INTELLIGENCE COMMUNITY
Center of Academic Excellence

Collaborative Governance

Antonia Boadi, Ph.D.
California State University Dominguez Hills
Department of Physics
DrToni@csudh.edu

International Council of Systems Engineering (INCOSE)
13 August 2019

Abstract

- The American homeland security enterprise was established eleven days after the September 11, 2011 terrorist attacks. The Department of Homeland Security (DHS) unified organizations from 22 federal agencies. In addition to responding to unprecedented technological challenges, DHS leadership has forged linkages between federal, state and regional entities, some of which had previously been prohibited from collaborating, or even sharing information.

- Collaborative governance is the ascendant paradigm in Public Administration and Public Policy. It aims to empower stakeholders with competing interests to arrive at a consensus and make recommendations regarding a policy or program. Dr. Boadi posits that collaborative governance processes can be enhanced through the application of Systems/Systems-of-Systems Engineering principles and methodologies.

Agenda

Establishment of Department of Homeland Security

Global Nuclear Detection Architecture (GNDA)

Application of SoSE/MBSE to GNDA

Case Study: Vulnerability of Small Vessels and Pleasure Harbors to Maritime Nuclear Terrorism

Questions


my
STUDENTS
are my
COLLABORATORS.
CSUDH.EDU/FutureStudents
California State University
DOMINGUEZ HILLS

Establishment of Department of Homeland Security

Homeland Security Enterprise

- Office of Homeland Security established 11 days after the terrorist events of September 11, 2001
  - Cabinet-level agency
  - unified 22 federal departments and agencies
  - oversaw and coordinated a comprehensive national strategy to safeguard the country against terrorism and respond to any future attacks
- Department of Homeland Security became standalone department in March 2003

Collaborative Governance
UNCG Collaborative Capacities Working Group (2012)

- process of establishing, steering, facilitating, operating, and monitoring cross-sector organizational arrangements to address public policy problems that cannot be easily addressed by a single organization or the public sector alone.
- stakeholders from different sectors engage in problem solving and decision-making
  - leverage and build on the unique attributes and resources of each stakeholder

The Nuclear and Radiological Threat

- Types of threats:
  - Nuclear Weapon
  - Improvised Nuclear Device (IND)
  - Radiological Dispersal Device (RDD) – (also referred to as “Dirty Bomb”)
  - Radiation Exposure Device (RED)

Crude sketch of nuclear device found in Afghanistan

HEU intercepted by Republic of Georgia in smuggling sting

Jose Padilla – convicted of plotting dirty bomb attack

RDD response exercise in New York

Sources of Radioactive Material*

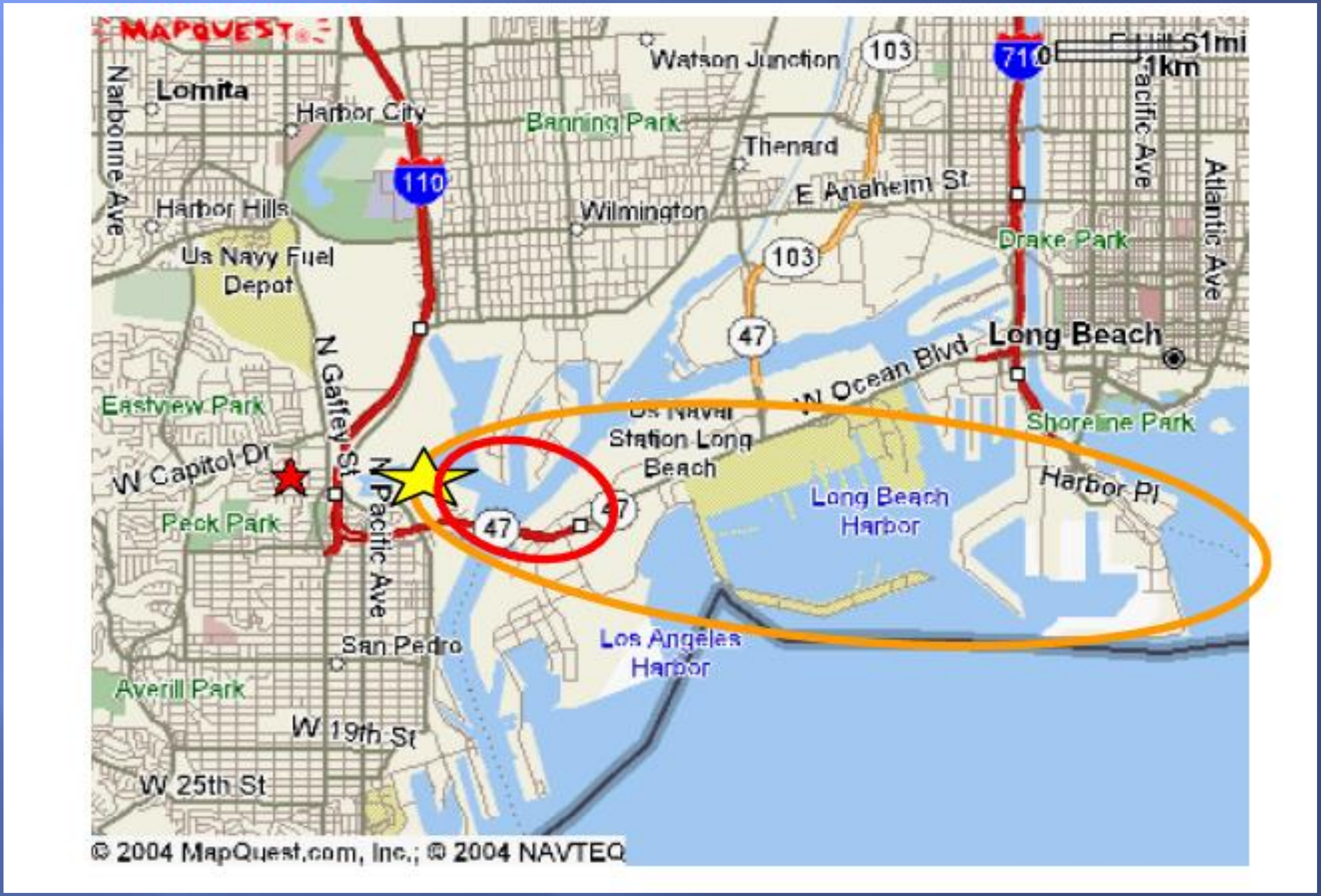
Source	Radioisotope	Radioactivity Level (curies)
Spent fuel assembly	Multiple sources	300,000 - 2,000,000
Industrial irradiator (sterilization & food preservation)	Cobalt 60 (Co 60)	Up to 4,000,000
	Cesium 137 (Cs 137)	Up to 3,000,000
Blood irradiator	Co 60	2,400 - 25,000
	Cs 137	50 - 15,000
Radiotherapy (single and multi-beam)	Co 60	4000 - 27,000
	Cs 137	500 - 13,500
Medical radiography	Co 60	1,000
	Iridium 192 (Ir 192)	1 - 200
Industrial radiography	Co 60	3 - 250
	Ir 192	3 - 250
Calibration	Co 60	20
	Cs 137	60
	Americium 241	10

Sources: Modified (1) Center for Nonproliferation Studies (CNS), The Four Faces of Nuclear Terrorism, 2005; (2) CNS, Commercial Radioactive Sources: Surveying the Security Risks, 2003; (3) IAEA, Categorization of Radioactive Sources, 2003; (4) Personal Communication with Tom Edmunds, Pacific Northwest National Laboratory, August 2004.

*Page 7, A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach
University of Southern California CREATE Center
Heather Rosoff and Detlof von Winterfeldt

Hypothetical Plume for a 10,000 Curie Release

*Page 23, A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach
University of Southern California CREATE Center
Heather Rosoff and Detlof von Winterfeldt



Hypothetical Plume for a 200,000 Curie Release

*Page 23, A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach
University of Southern California CREATE Center
Heather Rosoff and Detlof von Winterfeldt

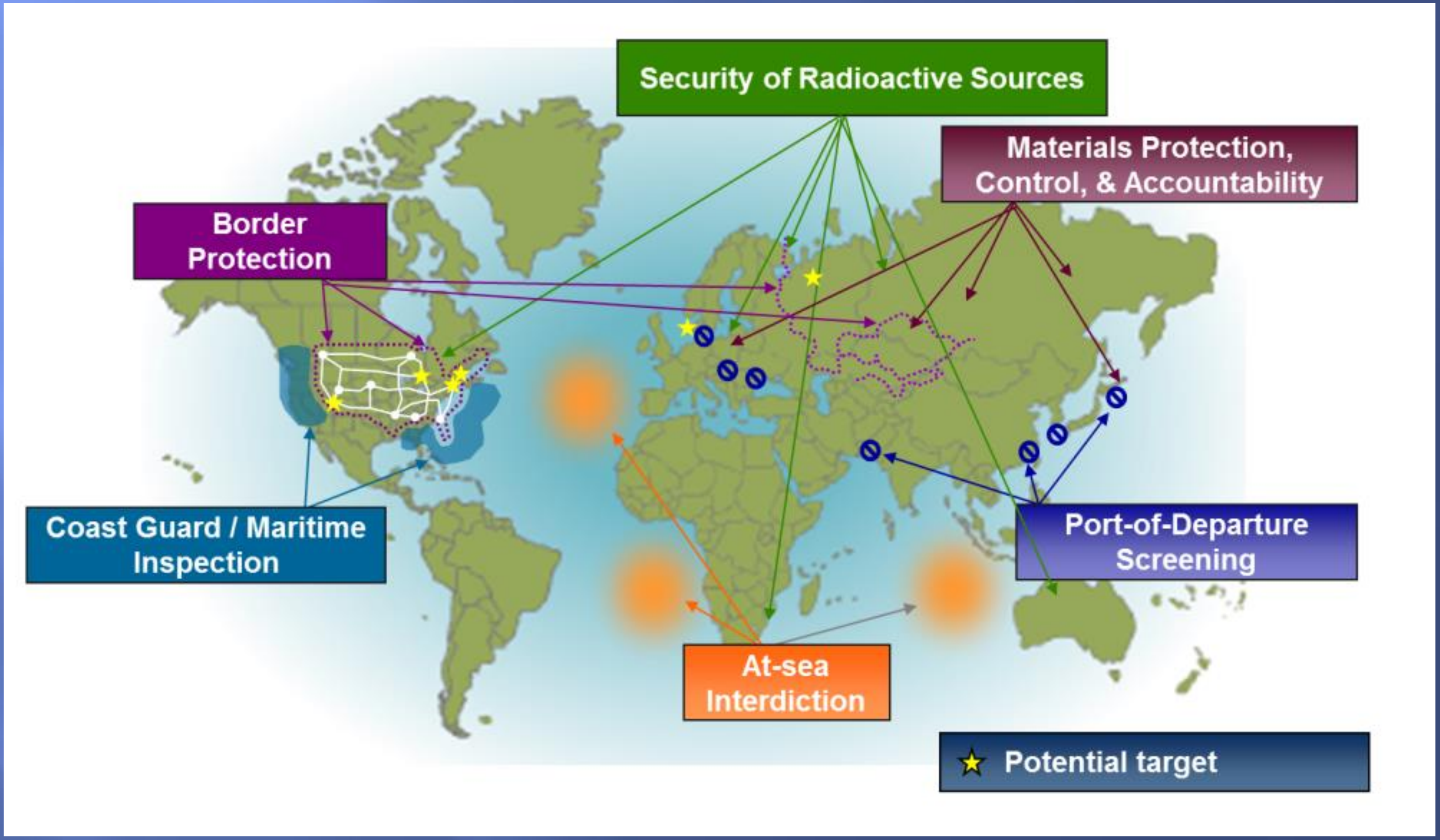
Estimates of Consequence Effects

*Page 21, A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach
University of Southern California CREATE Center
Heather Rosoff and Detlof von Winterfeldt

Consequences	10,000 Ci Release	200,000 Ci Release	Measure
Blast and Accute Radiation Effects	0-10	0-50	Fatalities
Latent Cancers	0-10	0-500	Fatalities
Port Shutdown and Related Business Losses	0-200 million	30-100 billion	Dollars
Evacuation Cost (Plume)	negligible	10-100 million	Dollars
Business Loss (Plume)	negligible	1-3 billion	Dollars
Property Values (Plume)	negligible	100-200 million	Dollars
Decontamination Costs (Plume)	10-100 million	1-100 billion	Dollars

Global Nuclear Detection Architecture (GNDA)

Global Nuclear Detection and Reporting Architecture



Coordinated by 74 federal departments from DHS, DoE, DoD State Department as well as partner nations

Preliminary Observations on the Domestic Nuclear Detection Office's Efforts to Develop a Global Nuclear Detection Architecture

GAO-08-999T

DHS, DoD, DoE, should develop a strategic plan to guide the development of a more comprehensive global nuclear detection architecture.

- The plan should:
  - (1) clearly define objectives to be accomplished
  - (2) identify the roles and responsibilities for meeting each objective,
  - (3) identify the funding necessary to achieve those objectives, and
  - (4) employ monitoring mechanisms to determine programmatic progress and identify needed improvements.

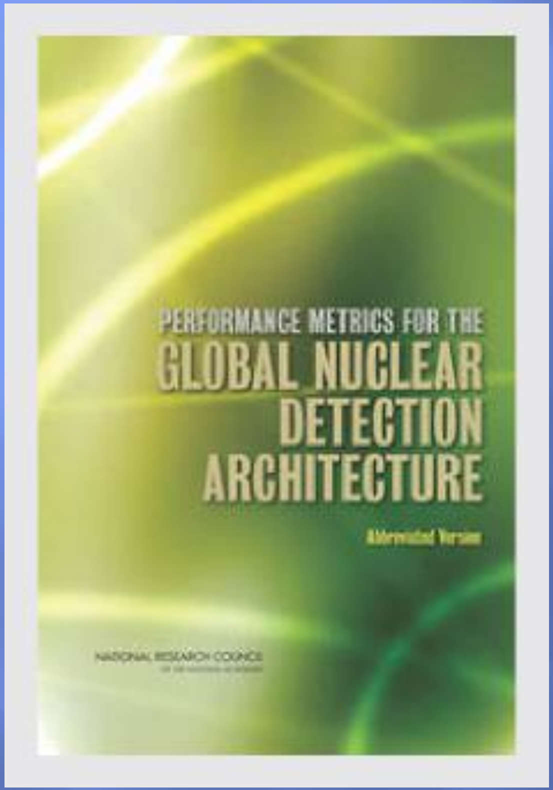
Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities

GAO-09-257

- DHS should:
  - develop a strategic plan for the domestic part of the global nuclear detection strategy to help ensure the future success of initiatives aimed at closing gaps and vulnerabilities.
  - develop criteria to assess the effectiveness, cost, and feasibility of the maritime radiological and nuclear pilot program.
    - establish time frames and costs for the three areas of recent focus--land border areas between ports of entry, aviation, and small maritime vessels.

GAO-10-883T: **DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps**

National Research Council (NRC)



National Research Council **2013**

Performance Metrics for the Global Nuclear Detection Architecture: Abbreviated Version. Washington, DC: The National Academies Press.

https://doi.org/10.17226/18424.

FINDINGS

- GNDA has no clear performance measures
- lack of a lead architect and centralized GNDA budget make it difficult for the GNDA to function as a system rather than a collection of programs.
- difficult to segregate actions and strategies focused on deterrence, detection, and reporting from other actions that support adjacent missions of federal agencies
- not feasible to develop outcome-based metrics against the existing strategic plan's goals, objectives, and performance goals because these components are primarily output- and process-based and are not linked directly to GNDA's mission

Current GNDA Capability	Future Capability
Port-centric detection strategy	Multi-layered detection strategy
Passive detection systems	Integrated passive/active systems
Fixed architecture	Fixed/mobile/relocatable architecture
Federal efforts	Federal/State/local efforts
Locally operated detectors	Networked detectors
U.S. focused strategy	Globally interconnected strategy
Targeted scanning	Comprehensive scanning
Primarily radioactive/nuclear detection	All signature detection

DHS Research and Development on Radiation Detection Technology Could Be Strengthened

GAO-15-263

- DNDO's documentation does not clearly describe how its process for planning and selecting R&D projects to fund aligns these investments with gaps in the GNDA.

Source: Oak Ridge National Laboratory (photo). | GAO-15-263

Prototype to detect and identify sources of illicit material traveling at normal speed over multiple lanes of traffic.

Source: InradOptics (photo). | GAO-15-263

Stilbene, a new material developed for detecting nuclear threats.

GAO Recommendations

- DNDO should develop a systematic approach for evaluating how the outcomes of its R&D projects collectively contribute to addressing research challenges
- DNDO should develop a research map and strategy

Cancelled Radiation Portal Monitor Program

The advanced spectroscopic portal monitor (ASP)--a next-generation radiation portal monitor (RPM) for screening trucks and cargo containers--did not pass field validation tests conducted in 2009 and 2010.


Source: GAO.


Source: GAO.

GAO Recommendations

To increase the probability of success for future acquisition programs, for cancelled acquisition programs:

- Make lessons learned reviews an institutional requirement
- Put documented processes in place to ensure that component agencies conduct timely lessons learned reviews.

Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries
GAO-06-311

- Secretary of State, working with the Secretaries of Defense and Energy and the Administrator of the National Nuclear Security Administration, should:
-
  - strengthen the Strategic Plan for Interagency Coordination of U.S. Government Nuclear Detection Assistance Overseas by including in the plan:
    - (1) specific performance measures to more effectively track and measure the progress U.S. programs are making toward achievement of interagency goals and objectives and
    - (2) overall cost estimates and projected time frames for completion of U.S. radiation detection equipment assistance efforts to determine the amount of U.S. government resources required to achieve interagency goals and objectives and under what time frames these resources will be required.
  - ensure continued maintenance of all radiation detection equipment provided to foreign governments, including all handheld equipment previously provided by State and other agencies.
  - account for all U.S.-funded radiation detection equipment provided to foreign governments, especially handheld equipment, by creating, maintaining, and sharing among all agencies a comprehensive list of such assistance.

NUCLEAR SECURITY
DOE Could Improve Aspects of Nuclear Security Reporting
GAO-17-239

- The Department of Energy's (DOE) and the National Nuclear Security Administration's (NNSA) annual reports:
  - did not fully meet the definition of quality information under the federal internal control standards.
  - did not always contain complete information on the assessments used to support the agencies' certifications that sites are secure and
  - were not provided to Congress in a timely manner
- **Recommendations**
- DOE should:
  - include more complete information in the reports
  - better align the review process and mandated deadlines
  - plan for infrastructure needs
  - inform Congress of the reason for delays in implementing its June 2011 order and any identified vulnerabilities

Application of SoSE /MBSE to GNDA

"The Department of Homeland Security should aggressively recruit professionals with DoD experience because of their expertise in guiding the development of complex systems."

The Honorable Bennie Thompson, Ranking Member,

House Homeland Security Committee

14 April 2014

Keynote Address presented at USC CREATE Center's 10th Anniversary Celebration

System of Systems

INCOSE

Systems of Systems Working Group

A set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities

Systems of Systems Engineering

The process of planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems into a system-of-systems capability that is greater than the sum of the capabilities of the constituent parts

Maier SoS Characterization

- Maier (1998) postulated five key characteristics of SoS:
  - Operational independence of component systems
  - Managerial independence of component systems
  - Geographical distribution
  - Evolutionary development processes
  - Emergent behavior

Differences Between Systems and SoS as They Apply to Systems Engineering

	Systems Engineering	Systems of Systems Engineering
Management & Oversight		
System	Physical engineering	Socio-technical management and engineering
Stakeholder Involvement	Clear set of stakeholders	Multiple levels of stakeholders with mixed and possibly competing interests
Governance	Aligned management and funding	Added levels of complexity due to management and funding for both SoS and systems; SoS does not have control over all constituent systems
Operational Focus (Goals)		
Operational Focus	Designed and developed to meet common objectives	Called upon to meet new SoS objectives using systems whose objectives may or may not align with the SoS objectives
Implementation		
Acquisition/Development	Aligned to established acquisition and development processes	Cross multiple system lifecycles across asynchronous acquisition and development efforts, involving legacy systems, developmental systems, and technology insertion
Process	Well-established	Learning and Adaptation
Test and Evaluation	Test and evaluation of the system is possible	Testing is more challenging due to systems' asynchronous life cycles and given the complexity of all the parts
Engineering & Design		
Boundaries and Interfaces	Focuses on boundaries and interfaces	Focus on identifying systems contributing to SoS objectives and enabling flow of data, control and functionality across the SoS while balancing needs of the systems OR focus on interactions between systems. Difficult to define system-of-interest
Performance and Behavior	Performance of the system to meet performance objectives	Performance across the SoS that satisfies SoS use capability needs while balancing needs of the systems
Metrics	Well defined (e.g., INCOSE handbook)	Difficult to define, agree, and quantify

From SEBoK 1.1

SoSI Complexity Drivers
(Madni/Sievers)

Acquisition

- multiple acquisition programs
- multiple systems’ life cycles across programs
- need to achieve interoperability among legacy and new systems

Structure changes dynamically as systems continue to enter/exit the SoS

Integration mechanisms require dynamic interoperability among constituent systems.

Verification and Validation (V&V)

- difficult to synchronize across multiple systems’ life cycles,
- dynamic entry/exit requirement for some of the SoS components,
- lack of defined behaviors or requirements for some operational environments

INCOSE MBSE Definition

"Model-based systems engineering (MBSE) is the *formalized application of modeling* to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases."

INCOSE SE Vision 2020 (INCOSE-TP-2004-004-02), Sept 2007

SoS Engineering Perspective
SoS MBSE Implications*

Legacy Systems	→	Models for behavior, interfaces, requirements, performance, e.g. SysML, Modelica, MARTE
Dynamic Reconfiguration of Architecture	→	Dynamic Reconfigurable models of architecture, e.g. UPDM with UML/SysML model version management
Service Oriented Architecture Enabler	→	SOA modeling language, e.g. SoaML, SOA Patterns
Protocols and Standards to Enable Interoperable Systems	→	Models for protocols, standards, interoperability, e.g. UPDM, DoDAF 2 MetaModel
Added "ilities" or Quality Attributes	→	Specialty Engineering models, e.g Assurance, RMAS
Federated Acquisition	→	Models for acquisition project synergy, e.g. UPDM, MODAF, DoDAF 2 MetaModel
Independent Systems	→	Models for independence in system functionality, e.g. Agent Based, federated models
Concept of Operations Critical	→	Models for CONOPs including Mission, Objectives, Courses of Action, etc. e.g. UPDM Operational Viewpoint, BPMN Business Processes
Ongoing Experimentation	→	Analysis of Alternatives models for all viewpoints and model versioning

*Ron Williamson, PhD Raytheon
INCOSE IW MBSE Workshop Breakout Session
INCOSE MBSE Wiki page: http://www.omgwiki.org/mbse
INCOSE MBSE SoS/Enterprise Modeling Wiki page: http://www.omgwiki.org/MBSE/doku.php?id=mbse:enterprise

MBSE & SoS Pain Points

(Ron Williamson, PhD Raytheon)

- SoS Management
  - Lack of SoS Authorities and Funding
  - Constituent Systems
  - Leadership
- SoS Technical Issues
  - Autonomy and Emergence
  - Capabilities and Requirements
  - Testing, Validation and Learning
  - SoS Principles

MBSE and SoS Management

Ron Williamson, PhD Raytheon

- Lack of SoS Authorities and Funding
  - Business Models
    - Top Down Command and Bottom Up Initiative
      - → Behavior models
  - Funding Models
    - Service Model, CrowdSourcing, Traditional
      - → Economic Models
- Constituent Systems Perspectives
  - Coordination and Management of Independent Systems
    - → Collaboration Models, Change Sensitivity Analysis Models
    - → Monte Carlo Based Emergence Models
- Leadership
  - Multiple Organizations
    - → Organizational Collaboration Models

MBSE & SoS Technical Issues

Ron Williamson, PhD Raytheon

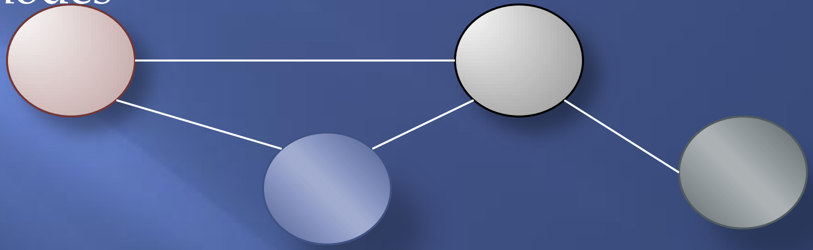
- Autonomy and Emergence
  - Expected behaviors based on combination of systems
    - → Monte Carlo Based Emergence Models, Constraint Models
    - → Interdependency Models (node-link analysis), Vulnerability/Fault Analysis Models
- Capabilities and Requirements
  - SoS Level and Traceability
    - → Capability, Function, Performance Models
    - → SoS Requirements Analysis Models
- Testing, Validation and Learning
  - Incremental, evolving
    - → Model based testing and validation
- SoS Principles
  - Processes, Examples, Workflow
    - → Process models, Model libraries, Behavior Models
    - → Visualization of SoS to detect anomalies

Generalized SoSE Approach

(Ron Williamson, PhD Raytheon)

- Start with an architecture addressing all the stakeholder viewpoints and concerns

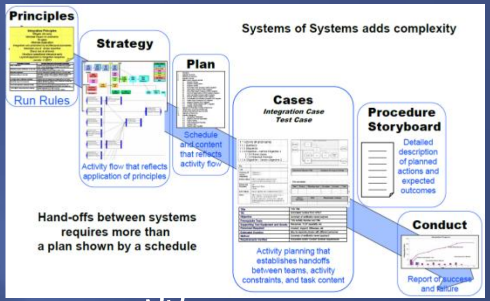
- Identify existing systems as nodes and assess interoperability and other quality attributes across nodes



- Design the “interoperability layer” or glue to enable inter node communications

- Integrate, Verify and Validate expected behaviors and quality & mitigate unexpected behaviors

vs.



Source: NDIA Test and Evaluation Conference Tutorial March 2012

Case Study: Vulnerability of Small Vessels and Pleasure Harbors to Maritime Terrorism

Post 9/11 Maritime Security Measures

- Maritime Transportation Security Act (MTSA) , or international agreements such as the International Maritime Organization (IMO) *International Ship and Port Facility Security* (ISPS) Code

- Focused on commercial shipping containers and ports
  - Limited oversight for vessels under 300 gross tons – recreational vehicles, fishing boats, speed boats, etc.

Small Vessel Threat

Terrorists, smugglers, and other criminals can use small vessels as platforms for their activities because small vessels are generally unregulated and largely anonymous

Coast Guard analysis states that small boats pose a greater threat than shipping containers for nuclear smuggling

Pleasure Harbors

Small vessels often dock adjacent to tourist attractions

- Amusement parks
- Novelty shopping areas
- Bicycle paths

Possible Threat Vectors

- Terrorist use of small vessels to transport or deliver weapons of mass destruction

- Conventional explosives delivery platform

  Terrorist groups have demonstrated a clear interest and ability to use small vessels to deliver waterborne improvised explosive devices (WBIED) in attacks against larger ships, as was the case in the attack on the USS COLE in 2000.

- Smuggling people and material

  Terrorists and criminal organizations might exploit small vessels to smuggle dangerous people and materials into the US

- Platform for weapon attack
  - Small vessels as platforms for standoff weapon (e.g., Man-Portable Air Defense Systems [MANPADS] or surface-to-surface missile platforms) attacks.

DHS Small Vessel Security Strategy (2008)

GAO-14-32: **DHS Could Benefit from Tracking Progress in Implementing the Small Vessel Security Strategy**

U.S. Department of Homeland Security
Domestic Nuclear Detection Office

Maritime Multi-Disciplinary Preventive Radiological/Nuclear Detection (PRND) Team

Description	A Maritime Multi-Disciplinary PRND Team is composed of maritime public safety personnel from various disciplines dedicated to the detection of RN material.				
Resource Category	Preventive Radiological/Nuclear Detection		**Resource Kind**	Team	
Overall Function	The team utilizes PRND tools and training to detect nuclear and radiological material out of regulatory control in the maritime environment. This team *may not be* capable of handling interdiction or other law enforcement PRND missions unless assigned sworn law enforcement personnel.		**Composition & Ordering Specifications**	May include sworn law enforcement, fire service, radiation health, EMS, or other appropriately trained personnel.	

Capability		**Type I**	**Type II**	**Type III**	**Type IV**	**Notes**
Component	**Metric / Measure**					
Team	Capabilities	Vessel borne wide area RN detection and isotope identification	Human-portable wide area RN detection and isotope identification	Limited area RN detection and isotope identification	Limited area RN detection	
Personnel	Team Composition	1- Coxswain 2-3- LE PRND Operators	1- Coxswain 2-3- LE PRND Operators	1- Coxswain 2-3- LE PRND Operators	1- Coxswain 2-3- LE PRND Operators	Operators should be familiar with maritime environment. Teams with a RIID must have at least one personnel trained for secondary screening.
Equipment	Vessel	1- Vessel	1- Vessel	1- Vessel	1- Vessel	
Equipment	Radiation Detection and Isotope Identification	4- Type II PRDs 1- Type I-III RIID 1- Type I-II Human-Portable Detector (Backpack) 1- Type I-IV Vehicle-Mounted Detection System	4- Type II PRDs 1- Type II-III RIID 1- Type I-II Human-Portable Detector (Backpack)	4- Type II PRDs 1- Type II-III RIID	4- Type II PRDs	Up to 1 extra PRD assigned for backup.
Equipment	Communication	Intra-team communications and ability to transmit spectra and other data to technical reachback.	Intra-team communications and ability to transmit spectra and other data to technical reachback.	Intra-team communications and ability to transmit spectra and other data to technical reachback.	Intra-team communications	Laptop/ aircard
Comments		Any teams operating with only PRDs should have established access to RIIDs to conduct secondary screening as needed.				
Reference(s)		EMAC Resource Request Checklist				

Securing the Cities (STC) Initiative

- In 2007 STC program initiated to reduce the risk of the deployment of a nuclear or radiological weapon by establishing capability in state and local agencies to detect and deter such threats
  - Funds PRND programs
- Los Angeles-Long Beach received STC funding in 2012; supports mobile detection capabilities

- GAO-19-327 identified limitations in STC program
  - STC requirement for sustainability not being tracked
  - DHS needs to
    - collect detailed information from cities on program expenditure
    - analyze risks related to sustainment
    - work with cities to address these risks
    - enforce sustainment-planning requirements

Addendum – Status of GAO Recommendations

GAO-08-999T : **Preliminary Observations on the Domestic Nuclear Detection Office's Efforts to Develop a Global Nuclear Detection Architecture**

- **Recommendation**
- Homeland Security, in coordination with the Secretary of Defense, the Secretary of Energy, and the Secretary of State, should develop a strategic plan to guide the development of a more comprehensive global nuclear detection architecture. Such a plan should (1) clearly define objectives to be accomplished, (2) identify the roles and responsibilities for meeting each objective, (3) identify the funding necessary to achieve those objectives, and (4) employ monitoring mechanisms to determine programmatic progress and identify needed improvements.
- **Agency Affected**: Department of Homeland Security
- Status: Closed https://www.gao.gov/products/GAO-08-999T

GAO-09-257: Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities

- Status of Recommendations: Closed and Implemented
  https://www.gao.gov/products/GAO-09-257

GAO-10-883 DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps

- This was testimony presented to Committee on Homeland Security and Governmental Affairs, U.S. Senate. As such there were no formal recommendations
- https://www.gao.gov/assets/130/124940.pdf

GAO-15-263
DHS Research and Development on Radiation Detection Technology Could Be Strengthened

- Recommendations closed and implemented
- https://www.gao.gov/products/GAO-15-263

GAO-13-256: **Lessons Learned from Cancelled Radiation Portal Monitor Program Could Help Future Acquisitions**

- Recommendations: Closed and implemented
- https://www.gao.gov/products/GAO-13-256

GAO-06-311: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries

- Recommendations: Closed and Implemented
- https://www.gao.gov/products/GAO-06-311

NUCLEAR SECURITY:
DOE Could Improve Aspects of Nuclear Security Reporting
GAO-17-239

- Recommendations: 1 recommendation closed and implemented; 3 recommendations still open

- https://www.gao.gov/products/GAO-17-239

Questions?

Thank You!!!!