factory.createMessage();
        SOAPElement element = message.getSOAPBody().addDocument(p_doc);
        p_body.addChildElement(element);
    }
    catch (Exception e) {
        System.err.println(e.getMessage());
    }
} // addDocumentToSOAPBody()

//-----
```



```
public static void main (String args[]) {
    ClientPostMessage cl = new ClientPostMessage();
    String sOutputFile = "PostMessageResponse.xml";
    String sDestination = cl.m_sCAPServiceUrl;
    String sCAPXml = cl.getXmlFromFile("xml/cap.xml");
    System.out.println("-*- Destination: " + sDestination);

    try {
        // Create the connection
        SOAPConnectionFactory soapConnFactory =
SOAPConnectionFactory.newInstance();
        SOAPConnection connection = soapConnFactory.createConnection();

        // Create the actual message
        MessageFactory messageFactory = MessageFactory.newInstance();
        SOAPMessage message = messageFactory.createMessage();
        SOAPPart soapPart = message.getSOAPPart();
        SOAPEnvelope envelope = soapPart.getEnvelope();

        // Define namespace
        envelope.addNamespaceDeclaration("wsu", "http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd");
        envelope.addNamespaceDeclaration("edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
        envelope.addNamespaceDeclaration("",
"urn:oasis:names:tc:emergency:cap:1.1");

        // SOAP headers: Create and populate the header
        /*
            <soap:Header>
            <edx:CAPHeaderTypeDef>
            <edx:logonUser>xxx</edx:logonUser>
            <edx:logonCogId>yyy</edx:logonCogId>
            </edx:CAPHeaderTypeDef>
            </soap:Header>
        */
        SOAPHeader header = message.getSOAPHeader();
        if (header == null)
            header = envelope.addHeader();

        Name capHeaderName = envelope.createName("CAPHeaderTypeDef", "edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
        SOAPHeaderElement capHeaderElem =
header.addHeaderElement(capHeaderName);
        // capHeaderElem.setMustUnderstand(true);

        Name logonUserName = envelope.createName("logonUser", "edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
        SOAPElement logonUserElem =
capHeaderElem.addChildElement(logonUserName);
        logonUserElem.addTextNode(cl.m_sLogonUser);

        Name logonCogIdName = envelope.createName("logonCogId", "edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
        SOAPElement logonCogIdElem =
capHeaderElem.addChildElement(logonCogIdName);
        logonCogIdElem.addTextNode(cl.m_sCogId);
    }
}
```



```
// end of SOAP headers

// SOAP body: Create and populate the body
/*
    <soap:Body>
        <edx:postCAPRequestTypeDef>
            <alert xmlns="urn:oasis:names:tc:emergency:cap:1.1">
                ...
            </alert>
        </edx:postCAPRequestTypeDef>
    </soap:Body>
*/
SOAPBody body = envelope.getBody();

Name postCAPRequestTypeDefName =
envelope.createName("postCAPRequestTypeDef", "edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
SOAPBodyElement myBody = body.addBodyElement(postCAPRequestTypeDefName);

// Load CAP xml into DOM Document
Document doc = cl.getDocument(sCAPXml);
if (doc != null) {
    // Add CAP Document into SOAP body
    cl.addDocumentToSOAPBody(myBody, doc);
}
message.saveChanges(); // Save the message
// end of SOAP body

// Print request XML message
System.out.println("\n-----Posted message:-----\n");
message.writeTo(System.out);
System.out.println();

// Send the message and get the reply
SOAPMessage reply = connection.call(message, sDestination);

// Print response XML message
System.out.println("\n-----Response: Wrote to
PostMessageResponse.xml -----\n");
// Create the transformer
TransformerFactory transformerFactory =
TransformerFactory.newInstance();
Transformer transformer = transformerFactory.newTransformer();
// Extract the content of the reply
Source sourceContent = reply.getSOAPPart().getContent();
// Set the output for the transformation
StringWriter writer = new StringWriter();
transformer.transform(sourceContent, new StreamResult(writer));

// Write to file
BufferedWriter out = new BufferedWriter(new FileWriter(sOutputFile));
out.write(writer.toString());
out.close();

//StreamResult result1 = new StreamResult(System.out);
//transformer.transform(sourceContent, result1);
```




```
// System.out.println();

// Close the connection
connection.close();
} catch (Exception e) {
    System.err.println(e.getMessage());
}

} // main()
}
```

Example Template D-4: A Java Program for Posting a Message to IPAWS-OPEN

```
package sample;

import java.io.FileInputStream;
import java.io.IOException;
import java.io.StringWriter;
import java.io.BufferedWriter;
import java.io.FileWriter;
import java.io.ByteArrayInputStream;
import java.util.Properties;
import javax.xml.soap.SOAPConnectionFactory;
import javax.xml.soap.SOAPConnection;
import javax.xml.soap.MessageFactory;
import javax.xml.soap.SOAPMessage;
import javax.xml.soap.SOAPPart;
import javax.xml.soap.SOAPEnvelope;
import javax.xml.soap.SOAPHeader;
import javax.xml.soap.Name;
import javax.xml.soap.SOAPHeaderElement;
import javax.xml.soap.SOAPElement;
import javax.xml.soap.SOAPBody;
import javax.xml.soap.SOAPBodyElement;
import javax.xml.transform.TransformerFactory;
import javax.xml.transform.Transformer;
import javax.xml.transform.Source;
import javax.xml.transform.stream.StreamResult;
import javax.xml.transform.stream.StreamSource;

public class ClientGetMessage {
    String m_sCAPServiceUrl = new String();
    String m_sLogonUser = new String();
    String m_sCogId = new String();

    public ClientGetMessage() {
        Properties properties = new Properties();
        try {
            FileInputStream fis = new FileInputStream("OPEN.properties");
            properties.load(fis);
        } catch (IOException e) {
            // Handle exception
        }
    }
}
```



```
m_sCAPServiceUrl = properties.getProperty("open.capServiceUrl");
m_sLogonUser = properties.getProperty("open.logonUser");
m_sCogId = properties.getProperty("open.cogId");
fis.close();

} catch (IOException e) {
    System.err.println("Problem reading properties file, use default CAP
url.");
    m_sCAPServiceUrl =
"https://tdl.integration.fema.gov/DMOPEN_CAPService/DMOPEN_CAPService";
    m_sLogonUser = "dmopentester";
    m_sCogId = "999";
}
} // ClientGetMessage()

//-----
public static void main (String args[]) {
    ClientGetMessage cl = new ClientGetMessage();
    String sOutputFile = "GMessageResponse.xml";
    String sDestination = cl.m_sCAPServiceUrl;
    System.out.println("-*- Destination: " + sDestination);

    String sCapId = args[0];
    // If no CAP id passed in, use default CAP id
    if ("${id}".equals(sCapId))
        sCapId = "gh_eas_003_16feb1";
    System.out.println("-*- CAP Id: " + sCapId);

    try {
        // Create the connection
        SOAPConnectionFactory soapConnFactory =
SOAPConnectionFactory.newInstance();
        SOAPConnection connection = soapConnFactory.createConnection();

        // Create the actual message
        MessageFactory messageFactory = MessageFactory.newInstance();
        SOAPMessage message = messageFactory.createMessage();
        SOAPPart soapPart = message.getSOAPPart();
        SOAPEnvelope envelope = soapPart.getEnvelope();

        // Define namespace
        envelope.addNamespaceDeclaration("wsu", "http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd");
        envelope.addNamespaceDeclaration("edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
        envelope.addNamespaceDeclaration("req",
"http://gov.fema.dmopen.services/caprequest");

        // SOAP headers: Create and populate the header
        /*
        <soap:Header>
            <edx:CAPHeaderTypeDef>
                <edx:logonUser>dmopentester</edx:logonUser>
                <edx:logonCogId>999</edx:logonCogId>
            </edx:CAPHeaderTypeDef>
        </soap:Header>
```



```
*/
SOAPHeader header = message.getSOAPHeader();
if (header == null)
    header = envelope.addHeader();

Name capHeaderName = envelope.createName("CAPHeaderTypeDef", "edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
SOAPHeaderElement capHeaderElem = header.addHeaderElement(capHeaderName);
// capHeaderElem.setMustUnderstand(true);

Name logonUserName = envelope.createName("logonUser", "edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
SOAPElement logonUserElem = capHeaderElem.addChildElement(logonUserName);
logonUserElem.addTextNode(cl.m_sLogonUser);

Name logonCogIdName = envelope.createName("logonCogId", "edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
SOAPElement logonCogIdElem =
capHeaderElem.addChildElement(logonCogIdName);
logonCogIdElem.addTextNode(cl.m_sCogId);
// end of SOAP headers

// SOAP body: Create and populate the body
/*
<soap:Body>
  <edx:getMessageTypeDef>
    <req:requestAPI>CAP11</req:requestAPI>
    <req:requestOperation>getMessage</req:requestOperation>
    <req:parameters>
      <req:parameterName>identifier</req:parameterName>
      <req:comparisonOp>equalto</req:comparisonOp>
      <req:parameterValue>gh_eas_003_16feb1</req:parameterValue>
      <req:logicalOp></req:logicalOp>
    </req:parameters>
  </edx:getMessageTypeDef>
</soap:Body>
*/
SOAPBody body = envelope.getBody();
Name requestTypeDefName = envelope.createName("getMessageTypeDef", "edx",
"http://gov.fema.dmopen.services/DMOPEN_CAPService/");
SOAPBodyElement requestTypeDefElem =
body.addBodyElement(requestTypeDefName);

Name requestAPIName = envelope.createName("requestAPI", "req",
"http://gov.fema.dmopen.services/caprequest");
SOAPElement requestAPIElem =
requestTypeDefElem.addChildElement(requestAPIName);
requestAPIElem.addTextNode("CAP11");

Name requestOperationName = envelope.createName("requestOperation", "req",
"http://gov.fema.dmopen.services/caprequest");
SOAPElement requestOperationElem =
requestTypeDefElem.addChildElement(requestOperationName);
requestOperationElem.addTextNode("getMessage");
```



```
Name requestParameters = envelope.createName("parameters", "req",
"http://gov.fema.dmopen.services/caprequest");
SOAPElement requestParametersElem =
requestTypeDefElem.addChildElement(requestParameters);

Name requestParameterName = envelope.createName("parameterName", "req",
"http://gov.fema.dmopen.services/caprequest");
SOAPElement requestParameterElem =
requestParametersElem.addChildElement(requestParameterName);
requestParameterElem.addTextNode("identifier");

Name requestComparisonOpName = envelope.createName("comparisonOp", "req",
"http://gov.fema.dmopen.services/caprequest");
SOAPElement requestComparisonOpElem =
requestParametersElem.addChildElement(requestComparisonOpName);
requestComparisonOpElem.addTextNode("equalto");

Name requestParameterValueName = envelope.createName("parameterValue",
"req", "http://gov.fema.dmopen.services/caprequest");
SOAPElement requestParameterValueElem =
requestParametersElem.addChildElement(requestParameterValueName);
requestParameterValueElem.addTextNode(sCapId);

Name requestLogicalOpName = envelope.createName("logicalOp", "req",
"http://gov.fema.dmopen.services/caprequest");
requestParametersElem.addChildElement(requestLogicalOpName);
message.saveChanges();    // Save the message
// end of SOAP body

// Print request XML message
System.out.println("\n-----Request:-----\n");
message.writeTo(System.out);
System.out.println();

// Send the message and get the reply
SOAPMessage reply = connection.call(message, sDestination);

// Print response XML message
System.out.println("\n-----Response: Wrote to GMessageResponse.xml ----
-----\n");
// Create the transformer
TransformerFactory transformerFactory = TransformerFactory.newInstance();
Transformer transformer = transformerFactory.newTransformer();
// Extract the content of the reply
Source sourceContent = reply.getSOAPPart().getContent();
// Set the output for the transformation
StringWriter writer = new StringWriter();
transformer.transform(sourceContent, new StreamResult(writer));

// Write to file
BufferedWriter out = new BufferedWriter(new FileWriter(sOutputFile));
out.write(writer.toString());
out.close();

// --- Write to standard output
// StreamResult result1 = new StreamResult(System.out);
```



```
// transformer.transform(sourceContent, result1);  
// System.out.println();  
  
// Close the connection  
connection.close();  
} catch (Exception e) {  
    System.err.println(e.getMessage());  
}  
}  
// main()  
}
```

Example Template D-5: A Java Program for Getting a Message from IPAWS-OPEN

QUESTION: How do you develop a Testbed for ICBRNE?

AUTHOR: Bruce Plutchak bruce.plutchak@navy.mil

ANSWER IN BRIEF: - SPAWAR Systems Center (SSC) Pacific (See <http://www.public.navy.mil/spawar/Pages/default.aspx>.)

SSC is the testbed lead for the ICBRNE program. SSC, along with its partners, has enabled a powerful mechanism for exploration, education, and testing of system-to-system interoperability utilizing standards and open architectures. The focus of the standardization effort is on EDXL and NIEM CBRN IEPD. The testbed includes important infrastructure components including a wiki, a RESTful repository, and routines for converting to various standard formats, and helpful links and educational material for learning EDXL.

The testbed approach is to enable interconnectivity of existing organizational users and their capabilities over the internet. The testbed approach also is to enable interoperability by providing a set of infrastructure capabilities, including a CBRN detection repository with a RESTful interface including translators to convert from one standard format into another. Other forms of infrastructure are also envisioned to enable users to obtain access to information in their desired formats to explore interoperability easily and effectively.

Any testbed participant has the opportunity to interoperate with sensor detections in a variety of formats accessible via URLs. A variety of visualizations are enabled, including Google Earth Overlays. A RESTful interface provides programmatic access to the repository for getting or posting data, with web-based encryption and authentication. The wiki provides educational information and status/progress reports on current activities by participants.



TEMPLATE LINK:	http://www.icbrne.org
HOW TO USE THE TEMPLATE:	The testbed can be utilized by requesting an account at http://www.icbrne.org . The testbed can be recreated by installing the Mediawiki and the specified software components to enable the data repository and format converters.
EXAMPLES:	The testbed resides at http://www.icbrne.org
BACKGROUND:	SSC is the Navy's premiere RDT&E System Center for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).
TO LEARN MORE:	http://icbrne.org/testbed_about.htm https://icbrne.info/icbrnewiki/index.php/Welcome to The Interoperability Testbed
SME:	bruce.plutchak@navy.mil , 619-553-3658



QUESTION: How do you create an “Energy Gradient” overlay using ICBRNE sensor data?

AUTHOR: Bruce Plutchak bruce.plutchak@navy.mil

ANSWER IN BRIEF: It is fairly easy, with multiple sensor readings, in various locations to create an “Energy Gradient” contour plot similar to similar to gradients developed by “Plume Modeling” software, but using actual data, to determine the realtime extent of the plume. The quality of the resulting “Energy Gradient” is determined the number of sensors in the field to create a realistic view of the data. It is also critical that the sensors are calibrated to output relative data. The “Energy Gradient” can be represented in multiple forms, for example by a “surface” or “contour” plot. The tool “Matlab” or the freeware version “Octave” can generate the graphical versions, and with the addition of a “GoogleEarth-Matlab” toolbox, KML files can be generated to be displayed on the tool “GoogleEarth”.

TEMPLATE: See the Example Template D-6 below as well as the instructions below on how to use the template.

HOW TO USE THE TEMPLATE:

1) Install Octave: Download Octave-3.2.2_i686-pc-mingw32_gcc-4.3.0_setup.exe or Matlab.

2) Download the the GoogleEarth Matlab toolkit

<http://code.google.com/p/googleearthtoolbox/>

3) Create CSV Data File "mydata.dat" LAT-LONG-Elevation-Magnitude

34.053,-118.292,0,328.8

34.059,-118.297,0,333.91

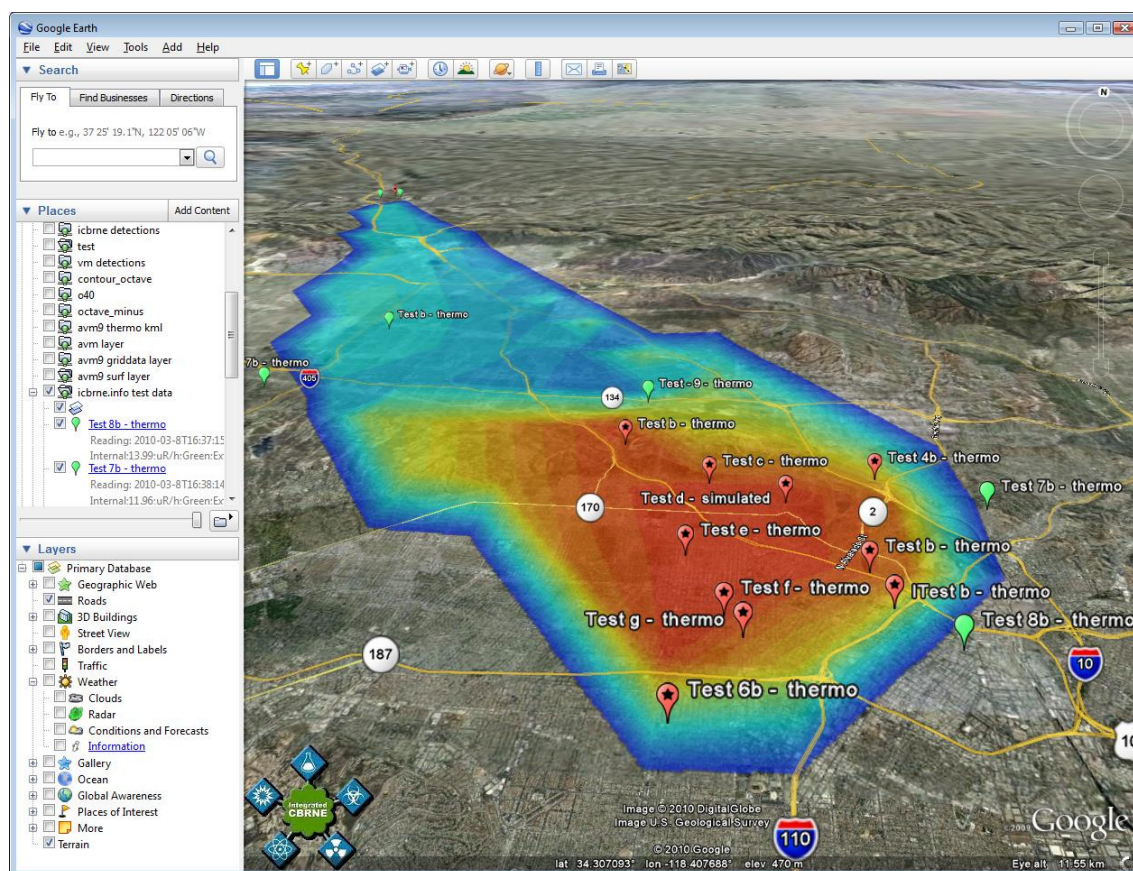
34.079,-118.309,0,337.02

.....

4) Run -> [Contour.m Octave/MATLAB Source](#) (The source code is also shown in Example Template D-6 below)

5) Load output KML file "contourbeta.kml" into GoogleEarth as local network Link.

EXAMPLES: The image below is an example of the gradient contour.



BACKGROUND:

For info on Matlab and contour plotting, see

<http://www.mathworks.com/help/techdoc/ref/contour.html>

For info on Matlab and plotting to KML for GoogleEarth, see

<http://www.mathworks.com/help/toolbox/map/ref/kmlwrite.html>



TO LEARN MORE:

https://icbrne.info/icbrnewiki/index.php/NEW_Sensor_Map_Overlays

https://icbrne.info/icbrnewiki/index.php/Google_Earth_Overlays

<http://code.google.com/apis/kml/documentation/>

<http://www.google.com/earth/index.html>

<http://www.gnu.org/software/octave/>

<http://www.mathworks.com/products/matlab/>

SME: bruce.plutchak@navy.mil, 619-553-3658

```
addpath('c:\ge_toolbox\googleearth\');

fid = fopen('mydata.dat','r');

[ Val, count] = fscanf(fid,'%f,%f,%f,%f');
fclose(fid);
num = size(Val,1)/4
Val = reshape(Val,4,num);
DataLat = Val(1,:);
DataLon = Val(2,:);
Val(4,:)
DataValue = log10(Val(4,:))

n = length(DataValue);

x=-118.7;
xplus = 0.03
xnum = 24;

y=33.8
yplus=0.03;
ynum=24;

tlon = x:xplus:x+xplus*xnum;
tlat = y:yplus:y+yplus*ynum;

[Xo,Yo] = meshgrid(tlon,tlat);
Zo = griddata(DataLon.',DataLat.',DataValue.',Xo,Yo,'linear');

xsize = size(tlon.',1);
ysize = size(tlat.',1) ;
```



```
for jj=1:xsize
    for kk=1:ysize
        if( isnan( Zo(jj,kk) ))
            Zo(jj,kk) = 0;
        end
    end
end

cMapColor = 'jet';
C = colormap(cMapColor);

for ii=1:10
    C(ii,1) = .2;
    C(ii,2) = .2;
    C(ii,3) = .2;
end

lineValues = [0:.1:3];

kmlStr = ge_contourf(Xo,Yo,Zo,...
    'cMap',C,...
    'lineValues',lineValues,...
    'polyAlpha','AA',...
    'lineColor','00FFFFFF',...
    'altitude',1e4,...
    'altitudeMode','clampToGround',...
    'cLimHigh',3,...
    'cLimLow',0);

ge_output('contourbeta.kml',kmlStr);
```

Example Template D-6: A Matlab Program for Creating a Gradient Countour (KML)



QUESTION: How do you “get” alerts (using the RESTful interface)?

AUTHOR: Jeff.Waters@navy.mil, 619-553-3657

ANSWER IN BRIEF:

Simply use the specified URL with parameters in your browser or, to access the alerts programmatically, you can do an HTTP GET with the same URL. For example, the following URL will return sensor detections in the Common Alert Protocol (CAP) format:

<https://icbrne.info/icbrne/detections/?form=cap>

TEMPLATE: The template format is:

[https://icbrne.info/icbrne/detections/?history=\[#ofDetections\]&start=\[#ofDays\]&form=\[outputtype\]](https://icbrne.info/icbrne/detections/?history=[#ofDetections]&start=[#ofDays]&form=[outputtype])

HOW TO USE THE TEMPLATE: <https://icbrne.info/icbrne/detections/?form=cap>

The format is:

[https://icbrne.info/icbrne/detections/?history=\[#ofDetections\]&start=\[#ofDays\]&form=\[outputtype\]](https://icbrne.info/icbrne/detections/?history=[#ofDetections]&start=[#ofDays]&form=[outputtype])

Optional parameters include:

history=[# of readings to return for each sensor] (Default: 1)

start=[# of past days to search for detections] (Default: 365)

form=[cap htмлlist kml edxl jsonxml]

incident=[SearchString] (The SearchString must be in the CAP to be returned)

- Retrieve Directory Contents (Via WebBrowser) of the location testdata.
 - Open the URL: <https://icbrne.info/icbrne/detection/>
- Retrieve Data (Single Sensor) (Via WebBrowser)
 - Open the URL: <https://icbrne.info/icbrne/detections/<repositorylocation>>



Retrieve Data (Multiple CAPS)

EXAMPLES: <https://icbrne.info/icbrne/detections/?form=cap>

<https://icbrne.info/icbrne/detections/?form=htmllist>

<https://icbrne.info/icbrne/detections/?form=kml>

BACKGROUND: REST is a simple way to access information using the same technique used everyday by web users when they access their web pages. Utilizing web standards, a simple URL using HTTP or HTTPS allows you to easily get the information you need.

TO LEARN MORE:

About REST: http://en.wikipedia.org/wiki/Representational_State_Transfer

About REST for sensor data:

https://icbrne.info/icbrnewiki/index.php/RESTful_Design_for_CBRNE_Applications

SME: Jeff.Waters@navy.mil, 619-553-3657

QUESTION: How do you use the Safe Environment Engineering GET Realtime data feed?

AUTHOR: Bruce.Plutchak@navy.mil

ANSWER IN BRIEF: Use the specified URL to GET the realtime Los Angeles region sensor feed from Safe Environment Engineering.

TEMPLATE LINK:

<http://icbrne.info/caphandler/Handler.ashx?un=<user>&pw=<password>==&type=getlastreading>



&cap=all

HOW TO USE THE TEMPLATE: Contact David Lamensdorf at the number below to obtain a username and password. Then use the template link provided above, inserting your username and password.

EXAMPLES: A login and password is required to see examples. Contact davidl@safeenv.com.

BACKGROUND: Safe Environment Engineering is the DHS ICBRNE lead for Los Angeles.

TO LEARN MORE: Visit <http://www.safeenv.com>

SME: David Lamensdorf, davidl@safeenv.com, 661-295-5500

QUESTION: How do you use the ICBRNE CAP Transforms?

AUTHOR: Jeff Waters, Jeff.Waters@navy.mil

ANSWER IN BRIEF: For a given sensor detection, a URL is available and the desired output format can be tacked onto the URL using the format specified below. The available outputformats include Common Alert Protocol (cap), Ucore (ucore), OASIS Distribution Element 1.0 (de), HTML (html), KML (kml), JSON (jsonxml), and GeoRSS (georss).

TEMPLATE LINK: The XSL transforms are provided in the Example Templates below:

Example Template D-7: Converting Sensor Data from CAP to Cursor-on-Target

Example Template D-8: Converting Sensor Data from CAP to GeoRSS

Example Template D-9: Converting Sensor Data from CAP to HTML

Example Template D-10: Converting Sensor Data from CAP to N25

Example Template D-11: Converting Sensor Data from CAP to KML

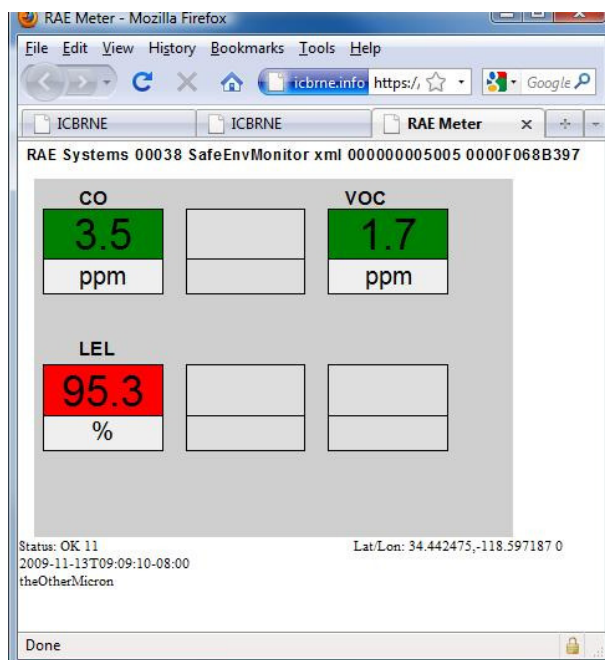
Example Template D-12: Converting Sensor Data from CAP to RDF

Example Template D-13: Converting Sensor Data from CAP to RSS



Example Template D-14: Converting Sensor Data from CAP to SWE – O & M
Example Template D-15: Converting Sensor Data from CAP to UCore

EXAMPLE:



Sensor Data from CAP to HTML

HOW TO USE THE TEMPLATE: See XSL instructions from previous templates.

BACKGROUND: Interoperability is achieved when each organizations can share information using their own chosen systems and standards. These converters enable the interoperability by allowing conversion from the Sensor CAP format to the specified format.

TO LEARN MORE: Visit <http://www.icbrne.org>.

SME: Henry Dong, henry.dong@navy.mil



```
<?xml version="1.0"?>
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1">
  <!-- <xsl:output method="xml" omit-xml-declaration="no"/> -->
  <xsl:output method="xml" indent="yes" encoding="UTF-8"/>
  <xsl:template match="/">
    <xsl:apply-templates />
  </xsl:template>

  <!-- Matches all attributes and all nodes being children of other nodes
and copies them over -->
  <xsl:template match="@*|node()">
    <xsl:copy>
      <xsl:apply-templates select="@*|node()"/>
    </xsl:copy>
  </xsl:template>

  <!-- Matches CAP message, transforms to Cursor on Target -->
  <xsl:template match="cap:alert">
    <event xsl:use-attribute-sets="eventAttributes">
      <point xsl:use-attribute-sets="pointAttributes"/>
      <detail>
        <remarks source="ICBRNE">
          <xsl:copy-of select="."/>
        </remarks>
      </detail>
    </event>
  </xsl:template>

  <xsl:variable name = "expires" select="//*[name()='expires']" />
  <xsl:variable name = "sent" select="//*[name()='sent']" />
  <xsl:variable name = "source" select="//cap:alert/cap:source" />
  <!-- Gets the mac id in the third token -->
  <xsl:variable name="macId" select="tokenize(normalize-space($source),
',,')"/>
  <xsl:attribute-set name="eventAttributes">
    <xsl:attribute name="version">2.0</xsl:attribute>
    <xsl:attribute name="uid">ICBRNE-<xsl:value-of select="$macId[3]" />
  </xsl:attribute>
    <xsl:attribute name="type">a-f-X-i-m</xsl:attribute>
    <xsl:attribute name="how">h-g-i-g-o</xsl:attribute>
    <xsl:attribute name="time"> <xsl:value-of select="$sent" />
  </xsl:attribute>
    <xsl:attribute name="start"> <xsl:value-of select="$sent" />
  </xsl:attribute>
    <xsl:attribute name="stale"> <xsl:value-of select="$expires" />
  </xsl:attribute>
  </xsl:attribute-set>

  <xsl:variable name = "circle"
select="//cap:alert/cap:info/cap:area/cap:circle" />
  <!-- if there is a comma between lat and lon, converts it to a space -->
  <xsl:variable name="values" select="translate($circle, ',', ' ')" />
  <!-- parses for Lat/Lon from the 'circle' tag in the CAP message -->
```



```

<xsl:variable name="latLon" select="tokenize(normalize-space($values), '
')"/>
<xsl:attribute-set name="pointAttributes">
  <xsl:attribute name="lat">
    <xsl:value-of select="$latLon[1]" /> <!-- Latitude -->
  </xsl:attribute>
  <xsl:attribute name="lon">
    <xsl:value-of select="$latLon[2]" /> <!-- Longitude -->
  </xsl:attribute>
  <xsl:attribute name="ce">0</xsl:attribute>
  <xsl:attribute name="hae">0</xsl:attribute>
  <xsl:attribute name="le">0</xsl:attribute>
</xsl:attribute-set>
</xsl:stylesheet>

```

Example Template D-7: Converting Sensor Data from CAP to Cursor-on-Target

```

<?xml version="1.0"?>
<xsl:stylesheet version="2.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns="http://www.w3.org/2005/Atom"
  xmlns:ms="urn:schemas-microsoft-com:xsl"
  xmlns:georss="http://www.georss.org/georss"
  xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1">
  <xsl:output method="xml" indent="yes" encoding="UTF-8"/>

  <xsl:variable name="emptySpace">
    <xsl:text>&#160;</xsl:text>
  </xsl:variable>

  <xsl:param name="CurDateTime" />

  <xsl:template match="/">
    <feed>
      <title>ICBRNE</title>
      <subtitle>Integrated Chemical, Biological, Radiological,
Nuclear and Explosive Program</subtitle>
      <link href="http://icbrne.org/" />
      <updated><xsl:value-of select="$CurDateTime" /></updated>

      <author>
        <name>David Lamensdorf</name>
        <email>davidl@safeenv.com</email>
      </author>
      <id></id>
      <xsl:apply-templates select="alerts/cap:alert" />
    </feed>
  </xsl:template>

  <xsl:template match="cap:alert">

```



```

    <entry>
      <title><xsl:value-of select="cap:source" /></title>
      <link href="http://icbrne.org" />
      <id><xsl:value-of select="cap:identifier" /></id>
      <updated><xsl:value-of select="cap:sent" /></updated>
      <summary><xsl:value-of select="cap:info/cap:headline"
/></summary>
      <xsl:apply-templates select="cap:info/cap:area/cap:circle"/>
    </entry>
  </xsl:template>

  <xsl:template match="cap:circle">
    <xsl:call-template name="LatAndLon" >
      </xsl:call-template>
    </xsl:template>

    <xsl:template name="LatAndLon">
      <xsl:variable name = "circle" select="." />
      <!-- if there is a comma between lat and lon, converts it to a space
-->
      <xsl:variable name="values" select="translate($circle, ',' , ' ' )"/>
      <!-- parses for Lat/Lon from the 'circle' tag in the CAP message -->
      <
        <xsl:variable name="latLon" select="tokenize(normalize-
space($values), ' ' )"/>
        <georss:point><xsl:value-of select="$latLon[1]" /> <xsl:value-of
select="$emptySpace"/> <xsl:value-of select="$latLon[2]" /></georss:point>

      </xsl:template>
    </xsl:stylesheet>

```

Example Template D-8: Converting Sensor Data from CAP to GeoRSS

```

<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:fo="http://www.w3.org/1999/XSL/Format"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:fn="http://www.w3.org/2005/xpath-functions">

  <!--<xsl:namespace-alias stylesheet-prefix="cap" result-prefix="xsl"/> -->

  <xsl:template match="/" xml:space=" ">

    <html>
    <body>

      <xsl:for-each select="/*[local-name()='alert']" > <!-- alert loop -->

        <table border="1" cellpadding="4" width="100%">

```



```

        <th bgcolor="#ff1111" colspan="2">ALERT MESSAGE</th>
        <tr><th width="15%" bgcolor="#6a9a9a">Identifier</th><td
width="85%"><xsl:value-of select=".[*[local-name()='identifier']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Sender</th><td><xsl:value-of
select=".[*[local-name()='sender']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Sent</th><td><xsl:value-of select=".[*[local-
name()='sent']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Status</th><td><xsl:value-of
select=".[*[local-name()='status']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Msg Type</th><td><xsl:value-of
select=".[*[local-name()='msgType']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Source</th><td><xsl:value-of
select=".[*[local-name()='source']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Scope</th><td><xsl:value-of select=".[*[local-
name()='scope']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Restriction</th><td><xsl:value-of
select=".[*[local-name()='restriction']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Notes</th><td><xsl:value-of select=".[*[local-
name()='notes']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Addresses</th><td><xsl:value-of
select=".[*[local-name()='addresses']]" /></td></tr>
        <tr><th bgcolor="#aaaaaa">Incidents</th><td><xsl:value-of
select=".[*[local-name()='incidents']]" /></td></tr>
    </table>

    <h5/>

    <table border="1" cellpadding="4" width="100%">
        <th bgcolor="#ffffdf" colspan="2">Handling Codes</th>
        <tr bgcolor="#aaaaaa">
            <th width="100%" align="left">Value</th>
        </tr>
        <xsl:for-each select=".[*[local-name()='code']]" >
            <tr>
                <td width="100%"><xsl:value-of select="."/></td>
            </tr>
        </xsl:for-each>
    </table>

    <h5/>

    <xsl:for-each select=".[*[local-name()='info']]" >

        <table border="3" cellpadding="9" width="100%">
            <th bgcolor="#2a9f9a" colspan="2">INFORMATION</th>
            <tr>

                <table border="1" cellpadding="4" width="100%">
                    <th bgcolor="#ffffdf" colspan="2"></th>
                    <tr><th width="15%" bgcolor="#9a6a9a">Onset</th><td
width="85%"><xsl:value-of select=".[*[local-name()='onset']]" /></td></tr>

```




```

        <tr><th bgcolor="#aaaaaa">Effective</th><td><xsl:value-of
select=".*[local-name()='effective']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Expires</th><td><xsl:value-of
select=".*[local-name()='expires']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Urgency</th><td><xsl:value-of
select=".*[local-name()='urgency']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Severity</th><td><xsl:value-of
select=".*[local-name()='severity']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Certainty</th><td><xsl:value-of
select=".*[local-name()='certainty']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Language</th><td><xsl:value-of
select=".*[local-name()='language']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Category</th><td><xsl:value-of
select=".*[local-name()='category']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Headline</th><td><xsl:value-of
select=".*[local-name()='headline']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Instruction</th><td><xsl:value-of
select=".*[local-name()='instruction']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Contact</th><td><xsl:value-of
select=".*[local-name()='contact']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Event</th><td><xsl:value-of
select=".*[local-name()='event']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Audience</th><td><xsl:value-of
select=".*[local-name()='audience']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Response Type</th><td><xsl:value-of
select=".*[local-name()='responseType']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Sender Name</th><td><xsl:value-of
select=".*[local-name()='senderName']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Web URI</th><td><xsl:value-of
select=".*[local-name()='web']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Description</th><td><xsl:value-of
select=".*[local-name()='description']"/></td></tr>
    </table>

    <h5/>
    <table border="1" cellpadding="4" width="100%">
        <tr><th colspan="2" bgcolor="#ffffdf">Event Codes</th>
        <tr><th colspan="2" bgcolor="#aaaaaa">
            <th width="15%">Name</th>
            <th width="85%" align="left">Value</th>
        </tr>
        <xsl:for-each select=".*[local-name()='eventCode']">
            <tr>
                <td><xsl:value-of select=".*[local-
name()='valueName']"/></td>
                <td><xsl:value-of select=".*[local-name()='value']"/></td>
            </tr>
        </xsl:for-each>
    </table>

    <h5/>
    <table border="1" cellpadding="4" width="100%">
        <tr><th colspan="2" bgcolor="#ffffdf">Parameters</th>
        <tr><th colspan="2" bgcolor="#aaaaaa">
            <th width="15%">Name</th>
            <th width="85%" align="left">Value</th>
        </tr>
    </table>

```



```

        <xsl:for-each select=".*[local-name()='parameter']" >
            <tr>
                <td><xsl:value-of select=".*[local-
name()='valueName']"/></td>
                <td><xsl:value-of select=".*[local-name()='value']"/></td>
            </tr>
        </xsl:for-each>
    </table>

    <xsl:for-each select=".*[local-name()='resource']" >
        <h5/>
        <table border="1" cellpadding="4" width="100%">
            <th bgcolor="#ffffdf" colspan="2">Resources</th>
            <tr><th width="15%" bgcolor="#aaaaaa">Mime Type</th><td
width="85%"><xsl:value-of select=".*[local-name()='mimeType']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Size</th><td><xsl:value-of
select=".*[local-name()='size']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">URI</th><td><xsl:value-of
select=".*[local-name()='uri']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Deref URI</th><td><xsl:value-of
select=".*[local-name()='derefUri']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Digest</th><td><xsl:value-of
select=".*[local-name()='digest']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Description</th><td><xsl:value-of
select=".*[local-name()='description']"/></td></tr>
        </table>
    </xsl:for-each>

    <xsl:for-each select=".*[local-name()='area']" >
        <h5/>
        <table border="1" cellpadding="4" width="100%">
            <th bgcolor="#ffffdf" colspan="2">Area</th>
            <tr><th width="15%" bgcolor="#aaaaaa">Description</th><td
width="85%"><xsl:value-of select=".*[local-name()='areaDesc']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Altitude</th><td><xsl:value-of
select=".*[local-name()='altitude']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Ceiling</th><td><xsl:value-of
select=".*[local-name()='ceiling']"/></td></tr>

        </table>

        <!-->
        <h4>Polygons</h4>
        <table border="1">
            <tr bgcolor="#aaaaaa">
                <th>Latitude</th>
                <th>Longitude</th>
            </tr>

            <xsl:for-each select="polygon">
                <xsl:variable name="values" select="."/>
                <xsl:choose>
                    <xsl:when test="contains($values, ',')">
                        <xsl:variable name="lat" select="substring-
before($values, ',')"/>
                        <xsl:variable name="remaining" select="substring-
after($values, ',')"/>

```



```

        <xsl:variable name="lon" select="substring-before($remaining,
'  ')" />
        <xsl:variable name="values" select="substring-
after($remaining, '  ')" />
        <tr>
            <td><xsl:value-of select="$lat"/></td>
            <td><xsl:value-of select="$lon"/></td>
            <br/>
        </tr>
    </xsl:when>
</xsl:choose>
</xsl:for-each>
</table> -->

<h5/>
<table border="1" cellpadding="4" width="100%">
    <th bgcolor="#ffffdf" colspan="2">Polygons</th>
    <tr bgcolor="#aaaaaa">
        <th width="100%" align="left">Latitude, Longitude</th>
    </tr>
    <xsl:for-each select=".*[local-name()='polygon']" >
        <tr>
            <td width="100%"><xsl:value-of select="."/></td>
        </tr>
    </xsl:for-each>
</table>

<h5/>
<table border="1" cellpadding="4" width="100%">
    <th bgcolor="#ffffdf" colspan="2">Circles</th>
    <tr bgcolor="#aaaaaa">
        <th width="100%" align="left">Latitude, Longitude
Radius</th>
    </tr>
    <xsl:for-each select=".*[local-name()='circle']" >
        <tr>
            <td width="100%"><xsl:value-of select="."/></td>
        </tr>
    </xsl:for-each>
</table>

<h5/>
<table border="1" cellpadding="4" width="100%">
    <th bgcolor="#ffffdf" colspan="2">Geocodes</th>
    <tr bgcolor="#aaaaaa">
        <th width="15%" >Name</th>
        <th width="85%" align="left">Value</th>
    </tr>
    <xsl:for-each select=".*[local-name()='geocode']" >
        <tr>
            <td><xsl:value-of select=".*[local-
name()='valueName']"/></td>
            <td><xsl:value-of select=".*[local-
name()='value']"/></td>
        </tr>
    </xsl:for-each>
</table>

```



```

        </xsl:for-each>

        </tr>
    </table>
    <br/>
</xsl:for-each>

</xsl:for-each>

</body>
</html>

</xsl:template>
</xsl:stylesheet>

```

Example Template D-9: Converting Sensor Data from CAP to HTML

```

<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:nc="http://niem.gov/niem/niem-core/2.0"
  xmlns:cbrn="http://www.dhs.gov/niem/dndo/CBRNSchema"
  xmlns:scr="http://niem.gov/niem/domains/screening/2.0"
  xmlns:em="http://niem.gov/niem/domains/emergencyManagement/2.0"
  xmlns:n25as="http://www.dhs.gov/niem/dndo/CBRNSchema/N25"
  xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xsl:param name="Length_4SubString" select="0"/>
  <xsl:output method="xml" indent="yes"/>
  <xsl:template match="/cap:alert" name="NIEM_IEPD">

    <n25as:AlarmSummaryMessage>
      <xsl:element name="n25as:MessageContentHeader">
        <xsl:element name="cbrn:MessageID"><xsl:value-of
select="cap:identifier"/></xsl:element>
        <xsl:element name="cbrn:MessageCreationDateTime"><xsl:value-of
select="cap:sent"/></xsl:element>
        <xsl:element name="cbrn:MessageKindCode"><xsl:value-of
select="string('AlarmSummaryMessage')"/></xsl:element>
      </xsl:element>

      <xsl:element name="n25as:MessageContent">
        <xsl:element name="cbrn:headline">
          <xsl:variable name="HL" select="tokenize(cap:info/cap:headline, ';')"/>
          <xsl:variable name="HeadLine" select="cap:info/cap:headline"/>
          <xsl:variable name="Count_HL" select="count($HL) div 4"/>

```



```

    <xsl:for-each select="$HeadLine">
      <xsl:if test="count($HL) > 0 and position() <= $Count_HL + 1">

        <xsl:element name="cbrn:detector">
          <xsl:element name="deviceType"><xsl:value-of
select="string('Chemical')"/></xsl:element>

          <xsl:variable name="SubString_HL" select="substring($HeadLine,
$Length_4SubString)"/>
          <xsl:variable name="HL1" select="substring-before($SubString_HL,
';')"/>
          <xsl:variable name="Length_HL1" select="string-length($HL1)"/>
          <xsl:variable name="SubString_HL1" select="substring($SubString_HL,
$Length_HL1 + 2)"/>

          <xsl:variable name="HL2" select="substring-
before($SubString_HL1, ';')"/>
          <xsl:variable name="Length_HL2" select="string-length($HL2)"/>
          <xsl:variable name="SubString_HL2" select="substring($SubString_HL1,
$Length_HL2 + 2)"/>

          <xsl:variable name="HL3" select="substring-
before($SubString_HL2, ';')"/>
          <xsl:variable name="Length_HL3" select="string-length($HL3)"/>
          <xsl:variable name="SubString_HL3" select="substring($SubString_HL2,
$Length_HL3 + 2)"/>

          <xsl:variable name="HL4" select="substring-
before($SubString_HL3, ';')"/>
          <xsl:variable name="Length_HL4" select="string-length($HL4)"/>
          <xsl:variable name="SubString_HL4" select="substring($SubString_HL3,
$Length_HL4 + 2)"/>

          <xsl:variable name="Length_HL" select="string-length($HeadLine)"/>

          <xsl:variable name="Length_4SubString" select="$Length_4SubString +
$Length_HL1 + $Length_HL2 + $Length_HL3 + $Length_HL4 + 5"/>

          <xsl:element name="cap:probeType"><xsl:value-of
select="$HL1"/></xsl:element>
          <xsl:element name="cap:reading"><xsl:value-of
select="$HL2"/></xsl:element>
          <xsl:element name="cap:units"><xsl:value-of
select="$HL3"/></xsl:element>
          <xsl:element name="cap:alertColor"><xsl:value-of
select="$HL4"/></xsl:element>

        </xsl:element>

      </xsl:if>
    </xsl:for-each>
  </xsl:element>
  <xsl:copy-of select="." />
</xsl:element>
</n25as:AlarmSummaryMessage>
</xsl:template>

```



```
</xsl:stylesheet>
```

Example Template D-10: Converting Sensor Data from CAP to N25

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:fo="http://www.w3.org/1999/XSL/Format"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:fn="http://www.w3.org/2005/xpath-functions">

  <!--<xsl:namespace-alias stylesheet-prefix="cap" result-prefix="xsl"/> -->

  <xsl:template match="/" xml:space=" ">

    <html>
    <body>

      <xsl:for-each select="//*[local-name()='alert']" > <!-- alert loop -->

        <table border="1" cellpadding="4" width="100%">
          <th bgcolor="#ff1111" colspan="2">ALERT MESSAGE</th>
          <tr><th width="15%" bgcolor="#6a9a9a">Identifier</th><td
width="85%"><xsl:value-of select=".[*[local-name()='identifier']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Sender</th><td><xsl:value-of
select=".[*[local-name()='sender']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Sent</th><td><xsl:value-of select=".[*[local-
name()='sent']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Status</th><td><xsl:value-of
select=".[*[local-name()='status']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Msg Type</th><td><xsl:value-of
select=".[*[local-name()='msgType']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Source</th><td><xsl:value-of
select=".[*[local-name()='source']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Scope</th><td><xsl:value-of select=".[*[local-
name()='scope']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Restriction</th><td><xsl:value-of
select=".[*[local-name()='restriction']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Notes</th><td><xsl:value-of select=".[*[local-
name()='notes']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Addresses</th><td><xsl:value-of
select=".[*[local-name()='addresses']"/></td></tr>
          <tr><th bgcolor="#aaaaaa">Incidents</th><td><xsl:value-of
select=".[*[local-name()='incidents']"/></td></tr>
        </table>

        <h5/>

        <table border="1" cellpadding="4" width="100%">
          <th bgcolor="#ffffdf" colspan="2">Handling Codes</th>
          <tr bgcolor="#aaaaaa">
```




```

        <th width="100%" align="left">Value</th>
    </tr>
    <xsl:for-each select=".*[local-name()='code']" >
        <tr>
            <td width="100%"><xsl:value-of select="."/></td>
        </tr>
    </xsl:for-each>
</table>

<h5/>

    <xsl:for-each select=".*[local-name()='info']" >

        <table border="3" cellpadding="9" width="100%">
            <th bgcolor="#2a9f9a" colspan="2">INFORMATION</th>
            <tr>

                <table border="1" cellpadding="4" width="100%">
                    <th bgcolor="#ffffdf" colspan="2"></th>
                    <tr><th width="15%" bgcolor="#9a6a9a">Onset</th><td
width="85%"><xsl:value-of select=".*[local-name()='onset']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Effective</th><td><xsl:value-of
select=".*[local-name()='effective']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Expires</th><td><xsl:value-of
select=".*[local-name()='expires']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Urgency</th><td><xsl:value-of
select=".*[local-name()='urgency']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Severity</th><td><xsl:value-of
select=".*[local-name()='severity']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Certainty</th><td><xsl:value-of
select=".*[local-name()='certainty']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Language</th><td><xsl:value-of
select=".*[local-name()='language']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Category</th><td><xsl:value-of
select=".*[local-name()='category']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Headline</th><td><xsl:value-of
select=".*[local-name()='headline']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Instruction</th><td><xsl:value-of
select=".*[local-name()='instruction']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Contact</th><td><xsl:value-of
select=".*[local-name()='contact']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Event</th><td><xsl:value-of
select=".*[local-name()='event']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Audience</th><td><xsl:value-of
select=".*[local-name()='audience']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Response Type</th><td><xsl:value-of
select=".*[local-name()='responseType']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Sender Name</th><td><xsl:value-of
select=".*[local-name()='senderName']"/></td></tr>
                    <tr><th bgcolor="#aaaaaa">Web URI</th><td><xsl:value-of
select=".*[local-name()='web']"/></td></tr>
                </table>
            </tr>
        </table>
    </xsl:for-each>

```



```

        <tr><th bgcolor="#aaaaaa">Description</th><td><xsl:value-of
select=".*[local-name()='description']"/></td></tr>
    </table>

    <h5/>
    <table border="1" cellpadding="4" width="100%">
        <th bgcolor="#ffffdf" colspan="2">Event Codes</th>
        <tr bgcolor="#aaaaaa">
            <th width="15%">Name</th>
            <th width="85%" align="left">Value</th>
        </tr>
        <xsl:for-each select=".*[local-name()='eventCode']" >
            <tr>
                <td><xsl:value-of select=".*[local-
name()='valueName']"/></td>
                <td><xsl:value-of select=".*[local-name()='value']"/></td>
            </tr>
        </xsl:for-each>
    </table>

    <h5/>
    <table border="1" cellpadding="4" width="100%">
        <th bgcolor="#ffffdf" colspan="2">Parameters</th>
        <tr bgcolor="#aaaaaa">
            <th width="15%">Name</th>
            <th width="85%" align="left">Value</th>
        </tr>
        <xsl:for-each select=".*[local-name()='parameter']" >
            <tr>
                <td><xsl:value-of select=".*[local-
name()='valueName']"/></td>
                <td><xsl:value-of select=".*[local-name()='value']"/></td>
            </tr>
        </xsl:for-each>
    </table>

    <xsl:for-each select=".*[local-name()='resource']" >
        <h5/>
        <table border="1" cellpadding="4" width="100%">
            <th bgcolor="#ffffdf" colspan="2">Resources</th>
            <tr><th width="15%" bgcolor="#aaaaaa">Mime Type</th><td
width="85%"><xsl:value-of select=".*[local-name()='mimeType']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Size</th><td><xsl:value-of
select=".*[local-name()='size']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">URI</th><td><xsl:value-of
select=".*[local-name()='uri']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Deref URI</th><td><xsl:value-of
select=".*[local-name()='derefUri']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Digest</th><td><xsl:value-of
select=".*[local-name()='digest']"/></td></tr>
            <tr><th bgcolor="#aaaaaa">Description</th><td><xsl:value-of
select=".*[local-name()='description']"/></td></tr>
        </table>
    </xsl:for-each>

    <xsl:for-each select=".*[local-name()='area']" >
        <h5/>

```



```

        <table border="1" cellpadding="4" width="100%">
        <th bgcolor="#ffffdf" colspan="2">Area</th>
        <tr><th width="15%" bgcolor="#aaaaaa">Description</th><td
width="85%"><xsl:value-of select=".*[local-name()='areaDesc']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Altitude</th><td><xsl:value-of
select=".*[local-name()='altitude']"/></td></tr>
        <tr><th bgcolor="#aaaaaa">Ceiling</th><td><xsl:value-of
select=".*[local-name()='ceiling']"/></td></tr>

        </table>

        <!-->
        <h4>Polygons</h4>
        <table border="1">
        <tr bgcolor="#aaaaaa">
        <th>Latitude</th>
        <th>Longitude</th>
        </tr>

        <xsl:for-each select="polygon">
        <xsl:variable name="values" select="."/>
        <xsl:choose>
        <xsl:when test="contains($values, ',')">
        <xsl:variable name="lat" select="substring-
before($values, ',')"/>
        <xsl:variable name="remaining" select="substring-
after($values, ',')"/>
        <xsl:variable name="lon" select="substring-before($remaining,
' ')" />
        <xsl:variable name="values" select="substring-
after($remaining, ' ')" />
        <tr>
        <td><xsl:value-of select="$lat"/></td>
        <td><xsl:value-of select="$lon"/></td>
        <br/>
        </tr>
        </xsl:when>
        </xsl:choose>
        </xsl:for-each>
        </table> -->

        <h5/>
        <table border="1" cellpadding="4" width="100%">
        <th bgcolor="#ffffdf" colspan="2">Polygons</th>
        <tr bgcolor="#aaaaaa">
        <th width="100%" align="left">Latitude, Longitude</th>
        </tr>
        <xsl:for-each select=".*[local-name()='polygon']" >
        <tr>
        <td width="100%"><xsl:value-of select="."/></td>
        </tr>
        </xsl:for-each>
        </table>

        <h5/>
        <table border="1" cellpadding="4" width="100%">
        <th bgcolor="#ffffdf" colspan="2">Circles</th>

```



```

        <tr bgcolor="#aaaaaa">
            <th width="100%" align="left">Latitude, Longitude
Radius</th>

        </tr>
        <xsl:for-each select=".*[local-name()='circle']" >
            <tr>
                <td width="100%"><xsl:value-of select="."/></td>
            </tr>
        </xsl:for-each>
    </table>

    <h5/>
    <table border="1" cellpadding="4" width="100%">
        <th bgcolor="#ffffdf" colspan="2">Geocodes</th>
        <tr bgcolor="#aaaaaa">
            <th width="15%" >Name</th>
            <th width="85%" align="left">Value</th>
        </tr>
        <xsl:for-each select=".*[local-name()='geocode']" >
            <tr>
                <td><xsl:value-of select=".*[local-
name()='valueName']"/></td>
                <td><xsl:value-of select=".*[local-
name()='value']"/></td>
            </tr>
        </xsl:for-each>
    </table>
    </xsl:for-each>

    </tr>
    </table>
    <br/>
</xsl:for-each>

    </xsl:for-each>

</body>
</html>

</xsl:template>
</xsl:stylesheet>

```

Example Template D-11: Converting Sensor Data from CAP to KML

```

<?xml version="1.0"?>
<xsl:stylesheet version="2.0"
    xmlns:xsl="http://www.w3.org/1999/XSL/Transform"

```



```

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://data-gov.tw.rpi.edu/vocab/p/32/"
xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
xmlns:dc="http://purl.org/dc/elements/1.1/"
xmlns:dgtwc="http://data-gov.tw.rpi.edu/2009/data-gov-twc.rdf#"
xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1">
<!-- <xsl:output method="xml" omit-xml-declaration="no"/> -->
<xsl:output method="xml" indent="yes" encoding="UTF-8"/>
<xsl:template match="/">
    <rdf:RDF xml:base="http://209.242.167.100/rdf/ICBRNE_data.rdf">

        <xsl:apply-templates select="alerts/cap:alert" />

    </rdf:RDF>
</xsl:template>

<xsl:attribute-set name="aboutAttributes">
    <xsl:attribute name="rdf:about"> <xsl:value-of
select="cap:identifier" /> </xsl:attribute>
</xsl:attribute-set>

<!-- Matches CAP message, transforms to RDF -->
<xsl:template match="cap:alert">
    <rdf:Description xsl:use-attribute-sets="aboutAttributes">
        <rdf:type rdf:resource="http://data-gov.tw.rpi.edu/2009/data-
gov-twc.rdf#DataEntry"/>
        <id><xsl:value-of select="cap:identifier"/></id>
        <sender><xsl:value-of select="cap:sender"/></sender>
        <sent><xsl:value-of select="cap:sent"/></sent>
        <status><xsl:value-of select="cap:status"/></status>
        <msgType><xsl:value-of select="cap:msgType"/></msgType>
        <source><xsl:value-of select="cap:source"/></source>
        <urgency><xsl:value-of
select="cap:info/cap:urgency"/></urgency>
        <severity><xsl:value-of
select="cap:info/cap:severity"/></severity>
        <certainty><xsl:value-of
select="cap:info/cap:certainty"/></certainty>
        <headline><xsl:value-of
select="cap:info/cap:headline"/></headline>
        <expires><xsl:value-of
select="cap:info/cap:expires"/></expires>
        <xsl:apply-templates select="cap:info/cap:area/cap:circle"/>
    </rdf:Description>
</xsl:template>

<xsl:template match="cap:circle">
    <xsl:call-template name="LatAndLon" >
    </xsl:call-template>
</xsl:template>

<xsl:template name="LatAndLon">
    <xsl:variable name = "circle" select="." />
    <!-- if there is a comma between lat and lon, converts it to a space
-->

```



```

        <xsl:variable name="values" select="translate($circle, ', ' , ' ' )"/>
        <!-- parses for Lat/Lon from the 'circle' tag in the CAP message -->
    >
        <xsl:variable name="latLon" select="tokenize(normalize-
space($values), ' ' )"/>
        <lat><xsl:value-of select="$latLon[1]" /></lat>
        <lon><xsl:value-of select="$latLon[2]" /></lon>
    </xsl:template>
</xsl:stylesheet>

```

Example Template D-12: Converting Sensor Data from CAP to RDF

```

<?xml version="1.0"?>
<xsl:stylesheet version="2.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:geo="http://www.w3.org/2003/01/geo/wgs84_pos#"
  xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1">
  <xsl:output method="xml" indent="yes" encoding="UTF-8"/>
  <xsl:template match="/">
    <rss version="2.0">
      <channel>
        <title>DHS ICBRNE</title>
        <link>http://icbrne.org</link>
        <description>Integrated Chemical, Biological, Radiological, Nuclear and
Explosive Program</description>
        <language>en-us</language>
        <copyright>2010 SPAWAR Systems Center Pacific</copyright>
        <lastBuildDate>Jul 22 2010 10:00:00</lastBuildDate>
        <docs></docs>
        <generator>ICBRNE Services</generator>
        <category domain="spawar.navy.mil">Other</category>
        <xsl:apply-templates select="alerts/cap:alert" />
      </channel>
    </rss>
  </xsl:template>

  <xsl:template match="cap:alert">
    <item>
      <title><xsl:value-of select="cap:source" /></title>
      <pubDate><xsl:value-of select="cap:sent" /></pubDate>
      <category><xsl:value-of select="cap:info/cap:category"
/></category>
      <author><xsl:value-of select="cap:sender" /></author>
      <link>http://icbrne.org</link>
      <description disable-output-escaping="yes"><![CDATA[]]><xsl:value-of
select="cap:info/cap:headline" /></description>
      <xsl:apply-templates select="cap:info/cap:area/cap:circle"/>
    </item>
  </xsl:template>

```




```

    <xsl:template match="cap:circle">
    <xsl:call-template name="LatAndLon" >
    </xsl:call-template>
    </xsl:template>

    <xsl:template name="LatAndLon">
    <xsl:variable name = "circle" select="." />
    <!-- if there is a comma between lat and lon, converts it to a space -->
    <xsl:variable name="values" select="translate($circle, ', ' , ' ' )"/>
    <!-- parses for Lat/Lon from the 'circle' tag in the CAP message -->
    <xsl:variable name="latLon" select="tokenize(normalize-space($values), '
    ')" />
    <geo:lat><xsl:value-of select="$latLon[1]" /></geo:lat>
    <geo:long><xsl:value-of select="$latLon[2]" /></geo:long>
    </xsl:template>
</xsl:stylesheet>

```

Example Template D-13: Converting Sensor Data from CAP to RSS

```

<?xml version="1.0"?>
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:swe="http://www.opengis.net/swe/1.0.01"
  xmlns:xlink="http://www.w3.org/1999/xlink"
  xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1">
  <!-- <xsl:output method="xml" omit-xml-declaration="no"/> -->
  <xsl:output method="xml" indent="yes" encoding="UTF-8"/>
  <xsl:template match="/">

    <xsl:call-template name="header"/>
  </xsl:template>
  <xsl:template name="header">
    <swe:DataRecord xmlns:gml="http://www.opengis.net/gml"
  xmlns:swe="http://www.opengis.net/swe/1.0.01"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xlink="http://www.w3.org/1999/xlink" >
      <xsl:apply-templates select="//cap:parameter" />
    </swe:DataRecord>
  </xsl:template>

  <xsl:template match="cap:parameter">
    <xsl:if test="cap:valueName = 'Sensor'">
      <swe:field xsl:use-attribute-sets="fieldAttributes">
        <swe:Quantity xsl:use-attribute-sets="qtyAttributes">
          <swe:uom xsl:use-attribute-sets="linkAttributes"/>
          <xsl:variable name = "capValue" select="cap:value" />
          <xsl:variable name="strTokenized" select="tokenize(normalize-
space($capValue), ', ')" />
          <xsl:choose>
            <!-- if the fifth token has a 'C=' string in it -->
            <xsl:when test="contains($strTokenized[5], 'C=')">
              <!-- get string value after the 'C=' string -->

```



```

        <xsl:variable name = "value" select="substring-
after($strTokenized[5], 'C=') " />
        <swe:value> <xsl:value-of select="$value" /> </swe:value>
    </xsl:when>
    <xsl:otherwise>
        <swe:value> <xsl:value-of select="$strTokenized[5]" />
    </swe:value>
    </xsl:otherwise>
</xsl:choose>
</swe:Quantity>
</swe:field>
</xsl:if>
</xsl:template>

<xsl:attribute-set name="fieldAttributes">
    <xsl:attribute name="name">
        <xsl:variable name = "capValue" select="cap:value" />
        <xsl:variable name="strTokenized" select="tokenize(normalize-
space($capValue), ', ')" />
        <!-- normalize-space - remove all blank space -->
        <xsl:value-of select="concat(normalize-
space($strTokenized[1]),$strTokenized[2])" />
    </xsl:attribute>
</xsl:attribute-set>

<xsl:attribute-set name="qtyAttributes">
    <xsl:attribute name="definition">
        <xsl:variable name = "capValue" select="cap:value" />
        <xsl:variable name="strTokenized" select="tokenize(normalize-
space($capValue), ', ')" />
        <!-- normalize-space - remove all blank space -->
        http://icbrne.spawar.navy.mil/ontology/icbrne.owl#<xsl:value-of
select="concat(normalize-space($strTokenized[1]),$strTokenized[2])" />
    </xsl:attribute>
</xsl:attribute-set>

<xsl:attribute-set name="linkAttributes">
    <xsl:attribute name="xlink:href">
        <xsl:variable name = "capValue" select="cap:value" />
        <xsl:variable name="strTokenized" select="tokenize(normalize-
space($capValue), ', ')" />
        http://icbrne.spawar.navy.mil/ontology/icbrne_uom.owl#<xsl:value-of
select="$strTokenized[6]" />
    </xsl:attribute>
</xsl:attribute-set>
</xsl:stylesheet>

```

Example Template D-14: Converting Sensor Data from CAP to SWE – Observations & Measures

```

<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="2.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
xmlns:fo="http://www.w3.org/1999/XSL/Format"

```



```

xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:fn="http://www.w3.org/2005/xpath-functions">

<xsl:template match="/"> <!-- match all root elements-->
  <ulexpd:doPublish
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ucore-ulex="urn:ucore:2.0:ulex-integration"
    xmlns:ucore="urn:ucore:2.0"
    xmlns:ulexpd="ulex:message:pd:1.0"
    xmlns:ulexcodes="ulex:message:codes:1.0"
    xmlns:ulex="ulex:message:structure:1.0"
    xmlns:icism="urn:us:gov:ic:ism:v2"
    xmlns:ddms="http://metadata.dod.mil/mdr/ns/DDMS/1.4/"
    xmlns:gml="http://www.opengis.net/gml"
    xmlns:aisns="urn:cs:4.1.3:service:post"
    xsi:schemaLocation="
      ulex:message:pd:1.0 ../../UCore/2.0.0a2/import/ULEX1.0beta/xsd/ulex/ulex-
publish-discover/1.0/ulex-publish-discover.xsd'
      ulex:message:codes:1.0 ../../UCore/2.0.0a2/import/ULEX1.0beta/xsd/ulex/ulex-
codes/1.0/ulex-codes.xsd
      ulex:message:structure:1.0
../../UCore/2.0.0a2/import/ULEX1.0beta/xsd/ulex/ulex/1.0/ulex.xsd
      urn:ucore:2.0 ../../UCore/2.0.0a2/ucore/ucore.xsd
      http://metadata.dod.mil/mdr/ns/DDMS/1.4/
../../UCore/2.0.0a2/import/DDMSv1.4.1/ns/DDMS/1.4.1/DDMS-v1_4_1.xsd
      urn:ucore:2.0:ulex-integration ../../UCore/2.0.0a2/ulex-integration/ulex-
integration.xsd">

    <ulex:PublishMessageContainer>
      <!--===== Message =====>
      <ulex:PublishMessage>
        <ulex:PDMetadata>
          <ulex:ULEXFramework>1.0</ulex:ULEXFramework>

          <ulex:ULEXImplementation>
            <ulex:ULEXImplementationVersion>1.0</ulex:ULEXImplementationVersion>
            <ulex:ULEXImplementationName></ulex:ULEXImplementationName>
          </ulex:ULEXImplementation>

          <ulex:MessageDateTime>
            <xsl:value-of select="current-dateTime()"/>
          </ulex:MessageDateTime>

          <ulex:MessageSequenceNumber></ulex:MessageSequenceNumber>
        </ulex:PDMetadata>
        <!--===== Data Submitter Metadata =====>
        <ulex:DataSubmitterMetadata>
          <ucore-ulex:SystemIdentifier>CAP to UCore Transform</ucore-
ulex:SystemIdentifier>
          <ucore-ulex:SystemContact>
            <ddms:Organization>
              <ddms:name>name</ddms:name>
              <ddms:phone>619-553-30000</ddms:phone>
              <ddms:email>test@test</ddms:email>
            </ddms:Organization>
          </ucore-ulex:SystemContact>

```



```

</ulex:DataSubmitterMetadata>

<!--===== Package =====>
  <ulex:DataItemPackage>
    <ulex:PackageMetadata>
      <ulex:DataItemID><xsl:value-of select="generate-
id()" /></ulex:DataItemID>
      <ulex:DataItemCompleteIndicator>true</ulex:DataItemCompleteIndicator>
      <ulex:DataItemDate><xsl:value-of select="current-date()" />
</ulex:DataItemDate>
      <ulex:DataItemReferenceID></ulex:DataItemReferenceID>
      <ucore-ulex:DataItemStatus>CAP to UCore Report</ucore-
ulex:DataItemStatus>

      <!--===== Data Owner Metadata
=====-->
      <ulex:DataOwnerMetadata>
        <ucore-ulex:DataOwnerIdentifier>
          <ddms:Organization>
            <ddms:name>Safe Environment Engineering</ddms:name>
          </ddms:Organization>
        </ucore-ulex:DataOwnerIdentifier>
        <ucore-ulex:DataOwnerContact>
          <ddms:Organization>
            <ddms:name>David Lamensdorf</ddms:name>
            <ddms:phone>(661) 295-5500</ddms:phone>
            <ddms:email>davidl@safeenv.com</ddms:email>
          </ddms:Organization>
        </ucore-ulex:DataOwnerContact>
      </ulex:DataOwnerMetadata>
      <ucore-ulex:DisseminationCriteria>
        <xsl:attribute name="icism:classification">U</xsl:attribute>
      </ucore-ulex:DisseminationCriteria>
    </ulex:PackageMetadata>

    <!--===== Digest =====>
    <ucore-ulex:digest>
      <xsl:for-each select="//*[local-name()='alert']" > <!-- alert loop --
>
      <ucore:Entity>
        <xsl:attribute name="id"><xsl:value-of select="generate-
id(./*[local-name()='identifier'])" /> </xsl:attribute>
        <ucore:descriptor>
          <xsl:value-of select="./*[local-name()='identifier']" /> -
Identifier
        </ucore:descriptor>
      </ucore:Entity>

      <ucore:Location>
        <xsl:attribute name="id">loc-
        <xsl:value-of select="generate-id(./*[local-
name()='info']/*[local-name()='area']/*[local-
name()='areaDesc'])" /></xsl:attribute>
        <ucore:descriptor>
          Location of <xsl:value-of select="./*[local-
name()='info']/*[local-name()='area']/*[local-name()='areaDesc']" />
        </ucore:descriptor>

```



```

        <ucore:geoLocation>
          <ddms:boundingGeometry>
            <gml:Point>
              <xsl:attribute name="gml:id">
                <xsl:value-of select="generate-id(./*[local-
name()='info']/*[local-name()='area']/*[local-name()='circle'])"/>
              </xsl:attribute>
              <gml:pos>
                <xsl:value-of select="./*[local-name()='info']/*[local-
name()='area']/*[local-name()='circle']"/><xsl:text>
              </xsl:text>
              </gml:pos>
            </gml:Point>
          </ddms:boundingGeometry>
        </ucore:geoLocation>
      </ucore:Location>

      <!--Relationships -->
      <ucore:LocatedAt>
        <ucore:metadata>
          <ucore:validityTime>
            <ucore:instant>
              <ucore:dateTime><xsl:value-of select="./*[local-
name()='sent']"/></ucore:dateTime>
            </ucore:instant>
          </ucore:validityTime>
          <ucore:InformationSource>
            <ddms:Service>
              <ddms:Name>
                <xsl:value-of select="./*[local-
name()='source']"/><xsl:text>
              </xsl:text>
            </ddms:Name>
          </ddms:Service>
        </ucore:InformationSource>
        </ucore:metadata>
        <ucore:entityRef>
          <xsl:attribute name="ref"><xsl:value-of select="generate-id(./*[local-
name()='identifier'])"/></xsl:attribute>
        </ucore:entityRef>
        <ucore:locationRef>
          <xsl:attribute name="ref">loc-
          <xsl:value-of select="generate-id(./*[local-name()='info']/*[local-
name()='area']/*[local-name()='circle'])"/></xsl:attribute>
        </ucore:locationRef>
      </ucore:LocatedAt>
    </xsl:for-each> <!-- end of alert loop-->
  </ucore-ulex:digest>

  <!--===== Attachment Links
=====-->
  <ulex:AttachmentLink>
    <ulex:AttachmentURI></ulex:AttachmentURI>
    <ulex:AttachmentViewableIndicator></ulex:AttachmentViewableIndicator>
    <ulex:AttachmentDescriptionText></ulex:AttachmentDescriptionText>
  </ulex:AttachmentLink>

```



```
<!--===== Rendering Instructions
=====-->
<ulex:RenderingInstructions>
  <ulex:RenderingMethod>HTMLStyleSheet</ulex:RenderingMethod>
</ulex:RenderingInstructions>
<!--===== Supporting Narrative
=====-->
<ucore-ulex:narrative>
  <xsl:attribute name="icism:classification">U</xsl:attribute>
  CAP (Ludlum Radiation Survey Meter Model 2241 CAP Status Samples) to
UCore transform.
</ucore-ulex:narrative>

</ulex:DataItemPackage>
</ulex:PublishMessage>
</ulex:PublishMessageContainer>

</ulexpd:doPublish>
</xsl:template>

</xsl:stylesheet>
```

Example Template D-15: Converting Sensor Data from CAP to UCore



14 Appendix F - Current Software Participants

MyStateUSA

www.MyStateUSA.com

208-377-1960



MyStateUSA couples the communications power of the Internet with our advanced communications technology to provide a system that enables rapid exchange of information between the government and its citizens. Communities, counties and government agencies throughout the United States are putting MyStateUSA technology into place.

Naval Research Laboratory

www.lcp.nrl.navy.mil/ct-analyst

202-767-3055



CT-Analyst provides accurate, instantaneous, 3D predictions of chemical, biological, & radiological (CBR) agent transport in urban settings. In the past, more accuracy has always meant more computing and more computing means more delay. Waiting even a fraction of a minute for a simplified scenario computation can be far too long for timely situational assessments. Therefore, CT-Analyst uses the best computations possible prepared well ahead of time and captures their salient results in a highly compressed database to be manipulated and displayed instantly.

Aristatek

www.aristatek.com

877-912-7200



The PEAC-WMD software is designed for use at the scene to support a First Responder in making informed decisions and provides immediate operational response for HAZMAT and CBRNE incidents when you need to KNOW! During an incident, when seconds count, the right decisions made early in an incident will pay dividends later as the incident unfolds allowing the responder to protect response personnel, the public, and property. Comprehensive information on hazardous substances, chemical reactivity, plus the ability to develop incident specific exclusion zones or safe standoff distances are just a click away and can be easily shared with others.

Safer Systems

www.saferssystem.com

805-383-9711



SAFER Systems is the global technology leader in chemical emergency management solutions, offering advanced plume measurement and monitoring solutions that integrate real-time weather and sensor data. The company's state-of-the-art solutions incorporate patented technologies and are designed to detect and accurately predict in real-time the dispersion of accidental or intentional releases of toxic chemicals. Our products provide the fastest, most accurate situation analysis enabling better command and control decision-making during a chemical event and greater post-event analysis.

Viper

<https://cop.vdem.virginia.gov>

804-674-2400



The Virginia Interoperability Picture for Emergency Response (VIPER) allows the Virginia Emergency Operations Center to display information that relates to each other spatially in order to drastically improve the situational awareness of response, recovery coordinators, and local emergency managers.

Solace Systems

www.solacesystems.com

613-271-1010



The Solace Message Router is a hardware implementation of messaging middleware that routes high volumes of messages with very low latency, and the Solace Content Router filters, personalizes and forwards information based on rules-based subscriptions. These products can be extended with functionality such as guaranteed delivery, message caching and geospatial routing.



DMIS

www.fema.gov/disastermanagement
866-972-3662



Disaster Management Interoperability Service (DMIS) Tools are provided by the United States Government at no charge to public safety organizations within the United States and Canada. This basic toolset supports dynamic collaboration among organizations working together to manage the consequences of an incident. They enable rapid alerting, sharing a map-centric common operating picture, and logistics "conversations" regarding specific resource needs.

Optimetrics

www.adashi.org
800-734-6956



ADASHI 3.0 is a comprehensive software platform for managing, communicating, responding to, and reporting critical incidents. It combines proven incident response and incident command capabilities in a networked emergency management system for coordinated use across all agencies, departments, and staff levels

Virtual Beverly Hills

<http://gis.beverlyhills.org>
310-285-1000



Virtual Beverly Hills is a cutting-edge GIS application. It is a system that allows users to visualize on a map, real-time resource data, disaster information, traffic conditions or anything else they imagine will be helpful.

Virtual Alabama

www.virtual.alabama.gov
800-392-8025



In October 2005, the Alabama Department of Homeland Security (AL DHS) initiated a project to access new technologies in 3D visualization. At the request of Governor Bob Riley, AL DHS began exploring and identifying ways to leverage existing state asset imagery and infrastructure data into a visualization tool that is affordable, scalable, maintainable, and capable of employing the power of existing and evolving internet based applications. As a result, the Virtual Alabama program was created.

Asynchrony

<http://asolutions.com>
314-678-2200



The Mobile Field Kit (MFK) puts state-of-the-art tools and technology directly in the hands of field team members, including First Responders, CBRNE Teams, Tactical Deployment Teams, Physical Security Teams, and Special Ops. It allows them to acquire, store, assess and share information, both within the team and across organizational boundaries.

Environmental Protection Agency

<http://epa.org>



The Viper system is designed to support the use of field sensors in a wide range of mobile and fixed applications ranging from emergency response to long term site control monitoring. The use of Viper enables EPA to integrate and communicate sensor data without dependence on vendor-specific propriety data communication systems

New York City Department of Health & Mental Hygiene



EMITS is the Environmental Monitoring Telemetry System. The system In wirelessly transmit radiological monitoring results in CAP format from a set of hand held and van-mounted instruments back to the Environmental Data Exchange Network (EDEN)



Instrumentation Participants

Canberra Industries, Inc.
800 Research Parkway, Meriden, CT 06450, U.S.A.
800-243-3955
www.canberra.com

Berkeley Nucleonics Corporation
2955 Kerner Blvd., San Rafael CA 94901 U.S.A
800-234-7858
www.berkeleynucleonics.com

Bruker Detection Corporation
40 Manning Rd, Billerica, MA 01821
978-663-3660
www.bruker.com/detection

Draeger Safety Inc.
101 Technology Drive. Pittsburgh, PA 15275-1057
800-922-5518
www.draeger.com

Fluke Corporation
6920 Seaway Blvd, Everett, WA 98203, USA
425-347-6100
www.fluke.com

FLIR
2100 Crystal Drive, Suite 650, Arlington, VA 22202
703-678-2111
www.icxt.com

Industrial Scientific Corporation
1001 Oakdale Road, Oakdale, PA 15071-1500
412-788-4353
www.indsci.com

Ludlum Measurements, Inc.
501 Oak Street, Sweetwater, Texas 79556 USA
800-622-0828
www.ludlums.com

Met One Instruments
1600 Washington Blvd., Grants Pass, OR 97526
541-471-7111
www.metone.com



MSA
1000 Cranberry Woods Drive, Cranberry Township, PA 16066
724-776-8600
www.msanorthamerica.com

RAE Systems
3775 North First Street, San Jose, CA 95134 USA
408-952-8200
www.raesystems.com








ThermoFisher
100 Technology Drive, Pittsburgh, PA 15219 USA
412-770-2326
www.thermofisher.com



15 Appendix G - Instrumentation Interfaces

The Instrumentation Interfaces, shown in the table below, provide a good overview of the types of sensors, data ports and data formats enabled by the ICBRNE Project. There are four columns in the table. The first column is the sensor manufacturer, model and type of sensor, for example “Canberra, PDR-77, Radiation”. The information exchanged between these sensors and external devices is governed by rules (conventions) that can be set out in a technical specification called a communication protocol standard. So, the second column is the communication protocol used by the device, e.g. “Serial”. (All of the transmission formats used by the sensors in this table are well-known standards.) The third column is the format of the data itself as it leaves the device. One or two of these sensors uses a well-known standard, but the rest use their own proprietary formats. (This is one of the benefits of the ICBRNE capability, namely the conversion of these proprietary formats into standard formats and the education of the community on the benefits of encouraging standardization.) If the data format is a non-standard format, then the format is simply marked “Proprietary”. The fourth column is a picture of the connector.

The table provides an easy-to-understand overview of the large variety of sensors and connectors enabled through the ICBRNE program.

Meter/Sensor Manufacturer, Model & Function	Protocol	Comm	Connector
Canberra, PDR-77, Radiation	Serial	Proprietary	
Berkeley Nucleonics, SAM940, Radiation	Serial or Ethernet	N42	
Bruker Daltronics, HAWK, Long Range Chemical	Ethernet	Proprietary	
Bruker Daltronics, RAID-M, CWA ¹	Serial	Proprietary	
Bruker Daltronics, RAID-XP CWA ¹ Radiation	Serial	Proprietary	
Draeger Safety, X-am 7000, Chemical	Serial-Ir	Proprietary	
Draeger Safety, X-am 2000/5000, Chemical	Serial-Ir	Proprietary	



Draeger Safety, IMS, CWA

Serial

Proprietary



EnviroNics, ChemPro 100, CWA¹

Serial

Proprietary



Fluke, 415B, Radiation

Serial

Proprietary



iCX, Stride, Radiation

Ethernet

Proprietary



Industrial Scientific, iTX, Chemical

Serial-TTL

Proprietary



Industrial Scientific, MX6/4, Chemical

Serial-Ir

Proprietary



Industrial Scientific, VX500, Chemical

Serial-TTL

Proprietary



Ludlum, 2241, Radiation

Serial

Proprietary



Ludlum, 2360, Radiation

Serial

Proprietary



Met One Instruments, EBAM, Particulate

Serial

Proprietary



MSA, Sirius, Chemical

Serial-Ir

Proprietary



MSA, Altair, Chemical

Serial-Ir

Proprietary



Rae Systems, AeraRae, Chemical, Radiation

Serial

Proprietary





Rae Systems, ChemRae, CWA¹

Serial

Proprietary



Rae Systems, MiniRae, Chemical

Serial

Proprietary



Rae Systems, PPBRae, Chemical

Serial

Proprietary



Rae Systems, MultiRae, Chemical

Serial

Proprietary



Rae Systems, Qrae, Chemical

Serial

Proprietary



Thermo Fisher Bicon, TPM-903A, Radiation Portal

Serial

Proprietary



Thermo Fisher Bicon, TPM-903B, Radiation Portal

Ethernet

Proprietary



Thermo Fisher, DataRam, Aerosol

Serial

Proprietary



Thermo Fisher, FH40G, Radiation

Serial-Ir

Proprietary



Thermo Fisher, Identifier, Radiation

Serial

Proprietary



Thermo Fisher, Interceptor, Radiation

Serial
Profile

Proprietary



Thermo Fisher, Raider, Radiation

Serial
Profile

Proprietary





ICBRNE Operational Report



Thermo Fisher, MDS, Radiation, GPS

Serial

Proprietary



Trimble, GPS

802.11b

NMEA





Appendix H - Virtual Golden Phoenix Overview

Virtual Golden Phoenix Overview

Testbed Interoperability Enabled Using Open Standards
Among Systems & Capabilities
including:

Coast Guard & SSC – Sensor Management System
DTRA – DE Routing Test
DHS OIC & OASIS – EDXL Standards
DHS DNDO – N25 & DE Routing
DHS CB S&T – ICBRNE
FEMA – DM OPEN
FEMA - IPAWS
Fleet Forces Command & SSC – C4ISuite
Kansas City Regional Terrorism Early Warning – SAVIEW
Mitre – IC.NET
Safe Environment Engineering – Wireless HAZMAT
Sensors
Solace – EDXL-DE & Geospatial Routing
SPAWAR Systems Center (SSC) Pacific – Virtual Interop.
Testbed
Virtual USA – GIS & Client Visualizations
Northcomm & SSC – SAGE
21st Century Systems – Command Responder



(1) Sensor Management System

- Coast Guard & SSC

Capability: The Sensor Management System (SMS) enables the Coast Guard to remotely access and maintain a wide variety of sensor capability, including video cameras, and to display the information on maps and real-time streaming visualizations.

Interoperability Enabled: The SMS system is now able to display the real-time sensor feeds enabled through the use of open standards like Common Alert Protocol (CAP), KML, and the ease-of-use of URL feeds enabled through the REST open architecture-style.

Mini-Scenario: A potential harbor-centered terrorist threat is suggested by the Los Angeles (LA) Fire Department radiation sensor detection near the port. Based on regional policy, the Coast Guard is immediately able to receive the detection alert and monitor the location and status of the sensor readings. Through this improved sensor sharing, the Coast Guard and LAFD can effectively execute a shared, regional response with each utilizing their own chosen visualization and management systems.

Demonstration: The SMS Interoperability is enabled and ongoing. The interoperability is documented on the Interoperability Testbed Wiki and visible on Coast Guard terminals. The SMS system can be demonstrated upon request to interested parties with appropriate approval upon request. POC: Sandi Lehan, 619-767-4173, Sandi.Lehan@navy.mil

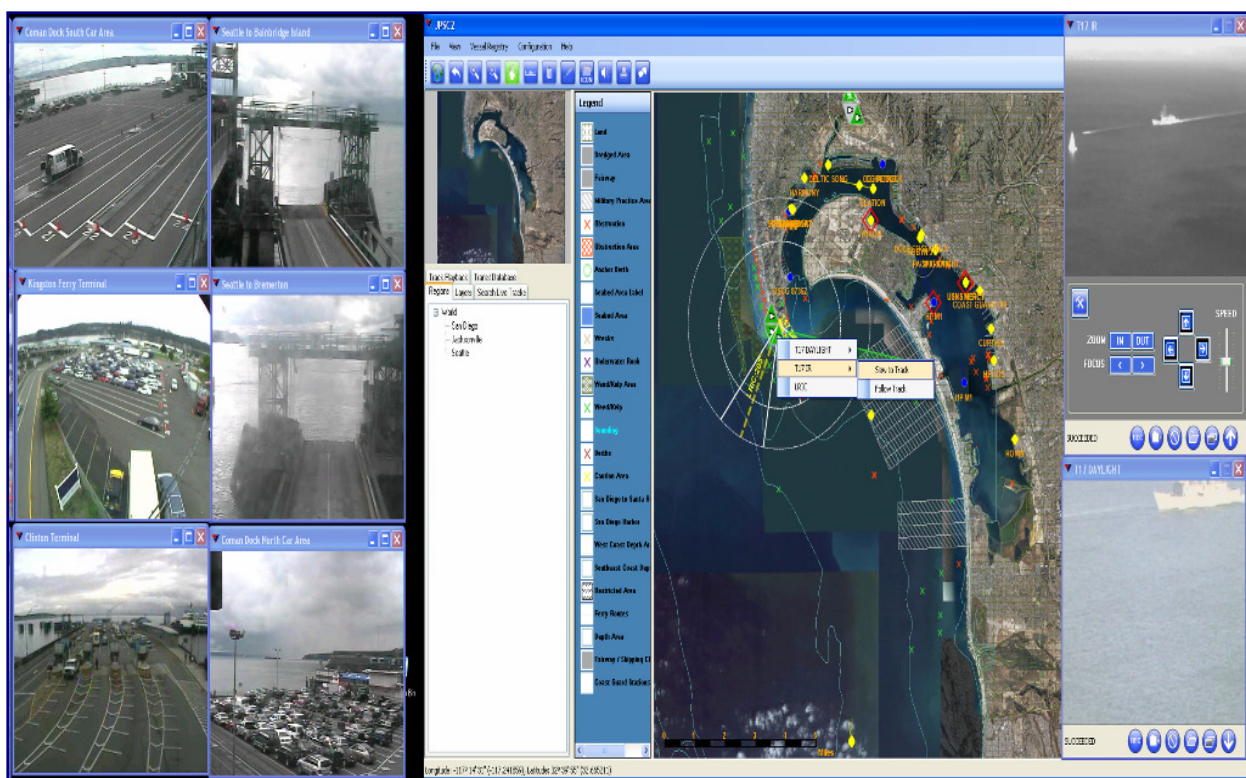


Figure 1: The Sensor Management System



(2) DE Routing Test

- Defense Threat Reduction Agency (DTRA)

Capability: DTRA is executing a test plan on behalf of DNDO to confirm the viability of standardized CBRN message sets routed using a commercial geospatial router.

Interoperability Enabled: Interoperability with the DTRA test router is enabled through the use of the National Information Exchange Model (NIEM) N25 (CBRN IEPD) message set and the use of the OASIS Distribution Element for specifying geographic point and keywords.

Mini-Scenario: A radiation detection occurs in key location of a major city. The detection is rapidly confirmed as being associated with a certain type of vehicle or device prior to detonation near a military facility or port. The detection-based information is shared in real-time and routed to other cities and regional authorities (military and civilian) who have subscribed to such alerts. Based on this tip-off, another major city is put on alert and is able to proactively move to disable a similar related threat in its own city. The other city is able to share its status, alerts, and proposed solutions with the original city to provide this type of proactive mutual aid.

Demonstration: The DTRA Router Test Interoperability is enabled and ongoing. The interoperability is documented on the Interoperability Testbed Wiki and visible on Coast Guard terminals. The DTRA routing results can be demonstrated upon request to interested parties with appropriate approval upon request.

POC: eric.perales@abq.dtra.mil

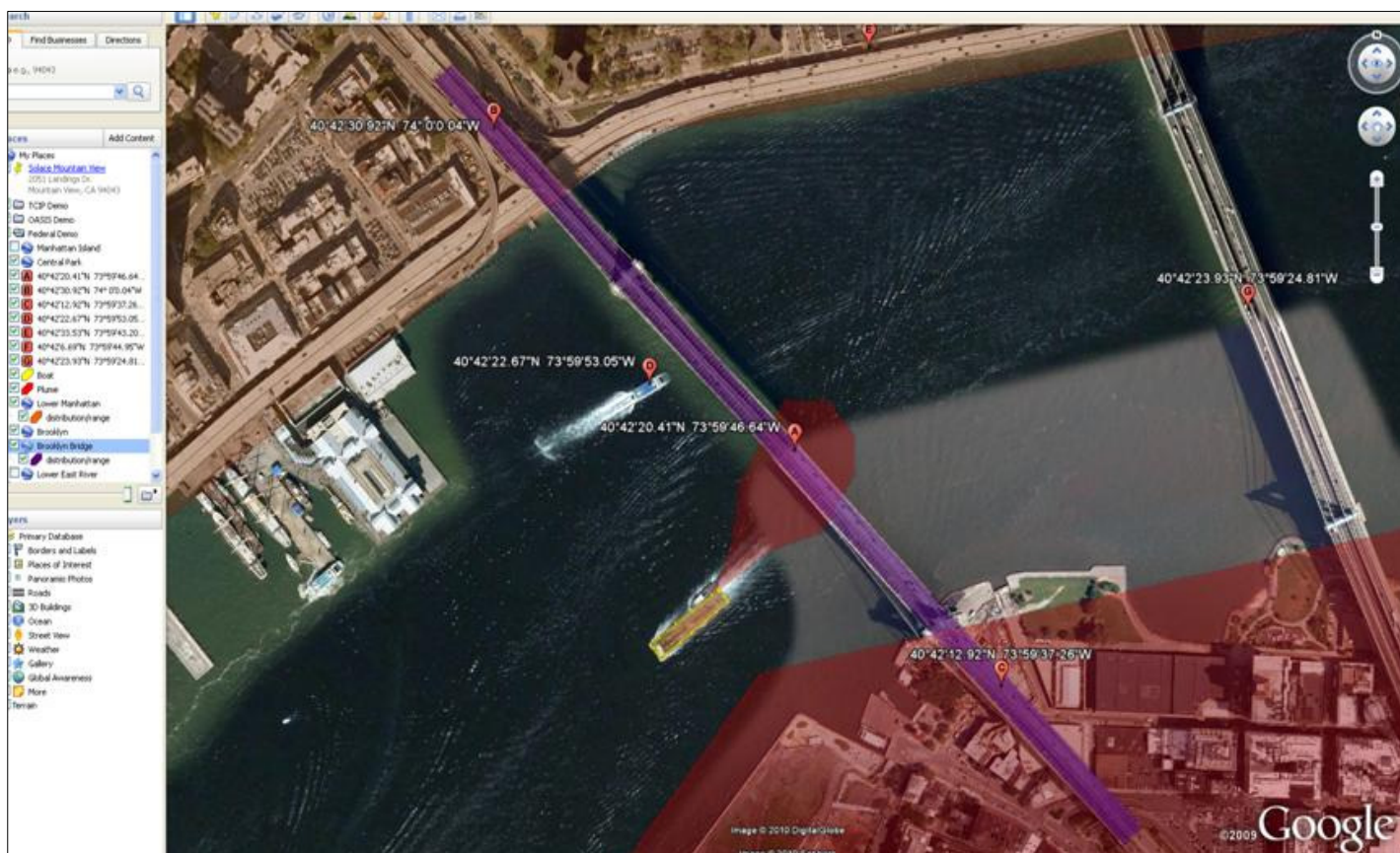


Figure 2: Sensor Detections Based on Geospatial Routing



(3) EDXL Standards

- DHS Office of Interoperability & Compatibility (OIC) and the Organization for the Advancement of Structured Information Systems (OASIS)

Capability: The standards comprising the Emergency Data Exchange Language (EDXL) facilitate emergency information sharing and data exchange across the local, state, tribal, national and non-governmental organizations. The effort focuses on standardization of specific messages to facilitate emergency communication and coordination. Any technology vendor or organization can easily develop their XML-based messaging exchanges using these standards, leveraging their existing legacy information technology applications. For more background on EDXL, see <http://xml.coverpages.org/edxl.html>.

Interoperability Enabled: The EDXL standards, primarily the Common Alert Protocol (CAP) and the Distribution Element, are a primary mechanism for improving interoperability as part of the message exchanges underway as part of Golden Phoenix. For example, the CBRN sensor detections are available from Los Angeles in the easy-to-use and widely understood CAP format. CAP can be converted into a variety of other formats as well. The Distribution Element is a wrapper facilitating geo and policy-oriented routing for any information payload. The DE is utilized for both routing CAP and N25 payloads.

Mini-Scenario: A radiation detection/alert must be shared across jurisdictions utilizing a number of emergency management tools not all of which understand specialized sensor formats. The detection is shared in CAP format since this format is well-understood by first responders and supported by a wide variety of existing emergency management tools. In addition, some jurisdictions are interested in subscribing to detections/alerts from anyone serving in a specified role in a specified geographic region. The jurisdictions can subscribe and receive the desired alerts in a standardized manner thanks to the use of the DE and the DE-enabled routers, like those used by DNDO.

Demonstration: The interoperability testbed includes a number of URL feeds which can be loaded into a browser to view the CAP and DE-wrapped sensor detections. DNDO and DTRA are using the DE in their demonstrations and the sensors feeding the various tools utilize the CAP format. For more information, please login to the interoperability testbed at <http://www.icbrne.org>. POC: David Lamensdorf, 661-295-5500, davidl@safeenv.com.

The screenshot shows the 'Cover Pages' website, which is an online resource for markup language technologies. The main content area is titled 'Emergency Data Exchange Language (EDXL)' and includes a 'Contents' section with links to Overview, Principal URLs, Specifications, and Articles, Papers, Presentations, Reports, News. Below this is an 'Overview' section that describes the initiative and lists several key documents, including the DHS-EIC Memorandum of Agreement (MOA), a slideset presentation on the Disaster Management eGov Initiative, and the EDXL Overview and Phased Approach. The website also features a sidebar with navigation links for Search, About, Core Standards, Technology Reports, Events, and Library.



(4) N25 (CBRN IEPD) & DE Routing

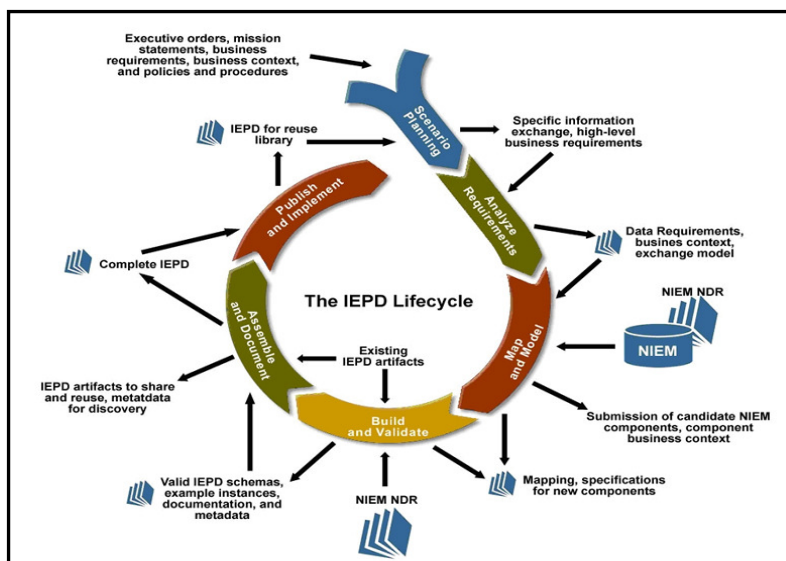
- Domestic Nuclear Detection Office (DNDO) & National Information Exchange Model (NIEM)

Capability: The National Information Exchange Model (NIEM) program enables a process for government organizations at all levels of government, including those representing first responders and emergency managers, to rapidly integrate multiple diverse standards with their concept of operations to enable effective message exchanges to meet their particular needs. The DNDO has been a leader in adopting this process, integrating a variety of standards relevant to their mission and conops (such as N25 conveyances and N42.42 radiation sensors), and developing a set of XML messages in the form of an Information Exchange Package Document (IEPD). In collaboration, with DHS CB S&T, a new version of the message set has been developed to include chemical and biological information. The result of these efforts is the CBRN IEPD which provides a holistic approach to ensuring the sensor detections are packaged in such a way that they become truly usable for a specific emergency management mission.

Interoperability Enabled: The current CBRN IEPD (also known by the term, N25) is being used by DNDO, DTRA, Solace, SSC and others as part of an interoperability pilot. You can learn more about the current CBRN IEPD at <http://www.niem.gov/CBRN.php>, and NIEM overall at <http://www.niem.gov/index.php>.

Mini-Scenario: A radiation detection/alert must be shared across a set of organizations that have developed a plan and collaborative process for handling such events. The detections occur at specified vehicle checkpoints with specified lanes of types of activity. When a detection is confirmed, the information, both a summary and a detailed analysis, is packaged in the CBRN IEPD along with information about the vehicle and about the specified checkpoint and lane of activity. This combined holistic set of information allows those at a remote analysis center to follow-up quickly with the summary information and make the decisions needed to respond to the incident. The detailed analysis information can also be routed to subject matter experts at remote collaborating organizations. Overall, the use of the CBRN IEPD allows these organizations to effectively enable their concept of operations using rapidly developed message sets based on standards.

Demonstration: The DNDO and DTRA are utilizing the CBRN IEPD in their routing test pilot activities which are ongoing. If you login to the testbed (<http://www.icbrne.org>), there are URLs which you can load into your browser to see the DE-wrapped CBRN IEPD message sets. Other visualizations are accessible by request. DNDO POC: Matt Kern, 202-254-7508, Matthew.Kern@associates.dhs.gov DTRA POC: Eric Perales, eric.perales@abq.dtra.mil





(5) Integrated Chemical Biological Radiological Nuclear and Explosive Detection Demonstration Program (ICBRNE)

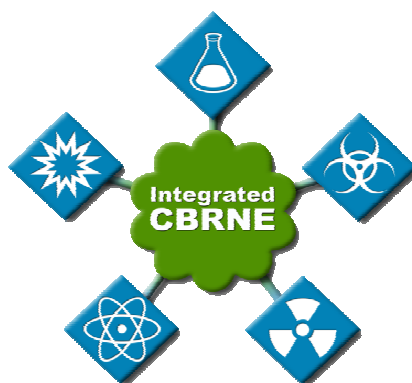
- DHS Science and Technology Directorate Chemical & Biological Division (see http://www.dhs.gov/xabout/structure/gc_1224531303278.shtm)

Capability: The DHS S&T Chemical and Biological Division launched the ICBRNE Detection Demonstration program to integrate interoperability standards and mechanisms with local policies and procedures to increase communication between both federal and first responder CBRNE sensor systems. The pilot is culminating in FY10 with the Golden Phoenix exercise in Los Angeles.

Interoperability Enabled: The effort has enabled Los Angeles to significantly improve its sharing of sensor detections with local, regional, state and federal stakeholders. Standards utilized include the EDXL and CBRN IEPD. Mechanisms enabled include the interoperability testbed and open architecture components. The overall result is better and faster regional response to CBRNE incidents and the resulting increase in saved lives and overall health and safety.

Mini-Scenario: When a hazmat incident occurs in a major city and region such as Los Angeles, there a variety of agencies that need to coordinate, including local (fire, police), regional (county health, port authorities, coroner, surrounding cities), state (highway patrol, governor), and federal (FEMA, other DHS, National Guard, nearby DoD military facilities). The use of standards, open architectures and lessons learned from the ICBRNE program allow the Los Angeles region, and other regions following the same model, to effectively share information and interoperate with each other for a combined regional response yet enabling each to continue using their own preferred tools and vendors.

Demonstration: The ICBRNE standards, mechanisms and lessons learned are on display at Golden Phoenix in Los Angeles on July 28, as well as in evidence on the documented results and capabilities accessible from the interoperability testbed. POC: Teresa Lustig, 202-254-5766, Teresa.Lustig@dhs.gov





(6) Disaster Management (DM) Open Platform for Emergency Networks (OPEN)

- FEMA (see <http://www.fema.gov/about/programs/disastermanagement/framework/conops.shtml>)

Capability: DM OPEN is an interoperability framework that is composed of a set of web service interfaces for sharing data among diverse systems. The interfaces are specifically designed to support EDXL messages, NIEM Information Exchange Packages, and standardized data structures that can be referenced by URI. In short, OPEN enables sharing of standardized messages among multiple organizations and jurisdictions. The DM OPEN capability will be aligned with the DM Framework which will provide a web interface, where users will interact via a browser in a composite web page comprised of configurable port lets. The combination of DM Framework and DM OPEN will provide a complete package for authoring, receiving, sharing and collaborating on emergency information.

Interoperability Enabled: The current sensor detections are being posted to OPEN in an IPAWS-compliant Common Alert Protocol (CAP) format. The IPAWS program, vendors, and others can access these detections for driving alerting devices.

Mini-Scenario: When a hazmat incident occurs, the public will need to be appropriately notified. When the Public Information Officer (PIO) for the appropriate jurisdiction determines it is appropriate, the PIO will issue an alert that can be carried over the Integrated Public Alert and Warning System (IPAWS) by posting to OPEN. In addition, new devices that are geo-aware, assisted by geo-enabled routers, have the potential to play highly targeted geographic alerts for a localized portion of the public most directly affected. Based on approved policies, this offers the potential for quick and automatic localized alerts similar to the type of capability enabled by a smoke alarm. Thus a confirmed sensor detection could drive a localized alert or warning.

Demonstration: The interoperability testbed is converting and posting sensor detections in IPAWS-compliant CAP format to a DM OPEN Collaborative Operations Group (COG) on an ongoing basis. Status and progress is documented on the interoperability testbed. A request for a DM OPEN account can be requested to access and utilize this COG and DM OPEN capabilities. POC: Gary Ham, 703-899-6241, gary.ham@eyestreet.com

FEMA

Contact Us | A-Z Index | Frequently Asked Questions | Español

Advanced Search [Go]

Home | About FEMA | Disaster Information | Plan & Prepare | Recover & Rebuild | Apply for Assistance | FEMA for You

Disaster Management

- DM-Framework & DM-OPEN 2.0
- DMIS Tools
- OPEN Web Services
- Interoperable Data Exchange
- Public Alerting
- About DM
- DM Contacts

DM Framework Concept of Operations

DM-Framework

Two major components of the DM-Framework will be a "Virtual Operations Center" or dashboard and an Incident Management application:

- DM Virtual Operations Center (VOC)/Work Center**
The DM-VOC is the strategic side of DM-Framework, providing the initial user interface for DM-Framework with dashboard capabilities that display summary level information on incidents, weather, maps, etc. The DM-WorkCenter dynamically connects people, applications, and knowledge with operational processes. The result is an intuitive environment in which different groups can work together effectively across geographical and institutional boundaries. The DM-VOC pulls and displays information from DM-WorkCenter, DM-OPEN 2.0, the Incident Management System (IMS), maps, and other applications.
- DM Incident Management System (IMS)**
The DM-IMS is the tactical component of DM-Framework, providing the basis for incident planning, management and response collaboration. The DM-IMS furnishes the functionality for authoring and sharing incident records and maps, operational planning, and emergency alerts.

DM-OPEN 2.0

DM-OPEN 2.0 will support four basic types of Web services, accessible to both DM-Framework and third party developers, with consistent methods for post and request operations:

- Common Alerting Protocol (CAP)**
Permits the exchange of emergency alert messages between organizations utilizing CAP-compliant, DM-OPEN 2.0 enabled services, including the DM-Framework and other, commercially available, systems.
- Non-Weather Emergency Messaging (NWEM)**
Routes a specialized form of CAP alert, the Non-weather Emergency Message, to the HazCollect server for distribution by the National Weather Service and relay to the Emergency Alert System.
- EDXL Distribution Element (EDXL-DE)**
Current and future EDXL standards-based messages are designed to be "wrapped" for delivery by the EDXL Distribution Element. Specific enhancements to EDXL-DE will improve message retrieval capabilities by leveraging category data structures, and hosting and providing access to type-lists for use in EDXL-DE messages.
- Administration**
Improved administration services will support retrieval and updating of basic system information.

DM Framework Related Documents

References

- Project Background
- Concept
- Stakeholders

Figure 6: DM OPEN (<http://www.fema.gov/about/programs/disastermanagement/framework/conops.shtml>)



(7) Integrated Public Alert & Warning System

- FEMA (see <http://www.fema.gov/emergency/ipaws/>)

Capability: IPAWS is the nation's next-generation infrastructure of alert and warning networks expanding upon the traditional audio-only radio and television Emergency Alert System (EAS) by providing one message over more media to more people for the preservation of life and property. IPAWS will provide federal, state, territorial, tribal, and local warning authorities the capabilities to alert and warn their respective communities of all hazards impacting public safety and well-being via multiple communications pathways.

Interoperability Enabled: OASIS has developed a specific version (profile) of its Common Alert Protocol (CAP) format to address IPAWS requirements. The current sensor detections are being posted to OPEN in this IPAWS-compliant Common Alert Protocol (CAP) format. The IPAWS program, vendors, and others can access these detections for driving alerting devices.

Mini-Scenario: A confirmed sensor detection-based alert is posted to OPEN in IPAWS-compliant format wrapped in a Distribution Element (DE). The alert is routed to appropriate portions of the public based on policies, sender Role, type of alert, and geography. An IPAWS-compliant device displays or plays the alert to those who need it.

Demonstration: The interoperability testbed is converting and posting sensor detections in IPAWS-compliant CAP format to a DM OPEN Collaborative Operations Group (COG) on an ongoing basis. Status and progress is documented on the interoperability testbed. IPAWS program participants can access and confirm that, if this were a real alert, it could be displayed or played through a variety of IPAWS compliant devices. POC: Tom Ferrentino, 716-913-4453, tferrentino@verizon.net

FEMA

Contact Us | A-Z Index | Frequently Asked Questions | Español

Advanced Search Go

Home | About FEMA | Disaster Information | Plan & Prepare | Recover & Rebuild | Apply for Assistance | FEMA for You

National Continuity Programs Directorate

Integrated Public Alert and Warning System (IPAWS)

History

Program Materials

IPAWS Projects

Partners

Industry Outreach

Accomplishments

Media Information

Integrated Public Alert and Warning System (IPAWS)

- [What is IPAWS?](#)
- [IPAWS Background](#)
- [What IPAWS Will Do](#)

What is IPAWS?

During an emergency, alert and warning officials need to provide the public with life-saving information quickly. The Integrated Public Alert and Warning System (IPAWS) is a modernization and integration of the nation's alert and warning infrastructure. IPAWS will integrate new and existing public alert and warning systems and technologies. Federal, State, territorial, tribal, and local government alert and warning systems will be able to integrate with the national alert and warning infrastructure providing a broader range of message options and communications pathways for the delivery of alert and warning information to the American people before, during, and after a disaster.

IPAWS is the nation's next-generation infrastructure of alert and warning networks expanding upon the traditional audio-only radio and television Emergency Alert System (EAS) by providing one message over more media to more people for the preservation of life and property.

IPAWS ensures the President can alert and warn the public under all conditions. IPAWS will provide federal, state, territorial, tribal, and local warning authorities the capabilities to alert and warn their respective communities of all hazards impacting public safety and well-being via multiple communications pathways.

IPAWS Program Vision: Timely Alert and Warning to American People in the preservation of life and property.

IPAWS Program Mission: Provide integrated services and capabilities to local, state, and federal authorities that enable them to alert and warn their respective communities via multiple communications methods.

IPAWS Program Strategic Goals:

- Goal 1 – Create and maintain an integrated interoperable environment for alert and warning
- Goal 2 – Make alert and warning more effective
- Goal 3 – Strengthen the Resilience of IPAWS Infrastructure

[Back To Top](#)

IPAWS Background

Since 2004, FEMA has served as the Federal Executive Branch lead agency for developing IPAWS. In June 2006, the President signed the [Public Alert and Warning System Executive Order](#) which states, "It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people...establish or adopt, as appropriate, common alerting and warning protocols, standards, terminology, and operating procedures for the public alert and warning system to enable interoperability and the secure delivery of coordinated messages to the American people through various communication pathways."

Figure 7: IPAWS: <http://www.fema.gov/emergency/ipaws/>



(8) C4ISuite

- Fleet Forces Command & SSC

Capability: C4ISuite is a situational awareness web-based capability that is providing the Fleet Forces Command improved overview, alerting, and visualization of status.

Interoperability Enabled: Through the use of open standards and architectures, the C4ISuite team was able to quickly integrate the sensor detections into their C4ISuite system and visualizations.

Mini-Scenario: A confirmed sensor detection-based alert is posted to the region. The Fleet Forces Command has assets that are potentially impacted. The command can get the alert in real-time and visualize along with their other status information. The command can now collaborate as policy allows with regional authorities on the incident.

Demonstration: Interoperability Testbed participants can request a demonstration of C4ISuite and its ability to visualize the sensor detections. A screen dump and documentation of the capability will be documented as well. The capability is ongoing and will help support future testbed activities. A version of C4ISuite accessible for exploration and testing by first responders is planned for the testbed. POC: Sandi Lehan, 619-767-4173, Sandi.Lehan@navy.mil

(9) SAView

- Kansas City Regional Terrorist Early Warning Center (TEW)

Capability: The TEW is a multi-agency analysis center which ensures a coordinated flow of intelligence to and from all sectors and levels of government. The TEW additionally identifies and addresses specific threats and response plans. The end result of this effort is the ability to view raw data from all sectors of the community and provide analytical insights with specific and actionable informational products to help agencies with the Homeland Security mission identify threats before terrorists can act. (See summary on page 15 of http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=81c0387a-e20c-4b02-8257-6885b0e1c3f5) The Situational Awareness Viewer (SAV) is a visualization and management capability enabled by the TEW to support the mission.

Interoperability Enabled: Sensor detections in CAP format are routed via the Distribution Element through the Solace router as part of the DNDO/DTRA pilot effort. The TEW can subscribe to items of interest, including these detections, based on geography, keywords, and roles. The CAP format is converted into the Air Force's standard Cursor on Target (CoT) to enable interoperability with SAV which can readily utilize data in CoT format.

Mini-Scenario: A jurisdiction of interest (e.g. the Kansas City TEW) subscribes for any early warnings of potential "terror" threats. In another jurisdiction, a sensor detection is received and confirmed to be from a suspicious device that might be a terror threat. The detection is routed to the subscriber and automatically converted into the desired format. The enabled interoperability via standards provides for easy conversion among the CAP and CoT formats. An early warning is received and the receiving jurisdiction is able to identify and disarm a similar threat from a multi-city terror incident.

Demonstration: An account to access the SAV interface is possible for certain approved individuals. The interoperability is ongoing based on subscriptions as needed, as part of the DNDO/DTRA router pilot. POC: Troy Campbell, (816) 413-3605, tcampbell@kcpd.org

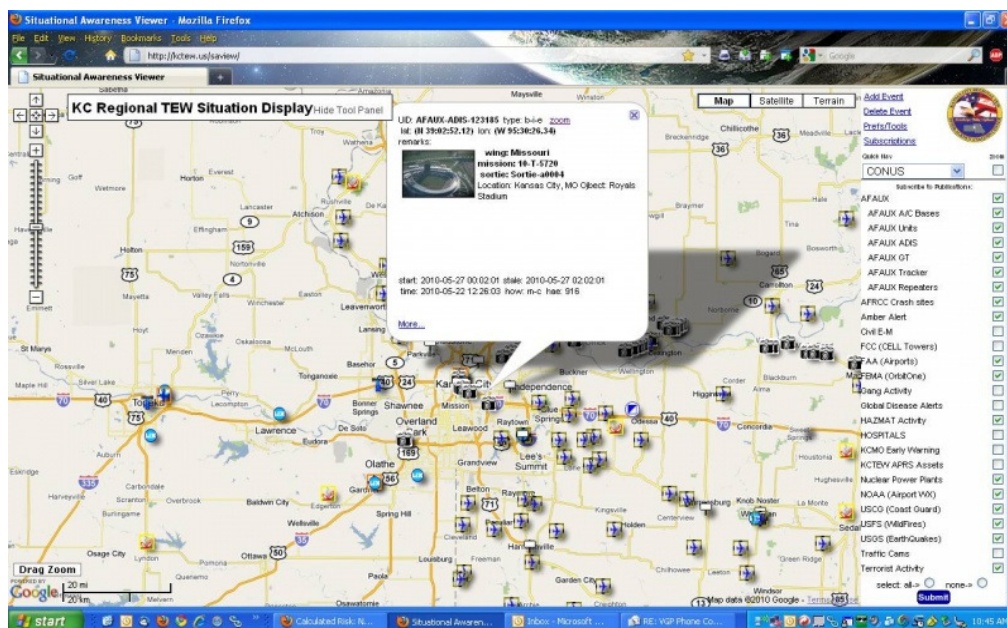


Figure 9: Situational Awareness Viewer (SAView)

(10) IC.NET

- The MITRE Corporation

Capability: MITRE is a non-profit Corporation that operates four Federally Funded Research & Development Centers for the US Government. Our work with the Virtual Golden Phoenix initiative is to support operational-level and bottom-up information sharing by empowering State and Local jurisdictions to be able to interoperate using data standards, existing COTS products, and research / prototyping efforts. IC.NET is a prototype designed for the exchange of Emergency Data at the ICS operational level. This prototype leverages the encapsulation and routing capabilities of the EDXL Distribution Element (EDXL-DE) and supports message payloads such as Common Alerting Protocol (CAP), EDXL Hospital Availability Exchange (EDXL-HAVE), EDXL Resource Messaging (EDXL-RM), and two placeholder standards for Situation Reporting and Tracking of Emergency Patients. Through this prototyping effort we sought to provide a common messaging platform to experiment with connecting of emergency systems such as Computer Aided Dispatch (CAD), Mobile Data Terminals (MDT), incident command software, field sensor data using the EDXL data standards.

Interoperability Enabled: Sensor detections in CAP format are routed via the Distribution Element through the IC.NET routing capability based on the appropriate role and keywords. The output is visualized in either of two Virtual USA visualizations, including Virtual Alabama and Viper.

Mini-Scenario: A jurisdiction of interest subscribes for any sensor detections from anyone in a given ICS role. The routing capability delivers the detection based on role and keywords. The information is automatically converted into the appropriate standard format (e.g. KML) to be displayed on the client visualization.

Demonstration: IC.NET is a prototype capability that will continue to be demonstrated and developed as part of a MITRE internal research effort. The capability will soon be extended and enabled as a capability accessible to first responders for exploration and testing, including as a node of the virtual interoperability testbed ongoing capability. POC: Don McGarry, The MITRE Corp. 703-595-9375, dmcgarry@mitre.org; Kelly Gerschevske, The MITRE Corp. 719-572-8366

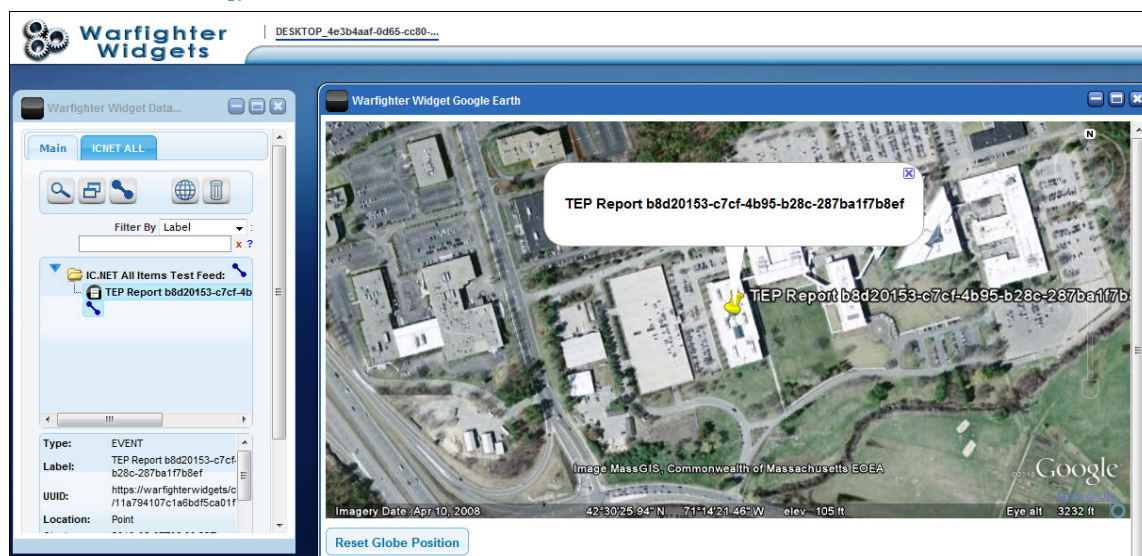


Figure 10: Visualization of IC.NET

(11) Interoperable Wireless Hazmat Sensors

- Safe Environment Engineering (see <http://www.safeenv.com>)

Capability: Safe Environment Engineering is the ICBRNE lead organization for the Los Angeles region and has been providing lifesaving wireless communications technologies since 1993. These technologies have greatly increased the safety of first responders, such as fire departments, rescue teams and maintenance personnel. At the same time they increase the efficiency of such departments, thereby reducing the cost of deployment and operations. Safe Environment Engineering provides the wireless Lifeline Interoperable Network Communicator (LINC) to enable traditional hand-held chemical, radiological and other sensors to send their readings for remote display anywhere in the world.

Interoperability Enabled: Safe Environment Engineering is the primary enabler of interoperability by interfacing with the proprietary sensor format and converting the information into a standard CAP format. Safe Environment is the enabler of the entire system of sensor detections which are then utilized by others for display, routing, assessment and decision-making.

Mini-Scenario: A hazmat incident is underway and firefighters are deployed with Level A suits. The weather, smoke, and other environmental conditions and demands make it difficult to read meter displays. But back in the fire truck, other fire personnel can review the meter readings; ensure accuracy and safety of the firefighters in the field, thanks to the wireless capability. The readings are also sent in real-time and visible to interested remote personnel for situational awareness, including other approved agencies and jurisdictions using other emergency management tools, thanks to the use of standard formats such as the EDXL Common Alert Protocol (CAP). Alerts and notices to off-site personnel are enabled using alerting services via the same approach to standardization and web-based architectures.

Demonstration: Visit <http://www.icbrne.org> for a brief video demonstration of the Interoperable Wireless Hazmat Sensor capability. The tools and capabilities visible throughout Golden Phoenix are utilizing the sensor feeds enabled through this wireless capability. Additional demonstrations are available upon request. POC: David Lamensdorf, 661-295-5500, davidl@safeenv.com

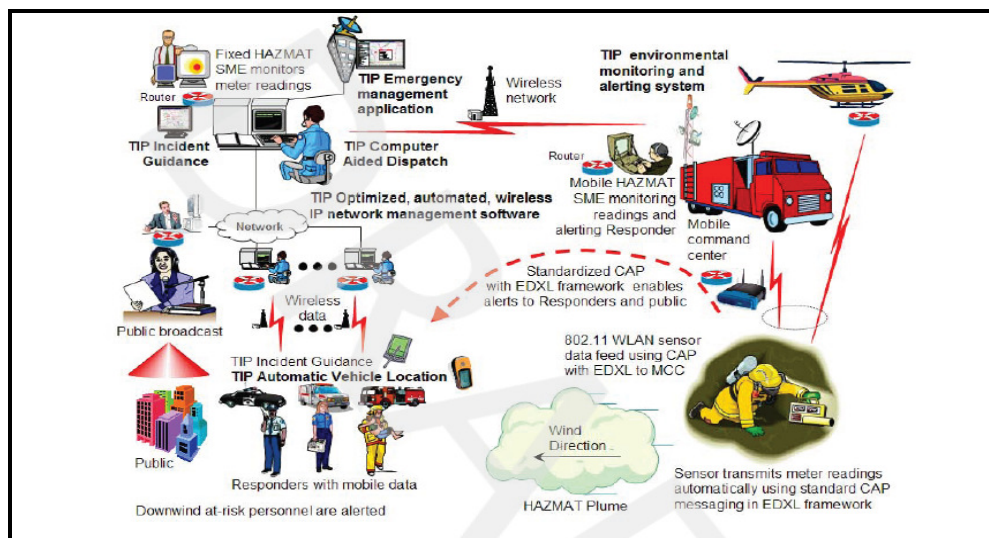


Figure 11. Interoperable Wireless Sensors in Action

(12) EDXL DE & Geospatial Routing

- Solace Systems (see <http://www.solacesystems.com/news/dhs-dndo-selects-solace-geospatial-routing-emergency-management-network>)

Capability: Solace is providing the capability for all participants to use the Solace Content Router for real-time exchange of XML messages using Publish/Subscribe. Message formats supported include (but not limited to) EDXL and NIEM. Messages can be stored on the router to enable senders and receivers to exchange messages when they are not both connected at the same time (i.e. guaranteed delivery). Access to the Solace Content Router is via API's which Solace will provide to any interested participant. Languages supported include C, C#/.Net, and Java. Platforms supported include Solaris, Linux, and Windows (although Java API also works on Apple Mac OSX or other Java capable platforms). The Solace Content Router also supports XML transformations using XSLT to convert messages from one format to another or to wrap messages (such as wrapping CAP messages in EDXL-DE). The Solace Content Router also supports geospatial routing and filtering of messages in EDXL-DE format.

Interoperability Enabled: Solace is providing the primary production-level geospatial routing capability with is EDXL-DE compliant and selected by DND0 for use in their routing pilot. Sensor detections are posted to the router in NIEM CBRN IEPD format, wrapped in a DE, and routed to subscribers based on policy and geospatial criteria. The input and output format are converted to a variety of standard formats as needed, such as CoT and CAP.

Mini-Scenario: Local jurisdictions have agreed upon an information sharing policy determined by type of information and sender and receiver roles. The policies can be implemented in the router and enabled with the use of the EDXL DE. In addition, geo-specific alerts can be routed to subscribers.

Demonstration: The Solace routing capability of sensor detections is ongoing. Pictures and details of the router and capabilities are available on the interoperability testbed (<http://www.icbrne.org>) and at <http://www.solacesystems.com/solutions/content-networking/geospatial-routing>. Live demonstrations are available upon request. POC: Hans Jespersen, (650) 924-2670, hans.jespersen@solacesystems.com

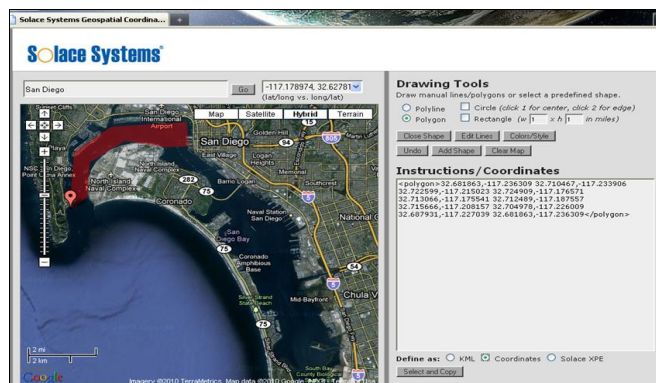


Figure 12: Solace Router Enables Geospatial Routing

(13) Virtual Interoperability Testbed

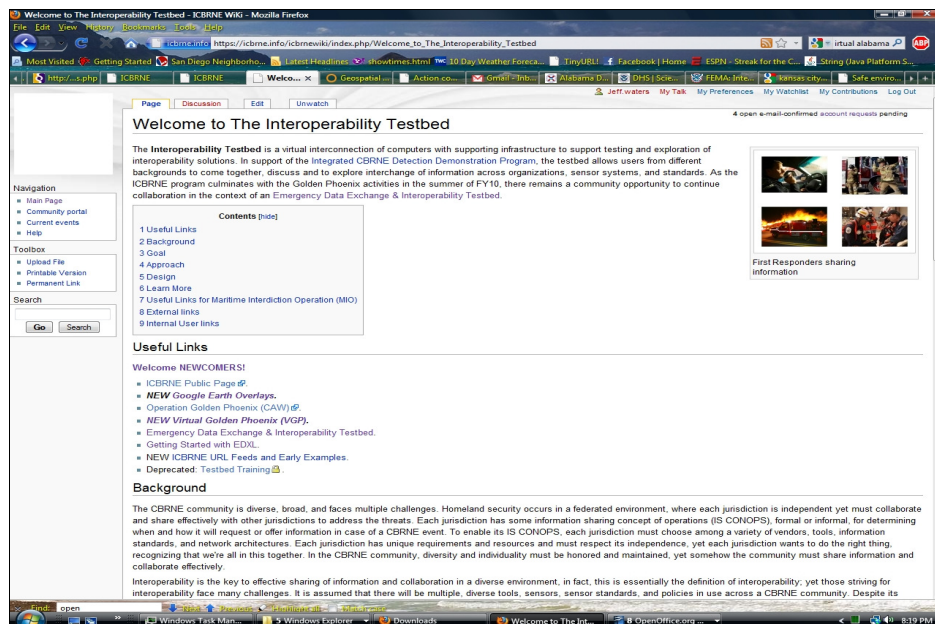
- SPAWAR Systems Center (SSC) Pacific (See <http://www.public.navy.mil/spawar/Pages/default.aspx>.)

Capability: SSC is the Navy's premiere RDT&E System Center for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). SSC is the testbed lead for the ICBRNE program. SSC, along with its partners, has enabled a powerful mechanism for exploration, education, and testing of system-to-system interoperability utilizing standards and open architectures. The focus of the standardization effort is on EDXL and NIEM CBRN IEPD. The testbed includes important infrastructure components including a wiki, a RESTful repository, and routines for converting to various standard formats, and helpful links and educational material for learning EDXL.

Interoperability Enabled: Any testbed participant has the opportunity to interoperate with sensor detections in a variety of formats accessible via URLs. A variety of visualizations are enabled, including Google Earth Overlays. A RESTful interface provides programmatic access to the repository for getting or posting data, with web-based encryption and authentication. The wiki provides educational information and status/progress reports on current activities by participants.

Mini-Scenario: A local jurisdiction does not have the budget to enable an IT staff and fancy new tools, but they do have an IT-savvy first responder with a passion for improving processes and a long-time trusted support vendor. The first responder and vendor obtain accounts on the interoperability testbed. There they learn quickly the practical use and benefits of standards like CAP and the DE. They learn from others, how to obtain and visualize sensor information, and how to improve sharing with web-based architectures. Soon they enable both a free mapping visualization and a web-based repository for sensor information and are able to share an existing router capability from a regional location. The local jurisdiction is able to bootstrap itself forward to enable real-time sensor detection-based information sharing and management.

Demonstration: Any first responder, government employee, or any person affiliated with a government agency, such as a vendor, may request and obtain an account on the interoperability testbed. Just go to <http://www.icbrne.org> the testbed is accessible 24/7 and your participation is welcome. POC: Sandi Lehan, 619-767-4173, Sandi.Lehan@navy.mil



(14) Virtual USA

- Department of Homeland Security (see http://www.dhs.gov/ynews/releases/pr_1260375414161.shtm)

Capability: Virtual USA is an information sharing initiative launched by DHS in December of 2009. Virtual USA links disparate tools and technologies in order to share the location and status of critical assets and information—such as power and water lines, flood detectors, helicopter-capable landing sites, emergency vehicle and ambulance locations, weather and traffic conditions, evacuation routes, and school and government building floor plans—across federal, state, local and tribal governments.

Interoperability Enabled: Although the Virtual USA pilot has not yet reached the southwest region, states such as Alabama have demonstrated leadership in developing their Virtual USA capability and sharing it with other jurisdictions. The Virtual Alabama team has granted accounts and access to their server in an effort to explore interoperability of sensor detection feeds with this model Virtual USA system. The major URL sensor feeds have been demonstrated to load and operate in the Virtual Alabama Google Earth client.

Mini-Scenario: A local jurisdiction needs to map all of its key geospatial information needed for effective response to an emergency, including a map of its sensor detections. The Virtual USA client can be leveraged to visualize this information and the server can host the links to the information but the information itself can be maintained and secured locally. The local jurisdiction gets the best of both worlds, it can leverage the successful mapping client, server and GIS information of a Virtual USA system but still keep control of and update its own information.

Demonstration: Screen dumps of the Virtual Alabama system showing the California sensor detections are available on the interoperability testbed. Those with a Virtual Alabama account and client can load the URL feeds available from the link for “New Google Earth Overlays” also on the testbed wiki. Other demonstrations are available upon request. For local use of the Virtual Alabama client, contact Sandi Lehan, 619-767-4173, Sandi.Lehan@navy.mil. For information on Virtual Alabama, visit http://www.dhs.alabama.gov/virtual_alabama/home.aspx and the Alabama POC: Chris Johnson, 256-721-7104, chrisj@gstac.org



(15) SAGE

- NORTHCOMM & SSC

Capability: SAGE is the Northern Command's unclassified Common Operational Picture. SAGE provides a wealth of information from the unclassified side of the house to aid in situational awareness and decision-making.

Interoperability Enabled: SAGE can accept typical mapping standards such as KML. The sensor detections can be easily converted once they are in a standard XML format like CAP. The conversion then allows posting of the alerts or pulling of the feeds from the URLs.

Mini-Scenario: A sensor detection in a local jurisdiction confirms a potential terror threat. While local authorities investigate, the detection is routed for situational awareness purposes to NORTHCOMM's unclassified COP, SAGE. Unknown to these local authorities another sensor detection in another jurisdiction also suggests a potential terror threat. SAGE receives both alerts and the authorities at NORTHCOMM begin to monitor the incidents more closely and look for parallels. The same hazardous material is identified on both readings and pictures and follow-up confirms the incidents are linked. The interoperability and sharing of sensor detections with SAGE helps to uncover a significant terror threat.

Demonstration: The interoperability is documented on the Interoperability Testbed Wiki whereby KML files will be overlaid onto SAGE. POC: Dave McKinley, SPAWAR, J623 United States Northern Command, david.mckinley@northcom.mil, 719-554-4950, Cell: 719-440-1813, Blackberry: 719-359-7930

(16) Command Responder

- 21st Century Systems, Inc.

Capability: Command Responder was developed to satisfy the following critical capabilities essential to the tasks and missions of Homeland Defense and emergency response organization. It provides a full spectrum emergency management tool that cuts across the pre-event and post-event phases of mitigation, preparedness, response and recovery. It develops and sustains shared situational awareness for public and private sector organizations involved in incident management by integrating multiple live data feeds with geospatial visualization and function-based data processing.

Interoperability Enabled: Through a deliberate design approach that integrates the human and technical aspects of the Incident Command System (ICS), Command Responder provides operators with a tiered development of situational awareness in order to facilitate time-critical decision making (see graphic on next page). In addition, the ability to integrate historical data and lessons learned with real-time data-feeds and information sharing enables incident commanders and their staffs at the local, state, national, and international levels to *rapidly transition from reactive to proactive incident action planning and response*. The system also enables operators to create and execute crucial disaster management tasks using a collaborative electronic checklist. This checklist component of CR employs a web-based, service oriented architecture (SOA) and web-client capabilities, thus allowing true event collaboration to a large number of response organizations with web access. Moreover, CR system architecture provides modular flexibility that allows for escalation or transfer of disaster management responsibilities to other emergency response organizations by simply logging into the event over a web connection. The CR program is structured to very quickly integrate agent based technology and fuse information from a combination of live data feeds, GIS layers and historical information in order to provide course of action recommendations to the planning arm of the organization

Mini Scenario: A confirmed sensor detection-based alert is posted to the region. The State and Locals utilizing Command Responder has assets that are potentially impacted. The Region can get the alert and



visualization in real-time and visualize along with their other status information. The Region can now collaborate as policy allows with other regional authorities (State, Local, Federal, and Tribal) on the incident

Demonstration: Interoperability Testbed participants can request a demonstration of Command Responder and its ability to visualize the sensor detections. A screen dump and documentation of the capability will be documented as well. The capability is ongoing and will help support future testbed activities. A version of Command Responder accessible for exploration and testing by first responders is planned for the testbed.

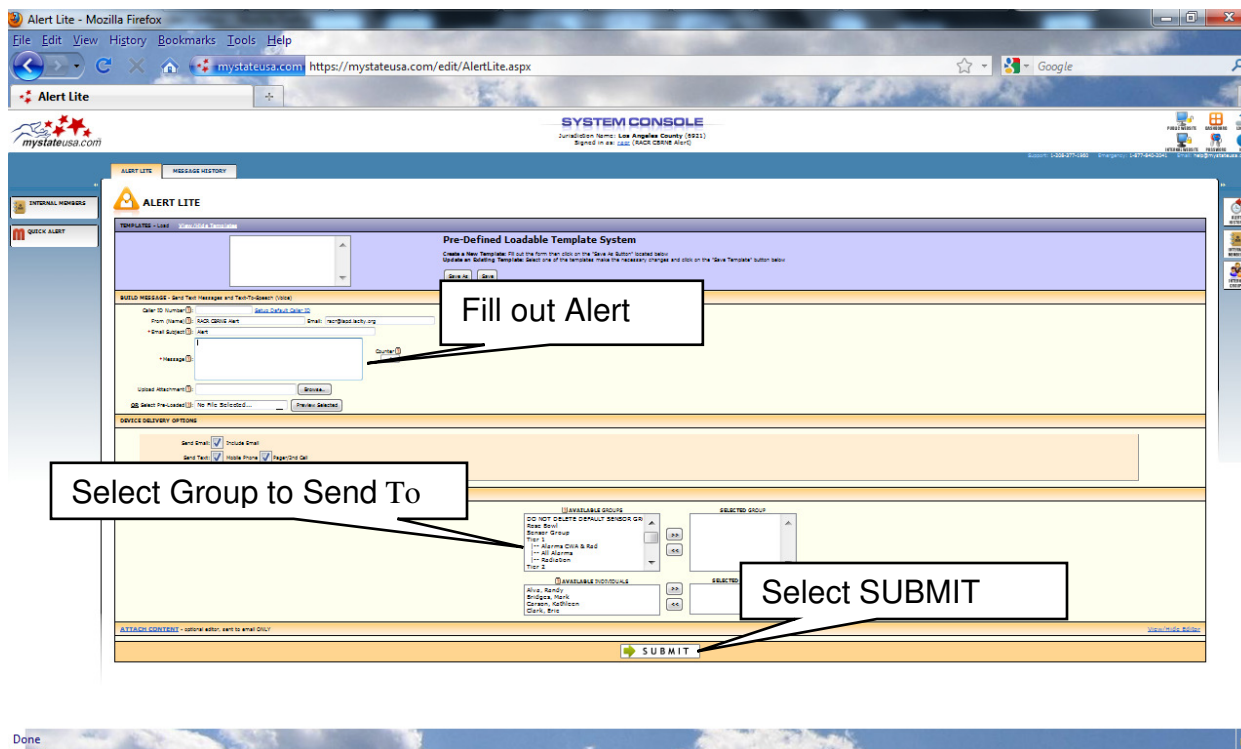
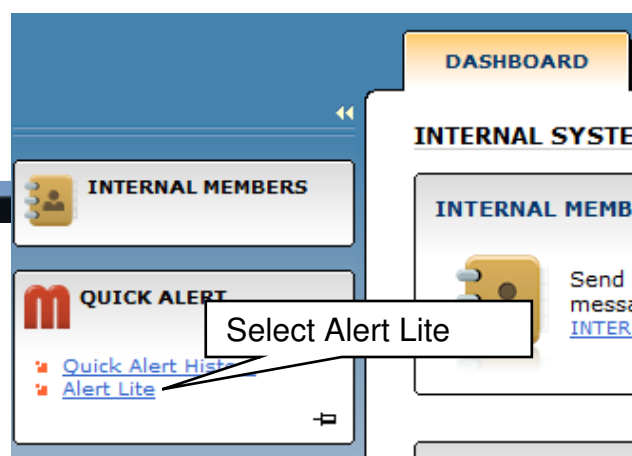
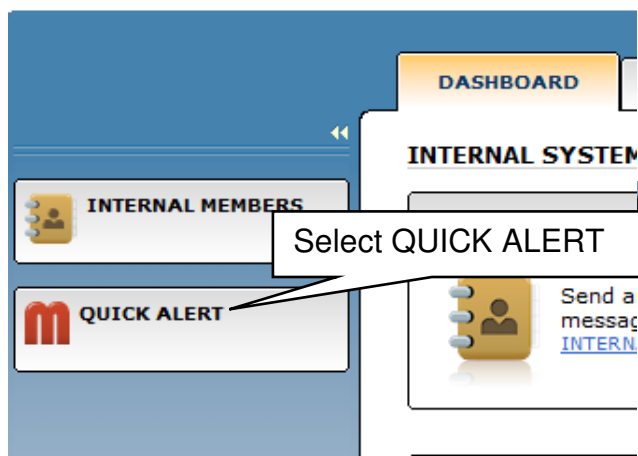
POC: Clifford Link (858) 254-1944 clifford.link@21csi.com



16 Appendix I – Training Materials

16.1 ICBRNE Alert Quick Start Guide

To Log-in





INTERNAL GROUPS | [ADD GROUP](#) | [VIEW UNGROUPED MEMBERS](#)

Group ?	Members	Description	Added On	
<input type="text"/>				<input type="button" value="FIND"/> <input type="button" value="ALL"/>
<input checked="" type="checkbox"/> DO NOT DELETE DEFAULT SENSOR GROUP	1	To test the CAP XML notification	2/24/09	Print Export Delete
<input checked="" type="checkbox"/> Rose Bowl	8		12/18/09	Print Export Delete
<input checked="" type="checkbox"/> Sensor Group	1		10/25/07	Print Export Delete
<input checked="" type="checkbox"/> Tier 1	0	Sensor Direct	2/14/10	Print Export Delete
<input type="checkbox"/> Alarms CWA & Rad	1		2/14/10	Print Export Delete
<input type="checkbox"/> All Alarms	9		2/14/10	Print Export Delete
<input type="checkbox"/> Radiation	1		2/14/10	Print Export Delete
<input checked="" type="checkbox"/> Tier 2	2	Sensor + Manual	2/14/10	Print Export Delete
<input checked="" type="checkbox"/> Tier 3	20	Situational CBRNE	2/14/10	Print Export Delete
<input checked="" type="checkbox"/> Tier 4	1	General Other CBRNE Related (ex: hospitals)	2/14/10	Print Export Delete
<input checked="" type="checkbox"/> Tier 5	3	Actual or Potential Fatalities	2/14/10	Print Export Delete
<input checked="" type="checkbox"/> Weather Alerts - All State	0	Members in this group will receive State-wide weather alerts.		Print Export
<input checked="" type="checkbox"/> Weather Alerts - County Only	0	Members in this group will receive County-wide weather alerts.	3/9/07	Print Export

Records Found: (12)



Testbed Demo Training



ICBRNE :

ICBRNE Testbed Demo Training



ICBRNE : ICBRNE Demo

Steps:

1) : Select "ICBRNE Demo"

The screenshot shows the ICBRNE website with the following content:

- Learn More**
 - [ICBRNE Video](#)
 - [OSDS CAP Specification](#)
 - [ICBRNE TESTBED](#)
 - [ICBRNE Overview \(pdf\)](#)
 - [ICBRNE Logo](#)
 - Demos**
 - [RealTime Sensors \(Mobile\)](#)
 - [RealTime Sensors \(VUL\)](#)
 - [RealTime Sensors \(VUL\)](#)
 - [RealTime Sensors \(VUL\)](#)
 - [ICBRNE Demo](#) (highlighted with a red box)
 - [Testbed Homepage \(All Demos\)](#)
 - Points of Contact**
 - [State Environment Engineering](#)
 - Objectives**
 - Address the concerns expressed that directed efforts to be taken to reduce communications gaps that arise from disparate CBRNE systems
 - Enhance multi-jurisdictional information Concept of Operations
 - Use Federal open standards and protocols
 - Goal**
 - Integrate interoperability standards and mechanisms with local policies and procedures to increase communications between both federal and first responder CBRNE sensor system
- News and Events**
 - Sept 28 - Oct 5 - 2009 - United Nations Exercise, Los Angeles CA
 - Sept 17, 2009 - New Meter Display Added: Thermofisher idenTFINDER
 - Sept 16, 2009 - New Website CDPF and Domain Name - The ICBRNE testbed integration website now has a new name and SSL certificate: "icbrne.info". Any browser favorites containing 64.160.7.213 should be changed to icbrne.info.
- Benefits of ICBRNE**
 - Save lives and protect property** by providing near real-time, vetted emergency management information to the responder community
 - Increase sharing across responders** - Facilitate the rapid, end-to-end transfer of CBRNE sensor information for risk assessment and decision support across multiple agencies and jurisdictions
 - Increase awareness** - Enable a collective view of response information and GIS overlays that will support responders in the field as well as housed and other SOCC analysis
 - Automate alerting and messaging** - Ensure rapid, secure sharing of sensor information to the agreed-to recipients (people and systems) within the response community
 - Develop policies and procedures** for information sharing across agencies - Facilitate regional collaboration to develop the business rules that deliver the right information, to the right person, at the right time
 - Execute a sustainable solution** - Demonstrate enhanced information sharing using city infrastructure to apply affordable, standards-based messaging protocols that can be commercially implemented to meet current and future needs
- Full Calendar**
 - August 2009
 - Aug. 5, 2009 Initial Planning Conference ("TableTop") - Test Bed Initial Demonstration
 - September 2009
 - Sept. 1, 2009 Stakeholders Recommend Vendor/Technical Reqs
 - Sept. 1, 2009 Interim Start of Test Bed Integration for Vendor/Technical Reqs
 - Sept. 16-18, 2009 (Rescheduled until October due to schedule conflicts) Test Bed - Online Training Session #1 for Program Managers



ICBRNE : Enter Username/password

Steps:

1) You should be prompted for a username/password.

If you do not have a username/password

a) Request an account on www.icbrne.org

Or

b) Contact: bruce.plutchak@navy.mil



ICBRNE : Sensor Detection Report – Sensors (Live) (Active Sensors)


Steps:

1) Select "Sensors (Live)" Tab

Shows Sensor "last Readings" (Reloads every 10 seconds)

SensorType	Org	MacID	Sent	View	User	Incident	Note	Data
Dräger X-am 7000	Squad48_xam_126.xml	000B28022952	2009-10-19T10:11:29-07:00	Meter				CO2 0.0 % CH4 0.0 % H2S 0.0 ppm LEL 0.0 %
Brüel Kjaer DAVID-M	Squad129_IHAZMAT_RaidM203.xml	000B6B7771A4	2009-10-19T10:12:38-07:00	Meter				Test: Noise B=0 C=0 L=0 mg m3
RAE Systems PGM-150-3P	Squad129_IHAZMAT_Rae205.xml	000B6B77737D	2009-10-19T10:12:37-07:00	Meter				CO 0.0 ppm VOC 0.0 ppm H2S 0.0 ppm LEL 0.0 %
Industrial Scientific ITX	squad48_ITX_120.xml	000B2802229E	2009-10-19T10:12:27-07:00	Meter	Squad 48 ITX 120			LEL 0.0 % CO 20.9 ppm H2S 0.0 ppm RDS 0.0 ppm
Ludlum Measurements Model 2241	Squad129_IHAZMAT_Ludlum202.xml	000B6B777186	2009-10-19T10:12:36-07:00	Meter				Parameter Model 44-9 Variable 0-5M Detector (Provisional) 10-19-03 µB/hr
Thermo FH 40 G	SafeEnvMonitor.xml	000B28024154	2009-10-19T10:11:29-07:00	Meter	SEE HQ Thermo FH40 G Unit			Internal 20.37 µB/h External 7.043 µB/h
RAE Systems 0003S	SafeEnvMonitor.xml	000000005005	2009-10-19T10:11:01-07:00	Meter	theOtherMicron	Test		CO 3.6 ppm VOC 1.6 ppm LEL 55.9 %
PostSampleMeter	SettingsFile	071217111	2009-10-19T10:11:19-07:00	Meter	sscUser	test	test	sensor 1 %

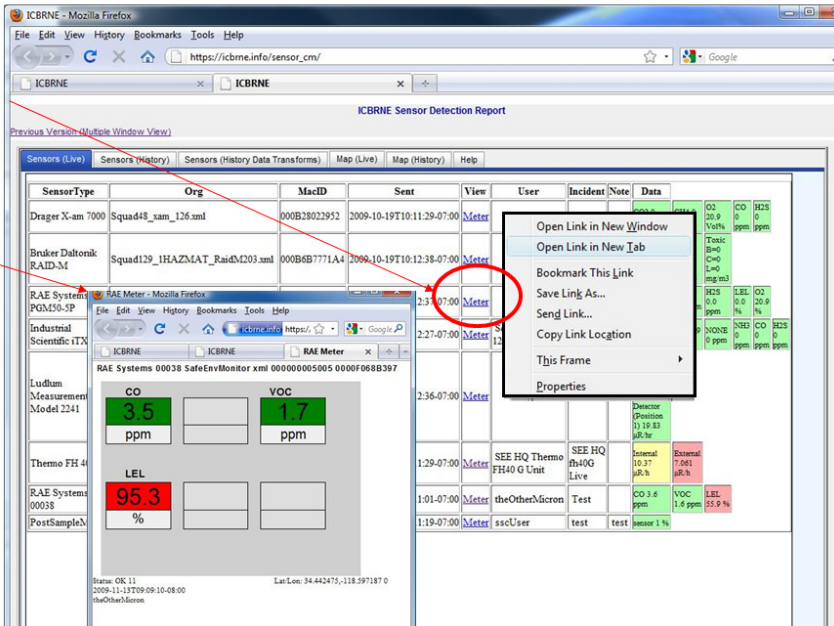





ICBRNE : Sensor Detection Report – Sensors (Live) View Meter

Steps:

- 1) Select "Meter" to View Meter
Live Meter readings will be displayed
- 2) Meter Displayed

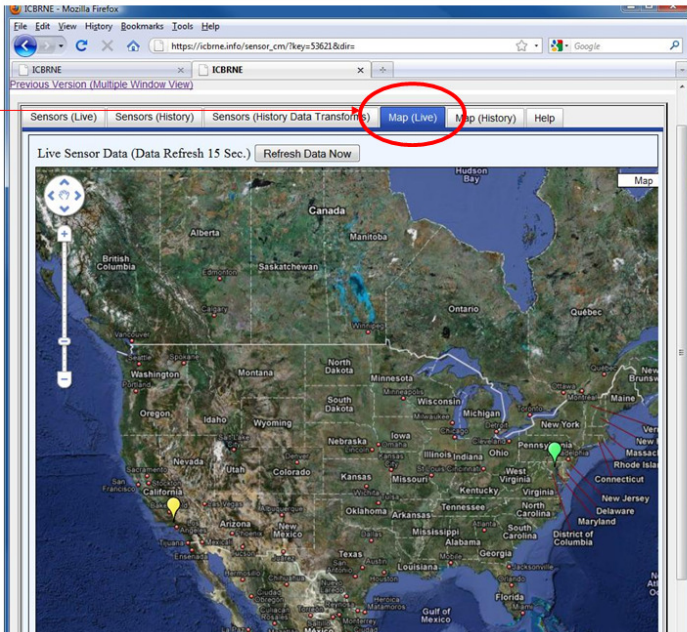




ICBRNE : Sensor Detection Report – Map (Live) (Active Sensors)

Steps:

- 1) Select "Map (Live)" Tab
Shows Sensor on GoogleMap "last Readings"
(Reloads every 10 seconds)





ICBRNE : Sensor Detection Report – History

Steps:

- 1) Select "Sensors (History)" Tab

Shows sensor history of "candidates". Item has gone "RED".

- 2) Select "All Data" Checkbox

If "All Data" is selected, multiple data points are returned for each sensor. If NOT selected, only the last reading is returned.

- 3) Filter-Search / Submit

Limits the result to CAP alerts containing the search string.

Sensor Type	ID	Date	Incident	Note
NIEM_Draeger_115	000B6B7790FC	2009-10-01T12:02:57-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-10-01T11:45:27-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-10-01T07:25:14-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-10-01T07:24:04-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-10-01T06:58:15-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T15:54:20-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T15:36:56-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T15:24:12-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T15:00:59-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T15:00:22-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T14:59:57-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T14:14:34-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T13:54:55-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T13:48:38-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T11:37:52-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T11:35:14-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T11:33:26-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T11:33:59-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T11:33:26-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T11:11:40-07:00	EIS_CAP 001	
NIEM_Draeger_115	000B6B7790FC	2009-09-30T10:49:03-07:00	EIS_CAP 001	

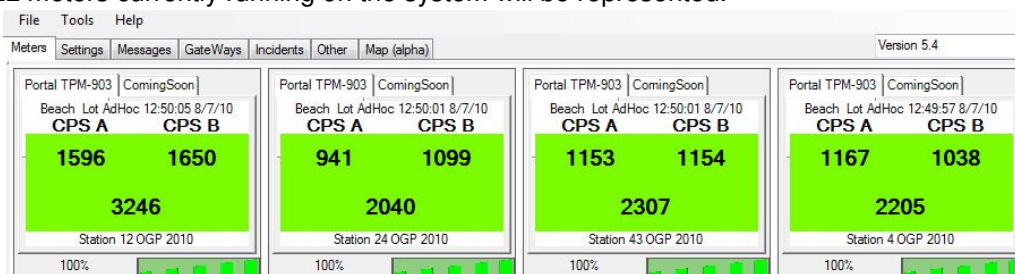


16.3 MultiMeterViewer Quick Start Guide

Double click on “MultiMeterViewer” Icon on desktop.



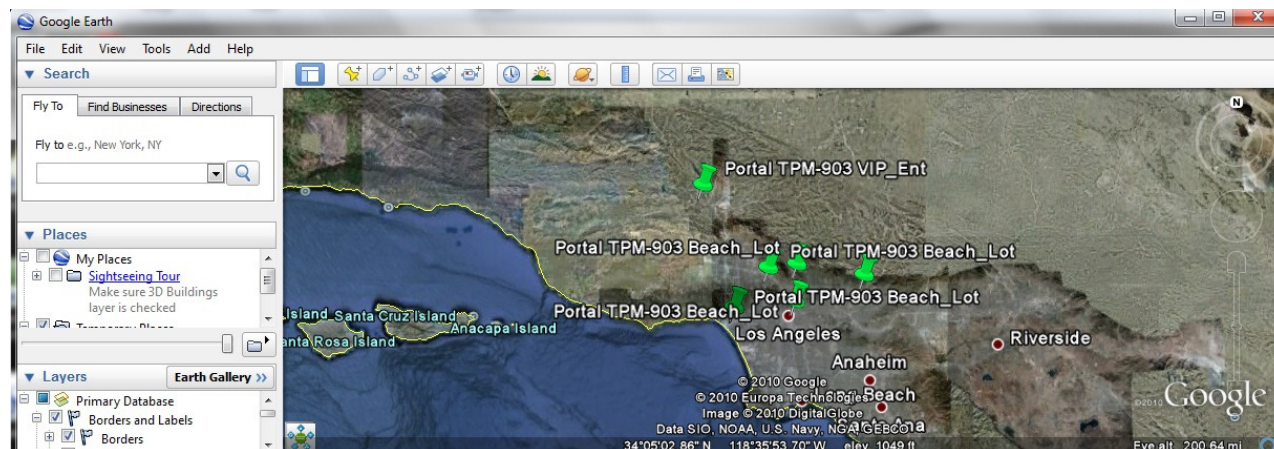
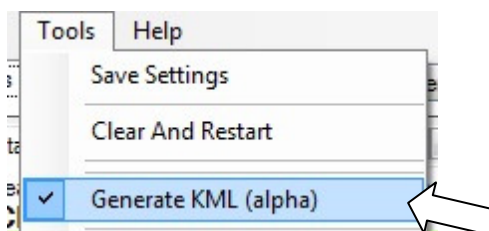
The safe environment LOGO will appear briefly.
The multi-meter viewing screen will appear within about 5-15 secs.
The readings will turn **green**, and data will populate the meter readings.
ALL meters currently running on the system will be represented.



Google Earth® Maps will activate automatically within about 1 minute, and will rotate to the location of the activated meter readings.

NOTE:

Google Earth Maps will “refresh” periodically, and can become an annoyance if one is trying to manage the “Multi-Meter-Viewer” program. Once the Google Earth® Maps application has activated, and the sensors are displayed, go to the Multi-Meter-Viewer main screen, and select the “tools” tab. The bottom menu item is “Generate KML (alpha)”. If this is un-checked, the map will not refresh. Once changes have been made to the system, and it is desired to have active readings on Google Earth® Maps again, the “generate KML” (alpha) can be re-checked.





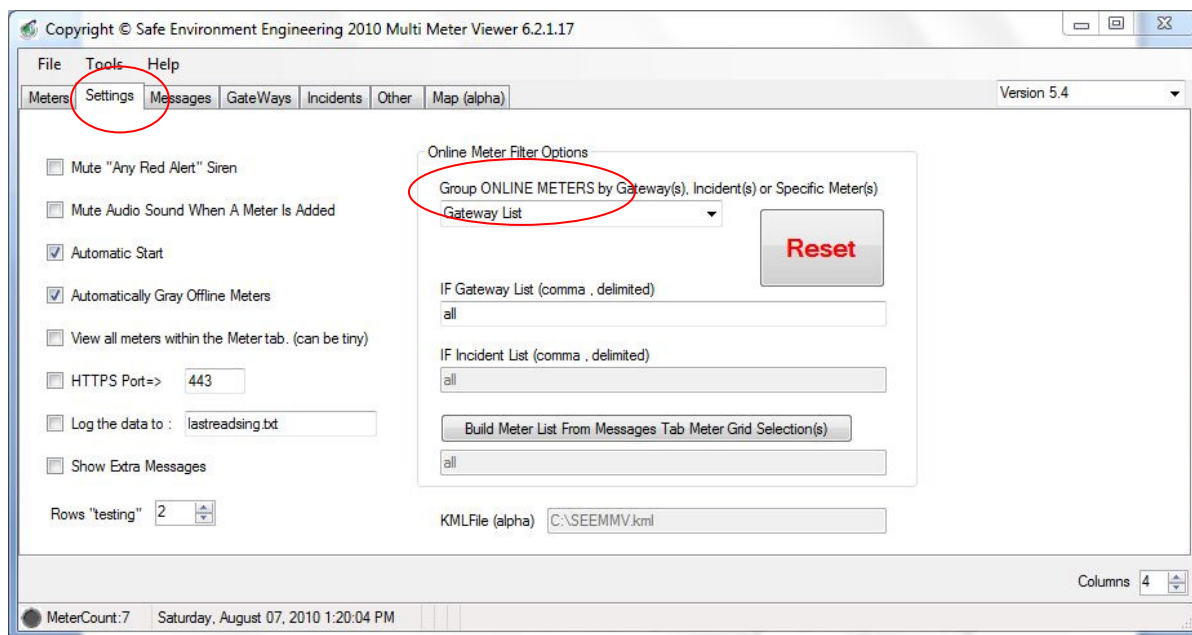
Filtering:

If filtering (limiting/increasing) the number of meters being viewed is desired, there are three (3) ways to limit the list of viewed meters to the user desired choices.

1. Open the “settings” tab.
2. Under the heading “Group ONLINE METERS by Gateway(s), Incident(s) or Specific Meters”, (adjacent to the **RED Reset** box), there are three choices within the pull-down menu.

NOTE: default setting is all meters from Gateway, Incident, or Specific Meter source(s).

By clicking the “**RESET**” button at any time, this clears/resets all previous settings and reverts the Meters viewer window to list **all** of the available online meters/sensors.



The first way to filter meters is: (refer to below graphic)

If a specific meter or a selection of meters is desired, go to the “Messages” tab and click/open. This will provide a complete list of the meters currently in communication with the server.

1. Move the cursor over the line for the desired meter to view, click once and highlight it. If additional meters need to be selected, hold down control key/button on keyboard while moving cursor over and highlighting additional desired meters to view.
2. Click on “Build Source List from Selected Meters” at bottom right hand side of the page.

NOTE: you must then click on the “Settings” tab and change the drop down under the heading “Group ONLINE METERS by Gateway(s) Incident(s) or Specific Meters” to “Meter Source List”

3. Go to the Tools Tab (top of page), open and select “Clear and Restart” The desired meter(s) will now be the only one(s) listed in the messages screen.
4. Finally, open the Meters Tab and the desired meters will be in the Multi-Meter viewing screen.



Copyright © Safe Environment Engineering 2010 Multi Meter Viewer 6.2.1.17

File Tools Help

Meters Settings Messages 1 s Incidents Other Map (alpha) Version 5.4

Meter List In DataGrid View

id	sent	meter	isRed	headline	Incident	meterStringUserID	batteryPercentage
1906	2010-08-07T13:4...	Portal TPM-903,L...	false	CPS Col A:1487;...	OGP 2010	Station 12	100
1907	2010-08-07T13:4...	Portal TPM-903,L...	false	CPS Col A:923;C...	OGP 2010	Station 24	100
1908	2010-08-07T13:4...	Portal TPM-903,L...	false	CPS Col A:1145;...	OGP 2010	Station 43	100
1909	2010-08-07T13:4...	Portal TPM-903,L...	false	CPS Col A:1162;...	OGP 2010	Station 4	100
1848	2010-07-21T18:5...	Portal TPM-903.5...	false	CPS Col A:939;C...	OGP 2010	Station 3	100
1849	2010-08-07T13:4...	Portal TPM-903.5...	false	CPS Col A:989;C...	OGP 2010	SafeEnv	0

2

3 Build Source List From Selected Meters (set data retrieval option to source to use)

☐ Scroll Messages Cut Into A Browser for Debug <http://seeicbme.net/caphandler/Handler.aspx?un=guest&pw=CE4DQ6B1b/BVMN9sc>

Last Readings Auto Start.
Attempting Start or Restart.
guest~CE4DQ6B1b/BVMN9scFyLiA==~gatewayreadings~all
gpsReader_evtReaderConnected: http://seeicbme.net/caphandler/Handler.aspx?un=guest&pw=CE4DQ6B1b/BVMN9scFyLiA==&cap=all&type=gatewayreadings~all
Running Normally...
Running Normally...

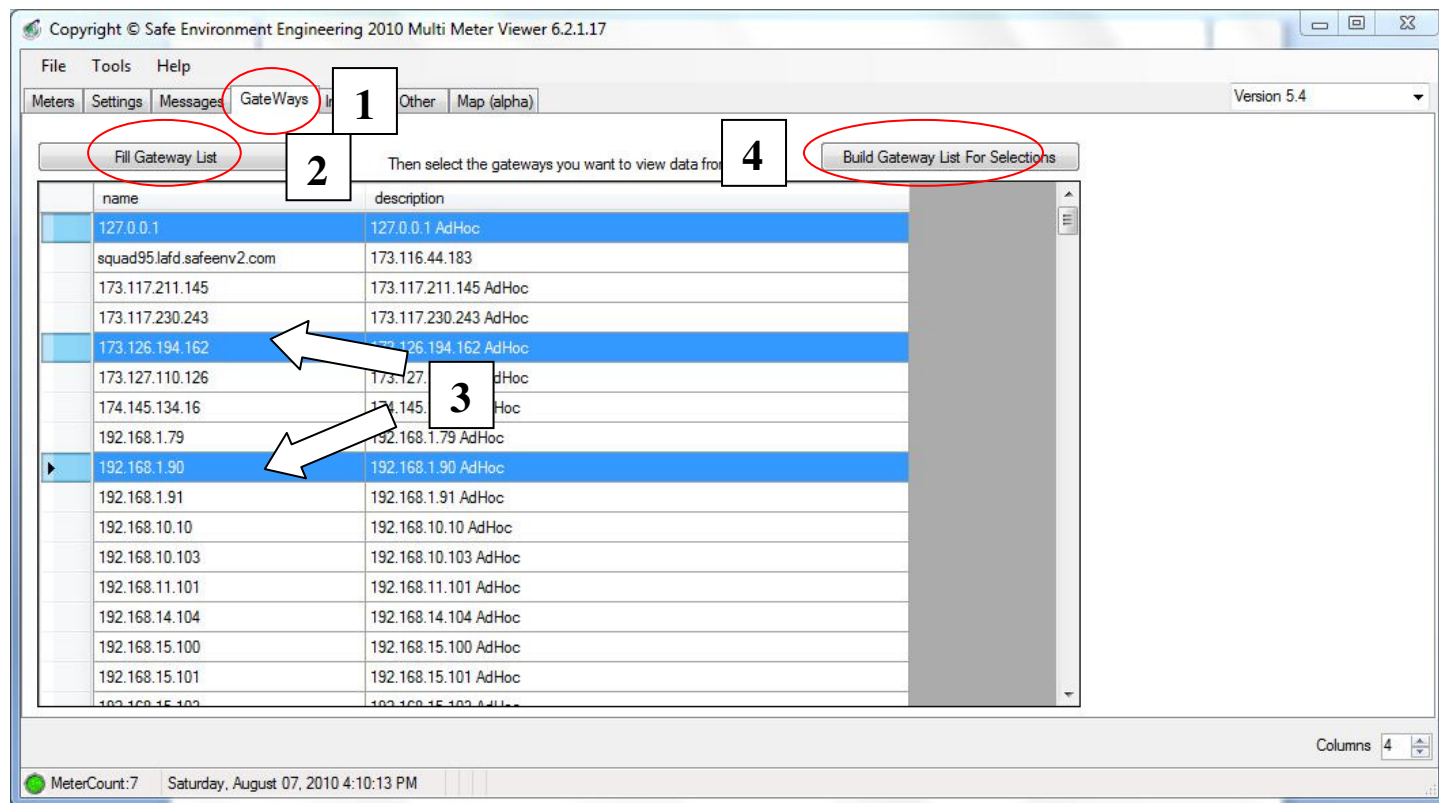
Columns 4

MeterCount:7 Saturday, August 07, 2010 1:53:58 PM

The second way to filter meters is: (refer to below graphic)

In the “settings” tab, select “**Gateway List**” from the “View Online Meters” menu pull-down. Gateways are the link between the meter output signal and the internet server connection. A gateway may service more than one meter at a time. Most HazMat response vehicles have 1 (one) gateway for several available meters or sensors.

1. Click/open “**GateWays**” tab
2. Single click the “Fill gateway list” tab. (This will bring up a complete list of the gateways that are a part of the Safe Environment Lifeline System).
3. Select the known/desired Gateway(s).
4. Click the “Build Gateway List for selection” tab.
5. Go to the tools tab, open and select “clear and restart”
6. Open the “Meters” tab, the meters running through the selected gateway(s) will be displayed in the Multi-Meter viewing screen.



The third way to filter meters is: (refer to below graphic)

The third way to select specific meters is to select by **"Incident"**. This format is dependent upon all participants at an incident assigning their instruments to the specific Named incident. Once this has been done,

1. In the settings tab, select **"Incident List"**.
2. Open the incidents tab, (to the right of the gateways tab).
3. Select fill incident list.
4. Select incident desired by highlighting, then click "build incident list"
5. Go to tools tab, open and select "clear and restart".
6. The desired meters will be in the Multi-Meter viewing screen.



Copyright © Safe Environment Engineering 2010 Multi Meter Viewer 6.2.1.17

File Tools Help

Meters Settings Messages GateWays Incidents 1 p (alpha) Version 5.4

2 Fill Incident List Then select the incidents you want to view data from. 4 Build Incident List From Selections

name	description
MyIncident	A meter was added without having an incident
1SEATAC	manual update of this description necessary
30;555;TANK 3;TEST;	manual update of this description necessary
30;TANK 3;	manual update of this description necessary
555;	update of this description necessary
Abcdefg Hijklnm Opqrst	update of this description necessary
big cat	manual update of this description necessary
chem pro test	manual update of this description necessary
Chemical Notification	manual update of this description necessary
ColdPizza	manual update of this description necessary
Convention Center	manual update of this description necessary
davetestincident	manual update of this description necessary
DHS RAD	manual update of this description necessary

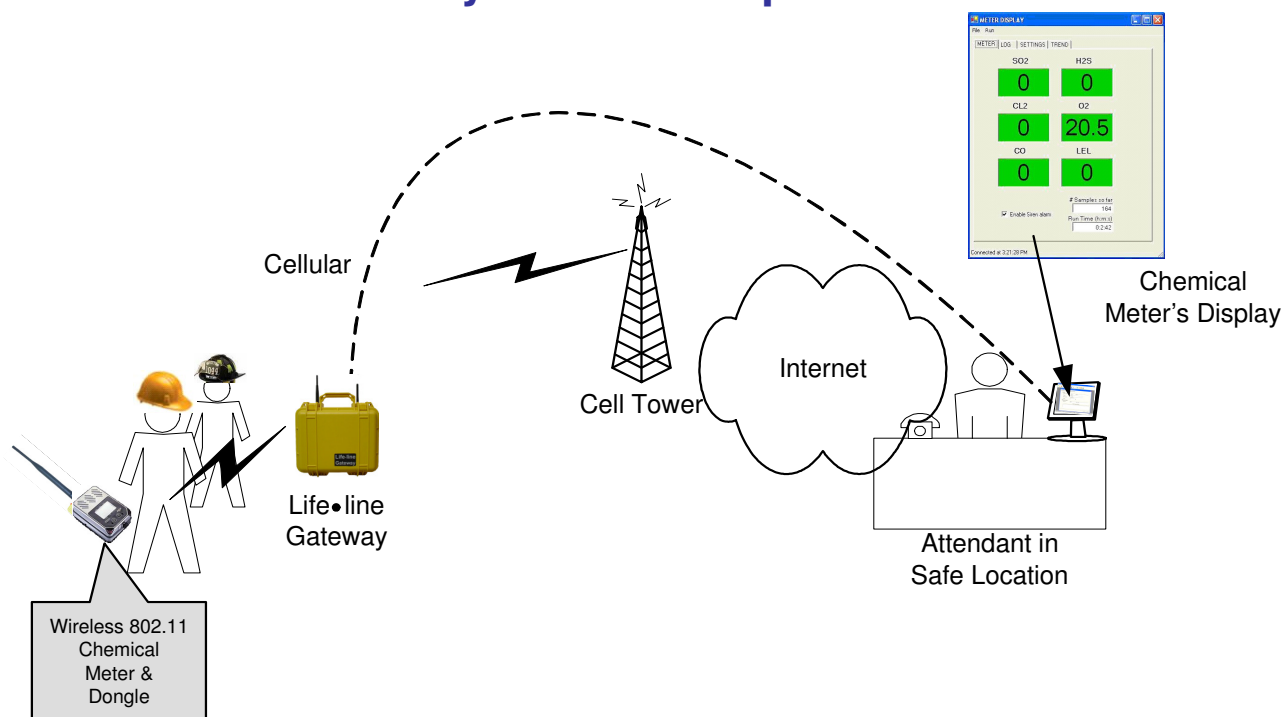
MeterCount:7 Saturday, August 07, 2010 4:58:16 PM Columns 4



16.4 Lifeline Gateway and LINC Operation



Life•line System Gateway and LINC Operation Manual



Safe Environment Engineering
28474 Westinghouse Place
Valencia, CA 91355
(661) 295-5500 • (661) 294-9246 Fax
www.safeenv.com • info@safeenv.com



1.0 Overview:

Management of hazards such as the release of chemical, radiological or biological agents requires timely information from sensors and detectors. Viewing meter readings while wearing Level A protection suits and gloves can be extremely cumbersome. The practice of transmitting readings by voice to incident command centers can be subject to security risks. Automatic wireless transmission of meter readings to incident command centers is a widely sought solution to these problems.

The solutions offered by Safe Environment Engineering provide a one stop total systems integration package for incident response agencies seeking the capability to communicate sensor data gathered on-site to an individual in an incident command center or anywhere in the world having an internet connection.

The Safe Environment Instrumentation Solution includes the following elements:

- Wireless data transmitters that can be physically attached to a variety of existing chemical, physiological or radiological sensors.
- Custom wired or infrared interconnections between the sensors and data transmitters that allow the capture of readings that appear on meter displays in a digital format.
- A wireless delivery system that can route data to any Internet connected computer.
- A software suite that remotely receives wireless data and includes real-time meter displays, settings for visible and audible alarms and charting components for visualizing trends.
- A variety of data sharing, alerting, visualization and messaging tools for data distribution among applications capable of using the Common Alerting Protocol (CAP).

The wireless software suite is built on a common operational platform (Microsoft .NET) that can be readily customized to provide archival data storage, data aggregation and data re-transmission. Sensor measurements can also be joined with GPS positional information and posted on map displays.

2.0 Installation:

The Lifeline Wireless Monitoring System application comes pre-installed on system computers, the Lifeline Interoperable Network Communicator (LINC) and Gateway. This configuration was designed to allow quick utilization of the system's capabilities.

2.1 Lifeline Gateway:

The Lifeline Gateway bridges the data acquired from a meter's medium distance Wi-Fi radio (LINC) through cellular to any computer having Internet access. The Lifeline Gateway is sealed and operates on fully charged batteries for at least 8 hours.



The Lifeline Gateway is also a local “Hot Spot” for wireless Wi-Fi equipped computers to gain access to the Internet for research or other library information.

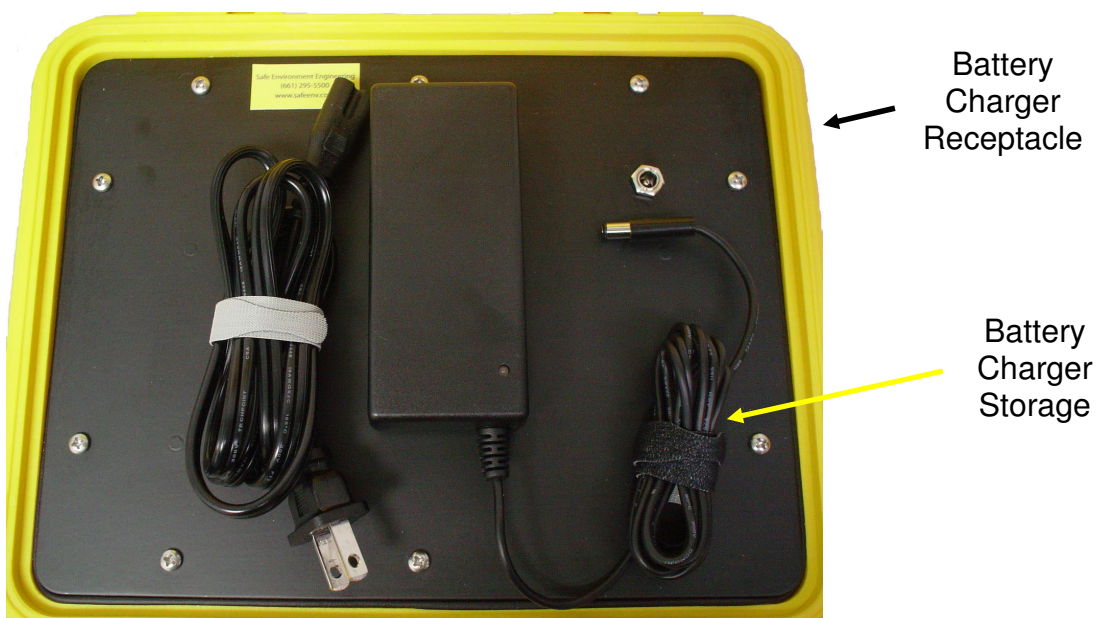


Lifeline Gateway



To turn on the Lifeline Gateway rotate antennas and toggle the power switch. An indicator on the power switch will glow green when the unit is on. The cellular and Wi-Fi indicators will turn on as soon as both networks are verified and operational.

Battery Charger





2.2 LINC Battery Installation:

Remove the 4 screws that hold on the LINC cover and insert a fully charge battery.

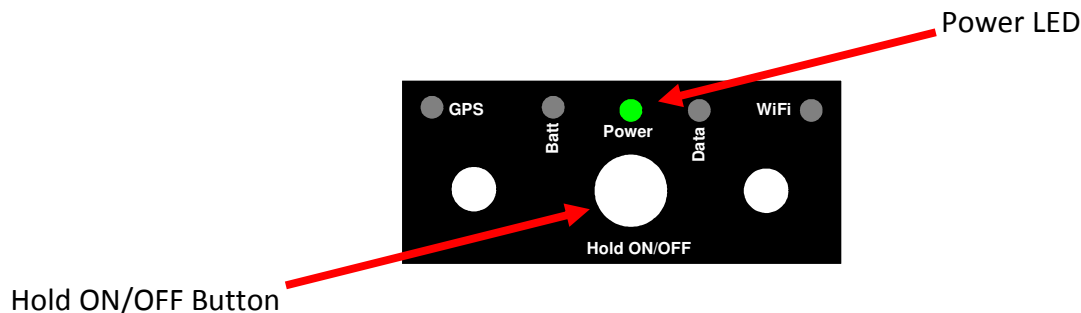


Install fully
charged battery



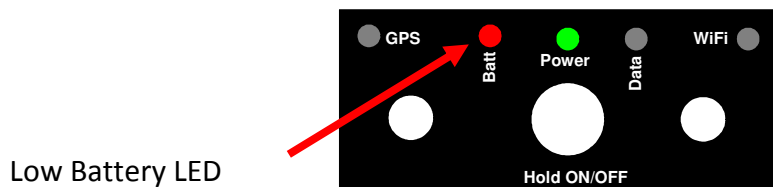
3.0 Turning On/Off the LINC:

Press and hold the Hold ON/OFF Button for 2 seconds until the Power LED illuminates green. Press and hold the Hold ON/OFF Button for 3 seconds to power off the LINC.



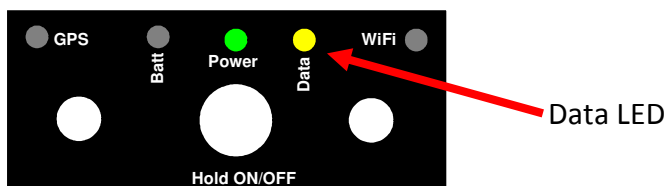
3.1 Low Battery Indicator:

A red Batt light indicates a low battery condition. The battery should be recharged or replaced.



3.2 Data Indicator:

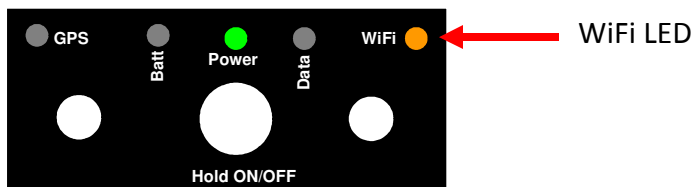
The yellow Data LED indicator lets the LINC user know that meter data is successfully getting back to the monitoring application.





3.3 WiFi Indicator:

The Orange WiFi LED indicator shows the status of the LINC's connection to a Lifeline Gateway or wireless local area network. If the LED is solid it indicated a connected condition if it is flashing it is not connected.



3.4 GPS Indicator:

The Blue GPS LED indicator provides confirmation of valid GPS acquisition.

