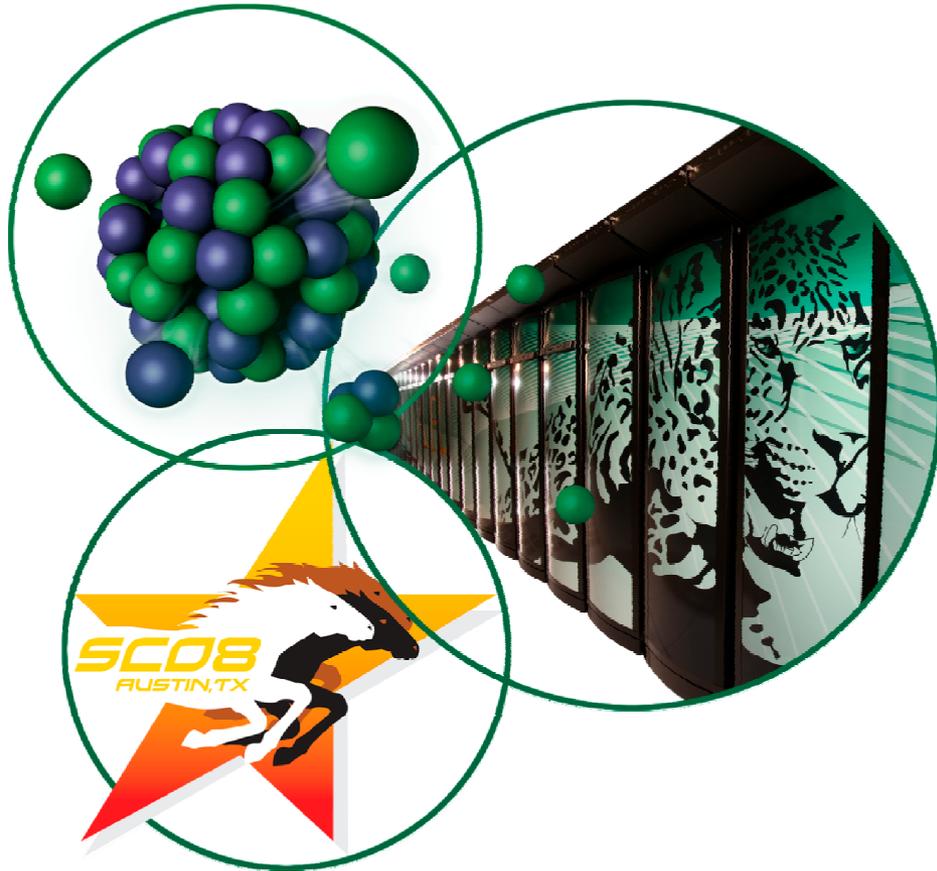


SensorNet: The New Science of Public Protection and Awareness

Presented by

Frank DeNap

SensorNet Program
Computational Sciences and
Engineering Division

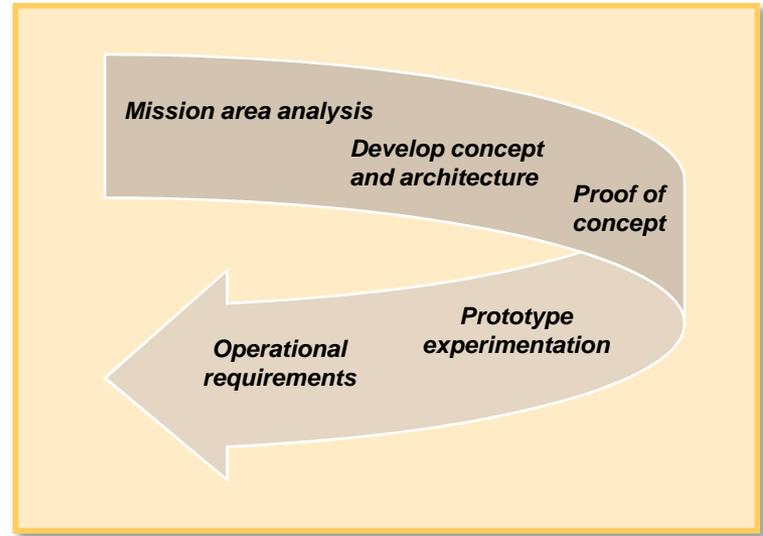


SensorNet

Collection ⇒ **Processing** ⇒ **Security** ⇒ **Dissemination** ⇒ **Knowledge generation**

Intelligent

- Collection
- Processing
- Security
- Dissemination
- Knowledge generation



Real world

- Politics
- Operational requirements
- Regulations
- Technology

Goal: Create an information-sharing and knowledge system in the Southeast, leveraging work from the SensorNet program

Sponsors:

DoD	SensorNet
DNDO	SETCP
DHS S&T	SERRI
DHS IP	Port of Memphis
TSA	SRRPP



SensorNet



SensorNet is ORNL's research in **sensor network interoperability, infrastructure, and application models**



SensorNet is an initiative that ORNL is undertaking with the Open Geospatial Consortium, NIST, IEEE, and others to **define the set of international and open standards for sensor network interoperability**



SensorNet is the **"middleware"** that ORNL is developing as a reference implementation of the SensorNet interoperability standards. This middleware **enables an adaptive, flexible, and pervasive "web"** to interconnect sensors, data, and applications. The development contributes to the SensorNet Implementation Guide

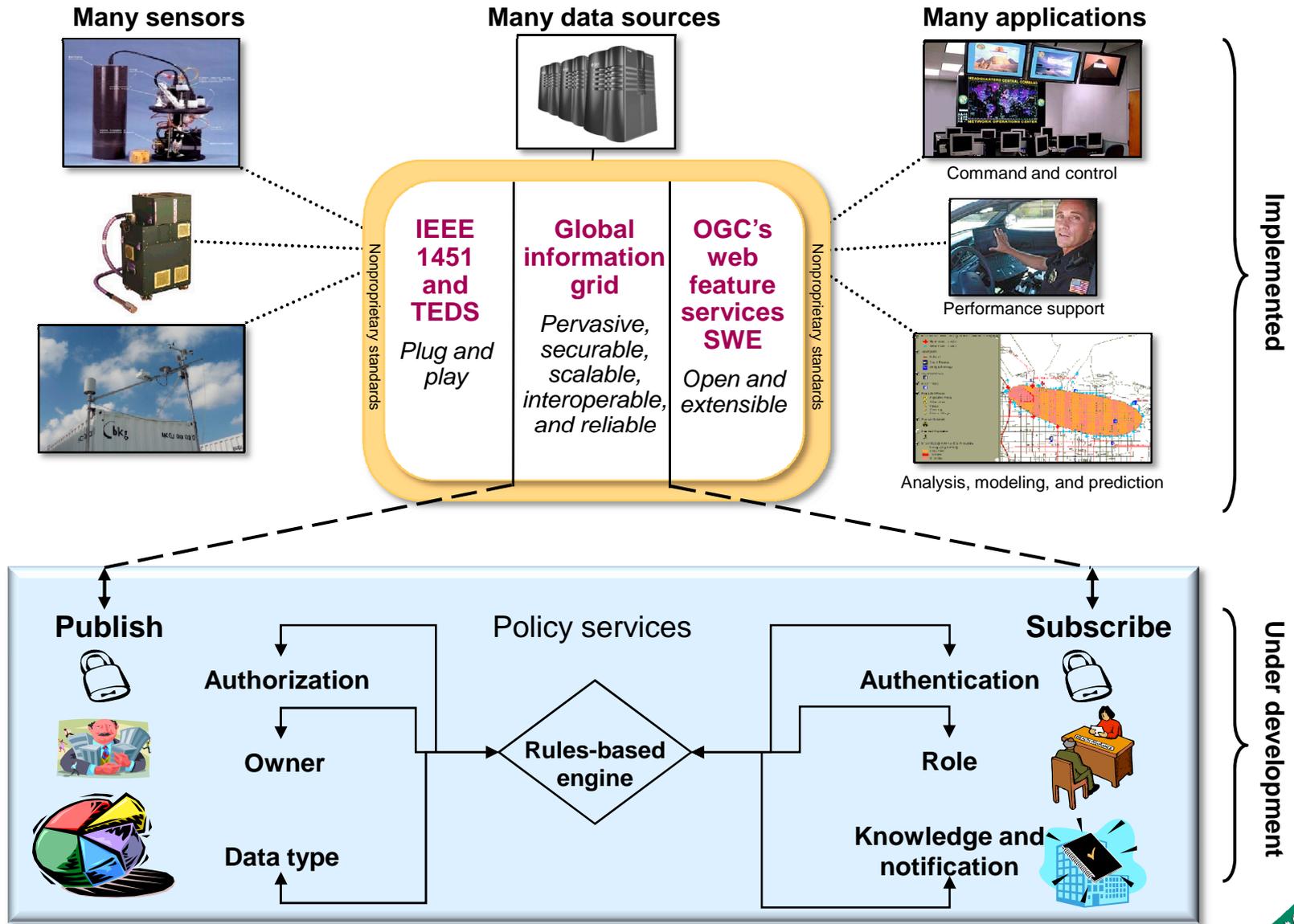


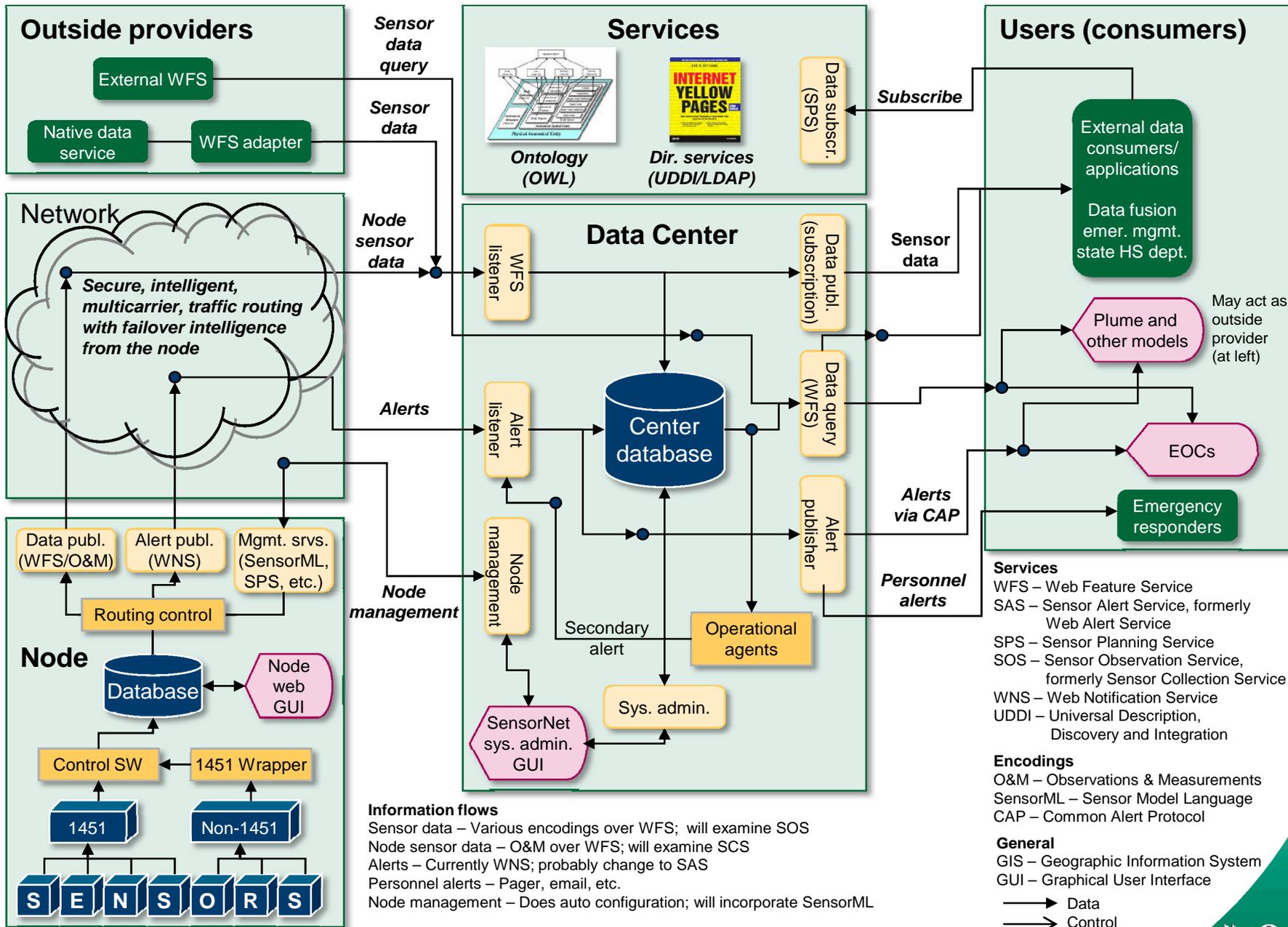
SensorNet is the **integration** of ORNL's middleware with commercial hardware, sensors, decision support software, communications, and databases to produce an **end-to-end system**



- SensorNet**
- Bragg experimental SensorNet test bed
 - Memphis operational SensorNet test bed
 - Snaps
 - Snaps commercial
 - Sniffer
 - Watt Road weigh station test bed
 - SETCP
 - SRRPP
 - Shelby County
 - KIFC
 - NOC

Interoperability-based design





SensorNet



OGF is an open community committed to driving the rapid evolution and adoption of applied distributed computing. Applied distributed computing is critical to developing new, innovative, and scalable applications and infrastructures that are essential to productivity in the enterprise and within the science community



OGC members are specifying interoperability interfaces and metadata encodings that enable real-time integration of heterogeneous sensor webs into the information infrastructure



TRUST, or Team for Research in Ubiquitous Secure Technology, is a science and technology center established by the National Science Foundation. TRUST brings together the top universities in security research, is devoted to the development of a new science and technology that will transform the ability of organizations (software vendors, operators, local and federal agencies) to design, build, and operate trustworthy information systems for our critical infrastructure



Developing a mobile sensor search algorithm comparing fixed versus mobile sensor deployment



Developing an efficient source-location algorithm with the minimum number of deployed sensors



Developing the technologies for tracking hazardous rail cargo, including information architecture and railcar monitoring devices

Evolution, test, and improve

From
Tennessee...



to SRRPP...

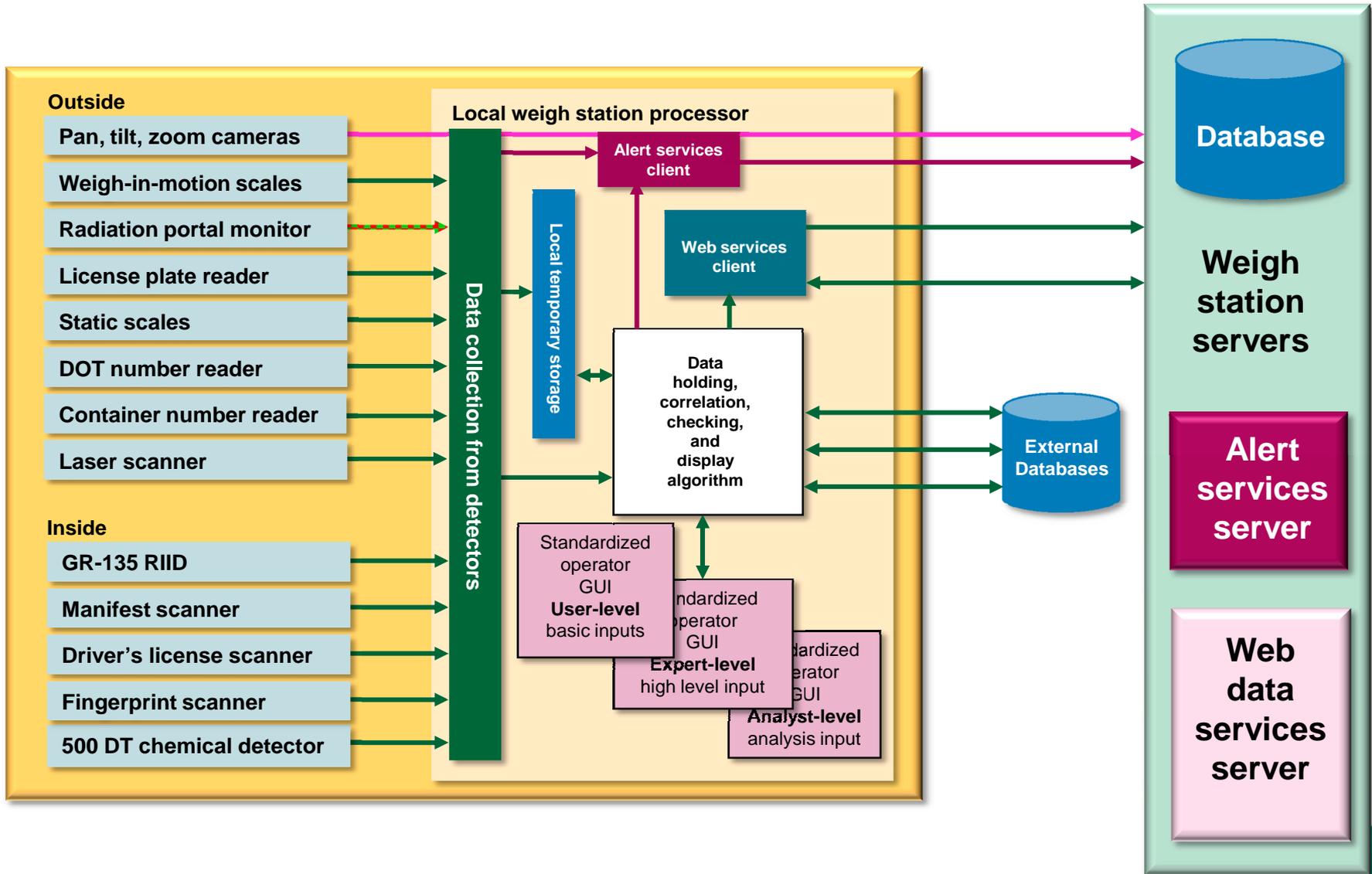


to SETCP...



to
Southern
Shield

Weigh station



Seahawk RAD/NUC detection program partners

- **DOJ/SEAHAWK**
 - Operational lead
 - Funded first vehicle-based and marine-based systems
- **South Carolina research authority/
Oak Ridge National Laboratory**
 - System integrators
 - RAD/NUC detection experts
- **DHS office of grants and training/TSA**
 - Funded system development through grant with SCRA
- **DHS/domestic nuclear detection office**
 - Provided training support
 - Participated in technical advisory board
 - SE transportation corridor pilot



**Homeland
Security**

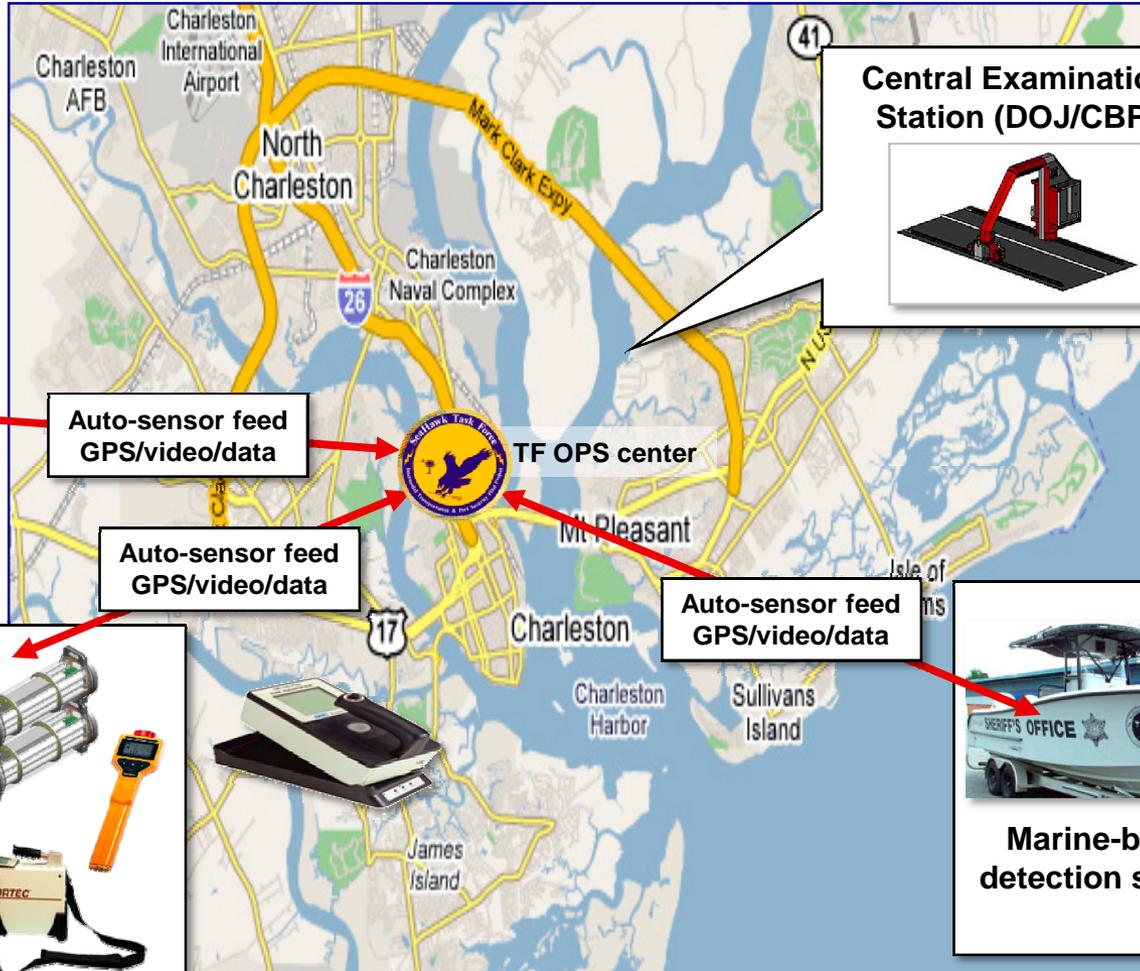
RAD/NUC detection architecture

Fixed detector array (CBP)

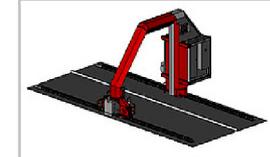


Other mobile equipment

900 MHz/EVDO wireless network



Central Examination Station (DOJ/CBP)



Auto-sensor feed
GPS/video/data

Auto-sensor feed
GPS/video/data

Auto-sensor feed
GPS/video/data

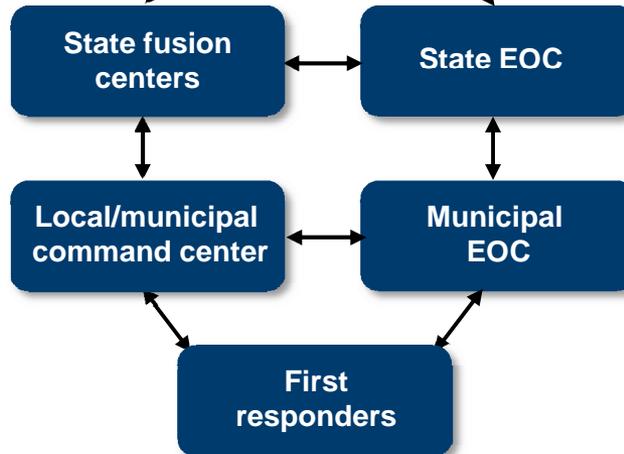
Vehicle-based detection system

Marine-based detection system

Information sharing and knowledge discovery



Leverage: NOC (DHS S&T)



Leverage: SETCP (DNDO)
Kentucky weigh stations (DHS grant)

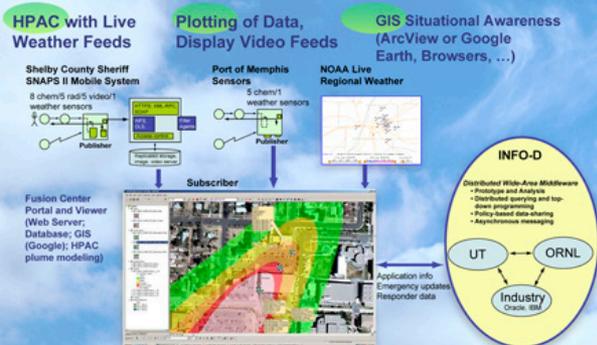


Memphis/Sherby County
Emergency Management Agency



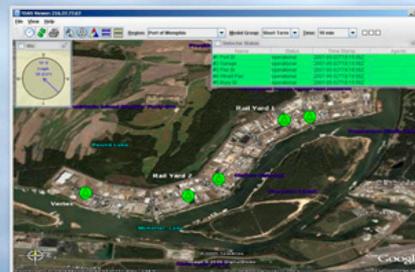
Leverage: Port of Memphis (DHS grant)
SNAPS (DHS grant)

SNAPS+POM NOAA_INFO-D



Port of Memphis

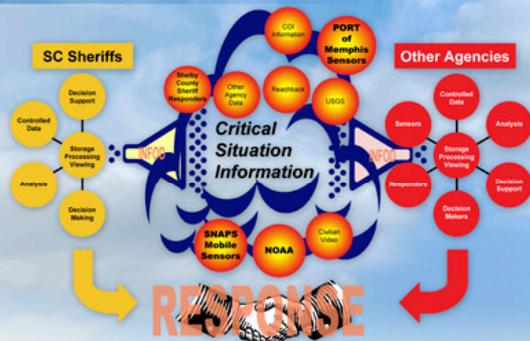
Fixed Chemical Detection



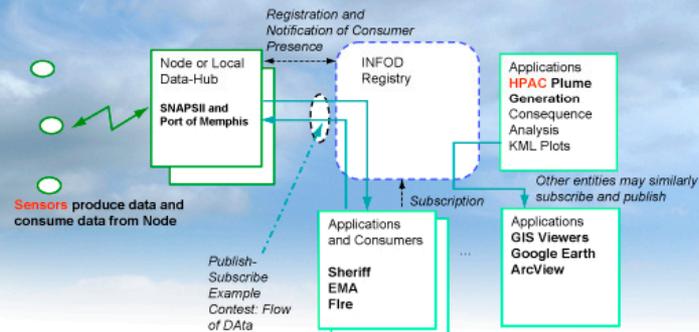
Plume Analysis



Sharing Near-Real-Time Information



INFOD Rapid Data Sharing



Registry matches sensor data publishers and application subscribers (and consumers)

SNAPS-Sensor Network Area Protection System Mobile Threat Detection System

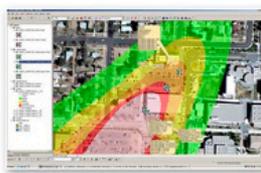
Mobile, re-configurable system components, rapidly deployed, Mobile SensorNet Operations Center



Wireless, GPS enabled sensors with battery operations. Sensors are 100% Mobile



Tower based "Auto-Eyes-On" from wireless video Slew to Sensor Alert



GIS auto-Plume at Alerts



GIS showing GPS locations of Sensors

Shelby County Fusion Center

Conclusions

- Rapid data transport to and from critical threat areas
- Pre-packaged data formats that are useful to consumers
- Ease of data integration from multiple sources into one portal
- GIS display of collective understanding
- Fully 'distilled' current 'threat-condition' information
- Seamless interface to secure data

Kentucky intelligence fusion center collaboration with NOC and other state fusion centers

- The Kentucky Information Fusion Center (KIFC) needs to share data and communicate with other state fusion centers as well as the National Operations Center (NOC) and Joint Analysis Center (JAC) in Washington, DC
- Data sharing services
 - HazMat data
 - Weigh station radiation data
 - Video streams
- Communication
 - Crisis management
 - Situational awareness
 - WebEOC
 - Collaboration tools
 - Computerized documentation of interaction
- The KIFC will have a map of the surrounding states with the location of the fusion centers for each state and NOC in Washington, DC indicated
- The icon representing the fusion center location will be color coded to represent the crisis status of the state or the communication status with that state
- The crisis status of the state will indicate the situation in that state
 - Normal operation (green)
 - Radiation situation (red)
 - Terrorist incident (blue)
 - Currently communicating (orange)



Contact

Frank DeNap

Computational Sciences and Engineering Division

(865) 576-8786

denapfa@ornl.gov