

# Research Alliance in Math and Science Faculty/Mentor Workshop

## **Cyber Security and Information Infrastructure Research**

**Robert K. Abercrombie**

**December 6, 2004**

# Cyber Security and Information Infrastructure Research

- **Focus**
  - Using various subject domains, conduct research on information infrastructures with emphasis on cyber security by:
    - Establishing a critical information infrastructure,
    - Collecting data and fusing it into information, and
    - Protecting the critical infrastructure.

*All while providing to our customers a product that they can only get from a National Lab, specifically ORNL.*

- **Examples**
  - IMR*ic*S (Identification and Monitoring of Radiation in commerce Shipments)
  - Weigh-in-Motion (WIM)
  - ICETECH (IAVA Compliance Enabling Technology)
  - Enterprise-Wide Distributed Zero-Day Attack Detection

# IMRics

*Identification and Monitoring of Radiation (in commerce) Shipments*

**Integrated Safety and Security Enforcement System  
for the 21st Century  
with  
Homeland Security Benefits**



Randy M. Walker,  
Robert K. Abercrombie, Ph.D.,  
Stephen G. Batsell, Ph.D.  
*Oak Ridge National Laboratory*

Vince Adams, Ph.D.,  
Richard W. Meehan  
*DOE - ORO*



# VISION

*Identification and Monitoring of Radiation (in commerce) Shipments*

**IMRiCS**

- **To increase the safety and security of the domestic transportation system by developing a vehicle monitoring system that will identify shipments not compliant with the following Federal and State regulations:**
  - **Transportation Safety,**
  - **Transportation Security,**
  - **Law Enforcement**
  - **Agricultural, and**
  - **Environmental**



# FOCUS

## State Enforcement “In Commerce” Issues

Identification and Monitoring of Radiation (in commerce) Shipments

IMRics





# **Weigh Stations are “accepted” *in commerce* Inspection Infrastructure**

Identification and Monitoring of Radiation (in commerce) Shipments

**IMRics**

## **Sensors Deployed *in commerce* infrastructure:**

- **Static Scales**
- **Weigh in Motion**
- **Weigh Station RFID Pre-Clearance Systems such as NORPASS and PrePass®**

## **Sensors DHS desires to Deploy include:**

- **Radiation Detection**
- **Chemical/Explosives Detection**
- **Optical Character Recognition**
- **Mobile/Deployable CBRNE Detection**



# Current Concept of Operations

*Identification and Monitoring of Radiation (in commerce) Shipments*

**IMRics**

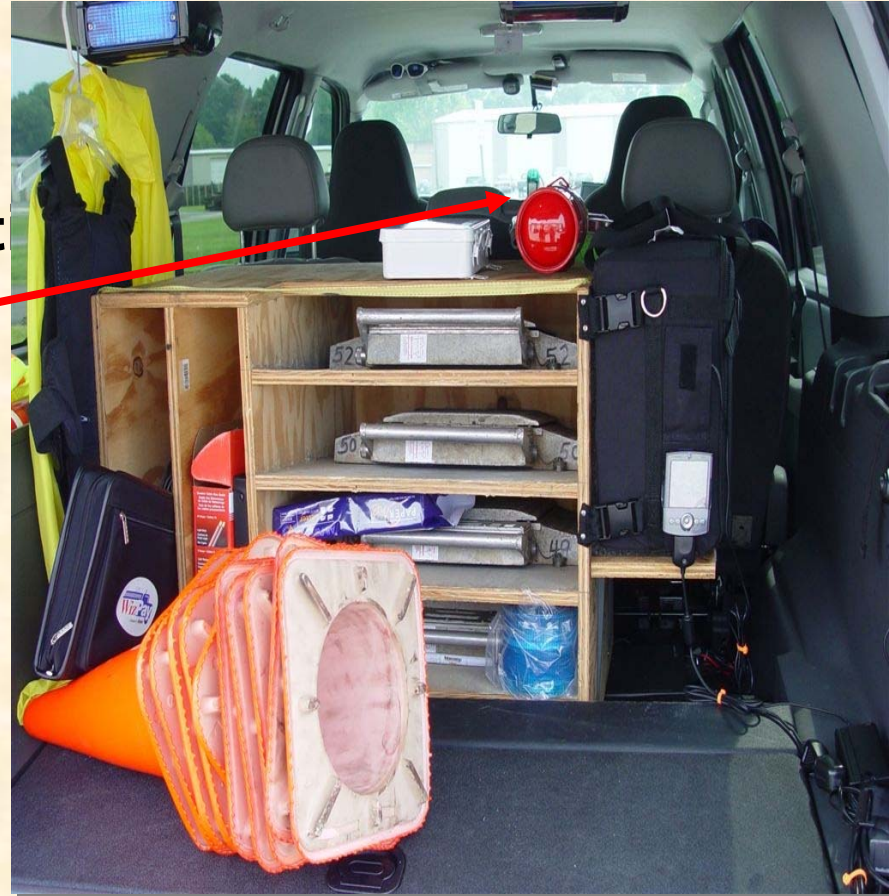
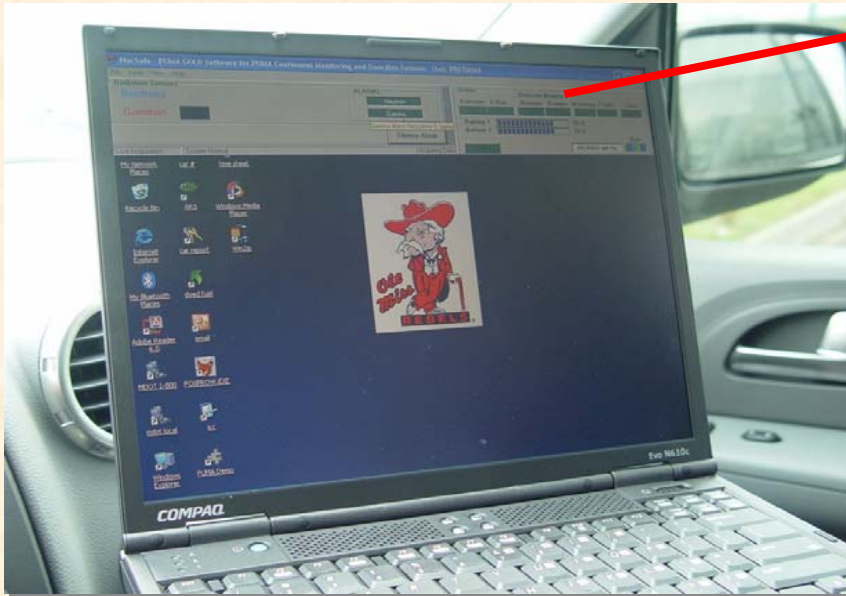
- **Sensors Deployed include Radiation, OCR, WIM, & Static Scale**
- **Alarms are set to Pickup cargo emitting radiation over background**
- **Police inspect alarms and collect shipping paper, sensor output & scale ticket data**
- **ORNL archives, secures and analyzes data**





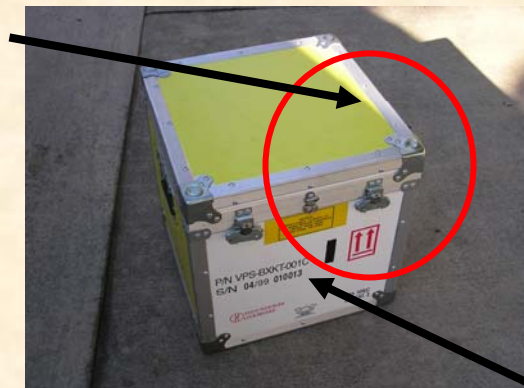
# Mobile Detection allows Constant Monitoring & Data Analysis for Police

- **Radiation Sensors in MDOT Vehicle**
- **SensorNet Enabled Connect**





# High Risk Commodity Packaging can be Identified and Monitored In Transit



**Radioactive  
Material  
Package RFID  
Equipped and  
Monitored**



# Expansion to other Modes of Transportation

- **Radiation Monitors installed in Inland Waterway Infrastructure**





# Monitoring of Barges and Personal Watercraft on the Tennessee River

- **Radiation Detectors in Watts Bar Dam Lock Doors**





# Components of Transportation Systems

Identification and Monitoring of Radiation (in commerce) Shipments

IMRics

Infrastructure • Operations • Vehicles •  
**IMRics** • Cargo • Enforcers •  
Transport Companies



# Cyber Security and Information Infrastructure Research

- Examples
  - IMR*i*cS (Identification and Monitoring of Radiation in commerce Shipments)
  - **Weigh-in-Motion (WIM)**
  - ICETECH (JAVA Compliance Enabling Technology)
  - Enterprise-Wide Distributed Zero-Day Attack Detection

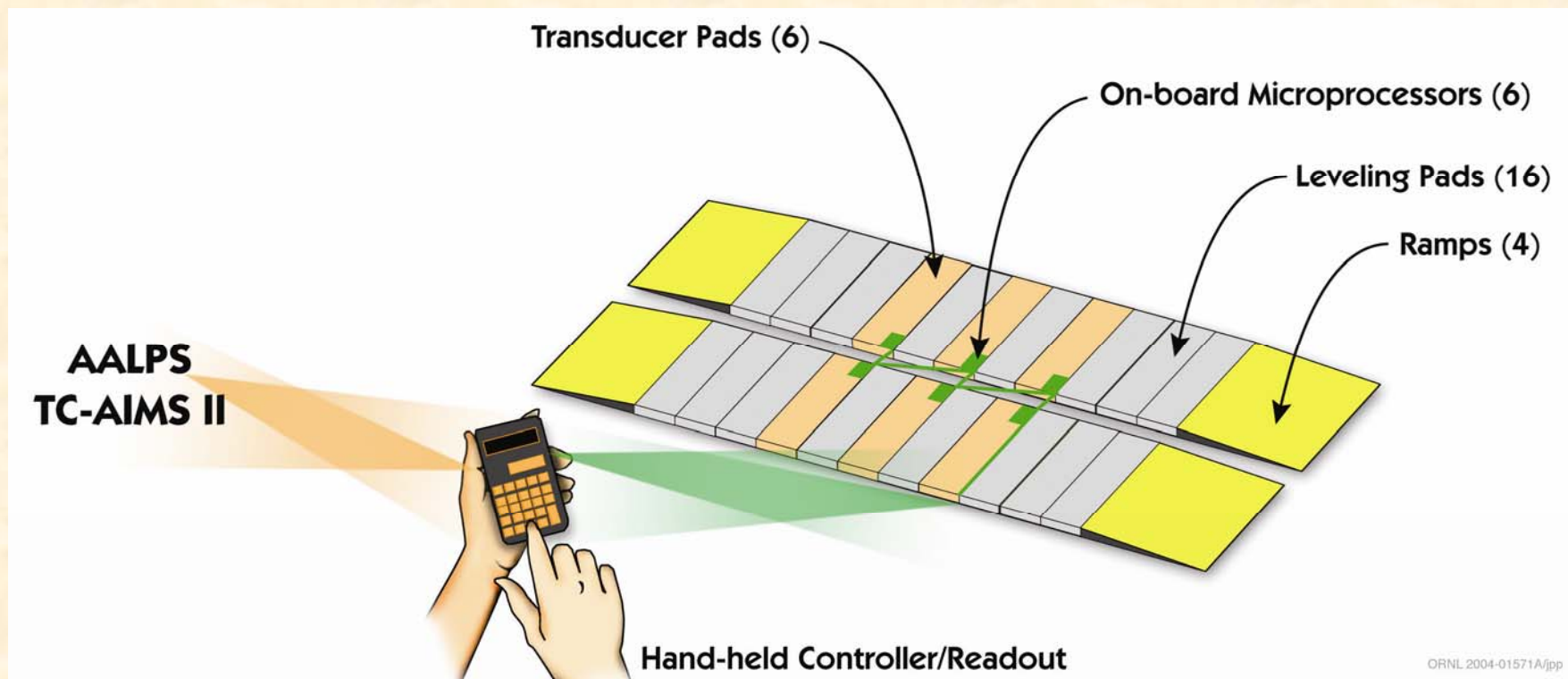




**5 Ton Truck Crossing WIM  
Demonstration at Ft. Bragg, NC**



# WIM Gen II Information Infrastructure Conceptual View



# WIM Process

- Retrieve Deployment Information
- Vehicle ID
- Weight & Balance
  - Dynamic/Static
  - Center of Balance
  - Actual Data processed
- Disseminate Actual Vehicle Information

OAK RIDGE NATIONAL LABORATORY  
U. S. DEPARTMENT OF ENERGY

## Logistics Transformation

ORNL is Developing the  
Next Generation Portable Weigh-In-Motion System (WIM)  
Enhancing the Defense Transportation System

The diagram illustrates the WIM process. A truck is shown on a scale. Arrows indicate the flow of information: from the truck to the left (planned weights), from the truck to the right (actual weights), and from the right back to the left (actual data processed). The truck is labeled 'WIM'.

Unit ID and Vehicle ID with planned weights via AIT:

- RFID
- MSL: 2D and/or 1D barcodes

Unit ID and Vehicle ID with actual weights:

- Weight (total)
- Individual axle
- Axle spacing
- Center of balance

Actual Weight and Center of Balance Data

TC-AIMS II (TIS)

AALPS

Updated Actual Movement Information

- Portable
- Fully automated—no operator error
- Wireless technology and load-planning
- Determines weight, center of balance, axle weight and spacing
- 500% productivity increase, save 40 minutes per plane
- Enhances safety of the vehicle/cargo weighing process and safety of deployments

Contacts: Robert K. Abercrombie, 865-241-6537, [abercrombie@ornl.gov](mailto:abercrombie@ornl.gov)  
D. L. Beshears, 865-576-0175, [beshearsdl@ornl.gov](mailto:beshearsdl@ornl.gov)

OAK RIDGE NATIONAL LABORATORY  
MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

ORNL P000-000077/mg





WIM provides the foundation to automate the monitoring of assets and their movement



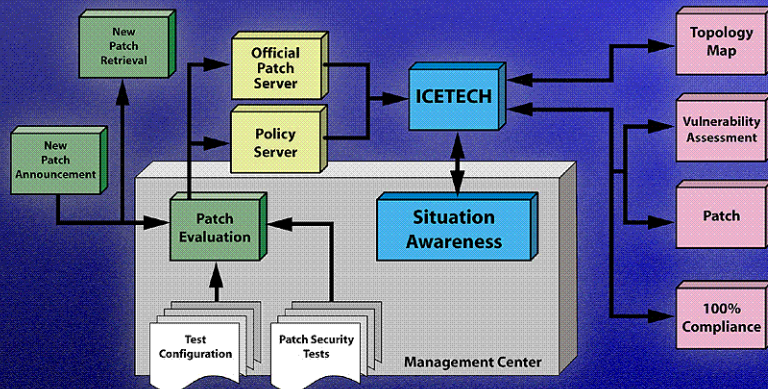
# Cyber Security and Information Infrastructure Research

- Examples
  - IMR*i*cS (Identification and Monitoring of Radiation in commerce Shipments)
  - Weigh-in-Motion (WIM)
  - **ICETECH (IAVA Compliance Enabling Technology)**
  - Enterprise-Wide Distributed Zero-Day Attack Detection

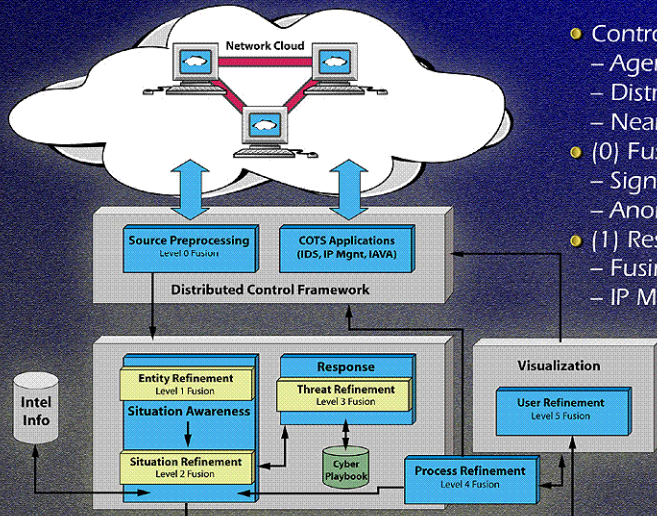


# IAVA Compliance Enabling Technology (ICETECH)

## ICETECH IAVA Concept of Operations



## Cyber Situational Awareness Architecture



- Control Framework
  - Agent Based
  - Distributed
  - Near Real Time Control
- (0) Fusion of Detections
  - Signature
  - Anomaly
- (1) Resource Mapping
  - Fusing Parallel Scans
  - IP Management
- (2) Spatial Fusion
  - Source Isolation
  - Meta fusion across Domains.
  - Fusion of Alternate data.
- (3) Predictive Modeling
  - L-M Engine
  - Predictive Emulation
- (4) Real-time Refinement
- (5) Visual Fusion
  - 3-D Gaming Engine

- **Goal:** Large Scale Situation Awareness and Information Assurance Vulnerability Assessment (IAVA).

- Teamed effort with EigenSoft.

- Tightly coupled agent framework to monitor and control network.

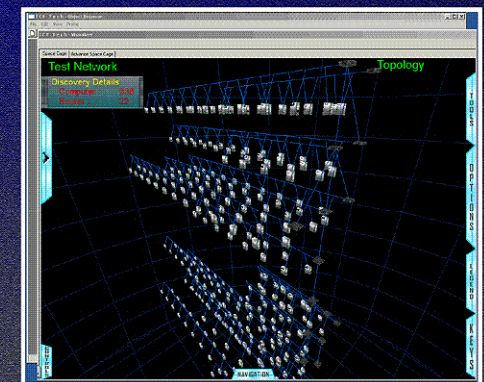
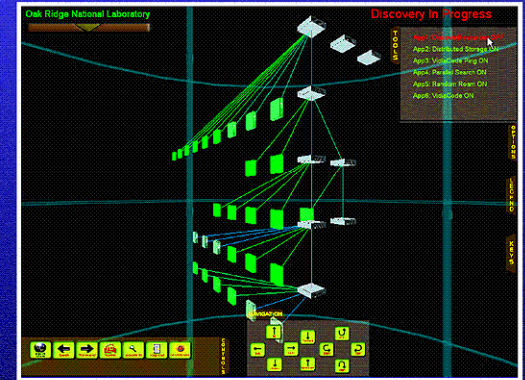
– Map the topology in near real-time including all hidden machines.

– Assess vulnerabilities.

– Patch vulnerabilities.

- **Current Sponsor:** Joint U. S. STRATCOM and DISA effort.

- **Demonstration Site:**  
U. S. Army Space Command,  
Colorado Springs, CO.



Real-Time Resource Discovery, 3-D Topology Mapping, Monitoring



OAK RIDGE NATIONAL LABORATORY

MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY





# Cyber Security and Information Infrastructure Research

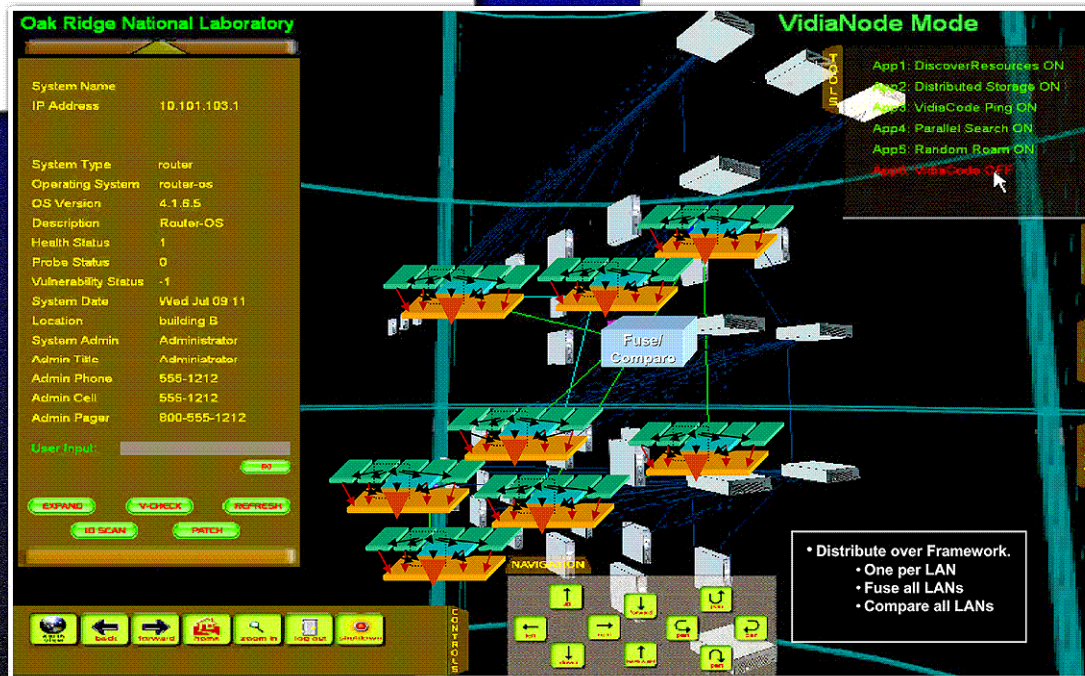
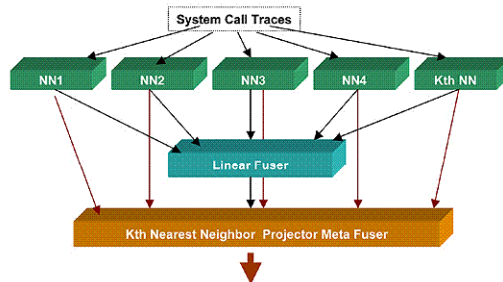
- Examples
  - IMR*ic*S (Identification and Monitoring of Radiation in commerce Shipments)
  - Weigh-in-Motion (WIM)
  - ICETECH (IAVA Compliance Enabling Technology)
  - **Enterprise-Wide Distributed Zero-Day Attack Detection**



# Enterprise-Wide Distributed Zero-Day Attack Detection

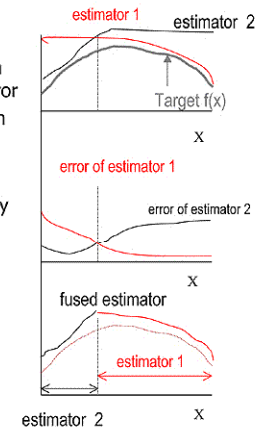
## Host System Call Monitor

- Anomaly Detector
- Monitors operation of each host.
  - NN- Neutral network
  - KNN- Kth Nearest Neighbor



## Illustration

- Optimal Fuser
  - Compute error regressions of information sources: project one with lowest local error
  - Fuser is better than best sub-combination
- Challenges:
  - In practice only finite measurements are given: error regressions cannot be exactly known
- Our results: **measurement-based approximation**
  - Cellular decomposition method
  - Nearest neighbor projective fuser



OAK RIDGE NATIONAL LABORATORY

MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

