Using Testbeds to Accelerate CBRN Readiness

Force Protection & Homeland Security

Complex systems require innovative testing

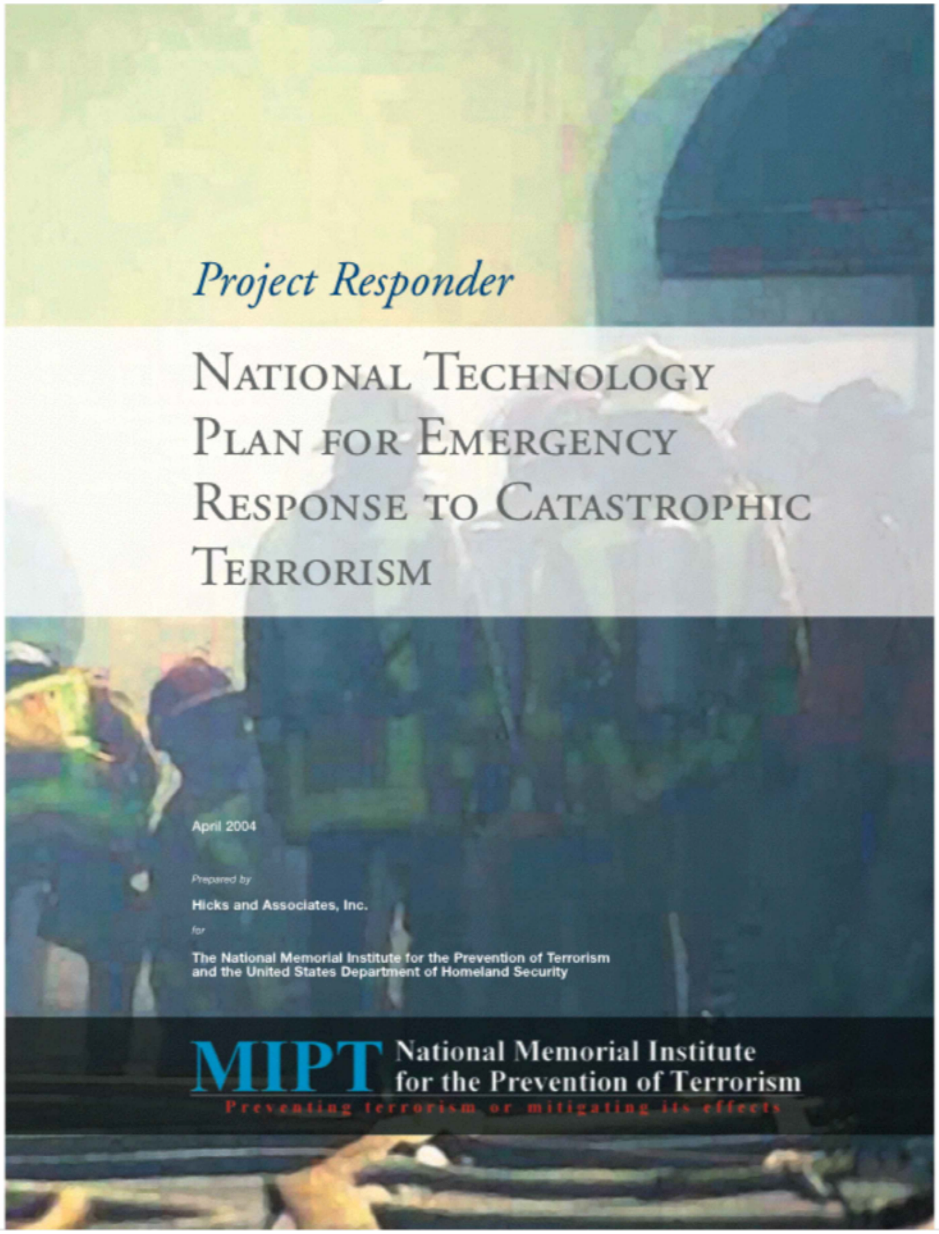
March 8, 2005

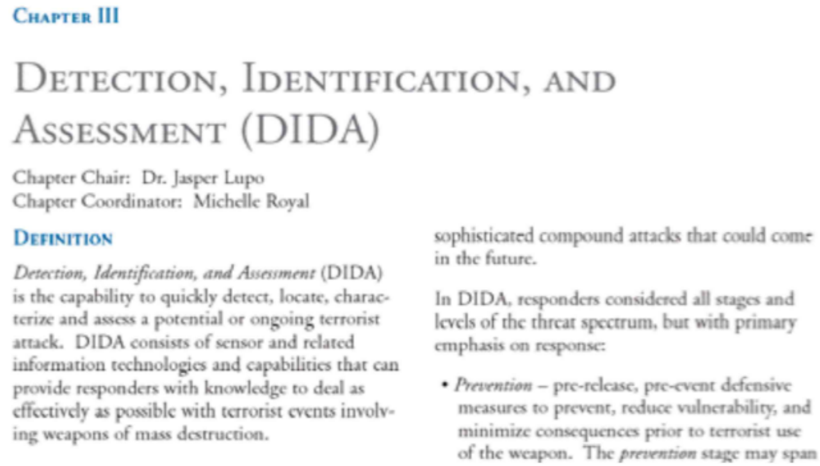
By: Dr. Jasper C. Lupo
Principal Scientist, Applied Research Associates
jlupo@ara.com

APPLIED RESEARCH ASSOCIATES, INC.
An Employee-Owned Company

Properties of Complex Systems for Force Protection & Homeland Security

- Systems of systems - examples: Guardian, Future Combat Systems
- Complex functions & interfaces
- Complex range of real-world scenarios
  - Wide range of environments - rural to urban, equatorial to near polar
  - Wide range of threats
  - Unpredictable human responses
  - Wide range of enemy attack options
- Variable CONOPS & threat levels





Chapter III

DETECTION, IDENTIFICATION, AND ASSESSMENT (DIDA)

Chapter Chair: Dr. Jasper Lupo
Chapter Coordinator: Michelle Royal

DEFINITION

Detection, Identification, and Assessment (DIDA) is the capability to quickly detect, locate, characterize and assess a potential or ongoing terrorist attack. DIDA consists of sensor and related information technologies and capabilities that can provide responders with knowledge to deal as effectively as possible with terrorist events involving weapons of mass destruction.

sophisticated compound attacks that could come in the future.

In DIDA, responders considered all stages and levels of the threat spectrum, but with primary emphasis on response:

- *Prevention* – pre-release, pre-event defensive measures to prevent, reduce vulnerability, and minimize consequences prior to terrorist use of the weapon. The *prevention* stage may span

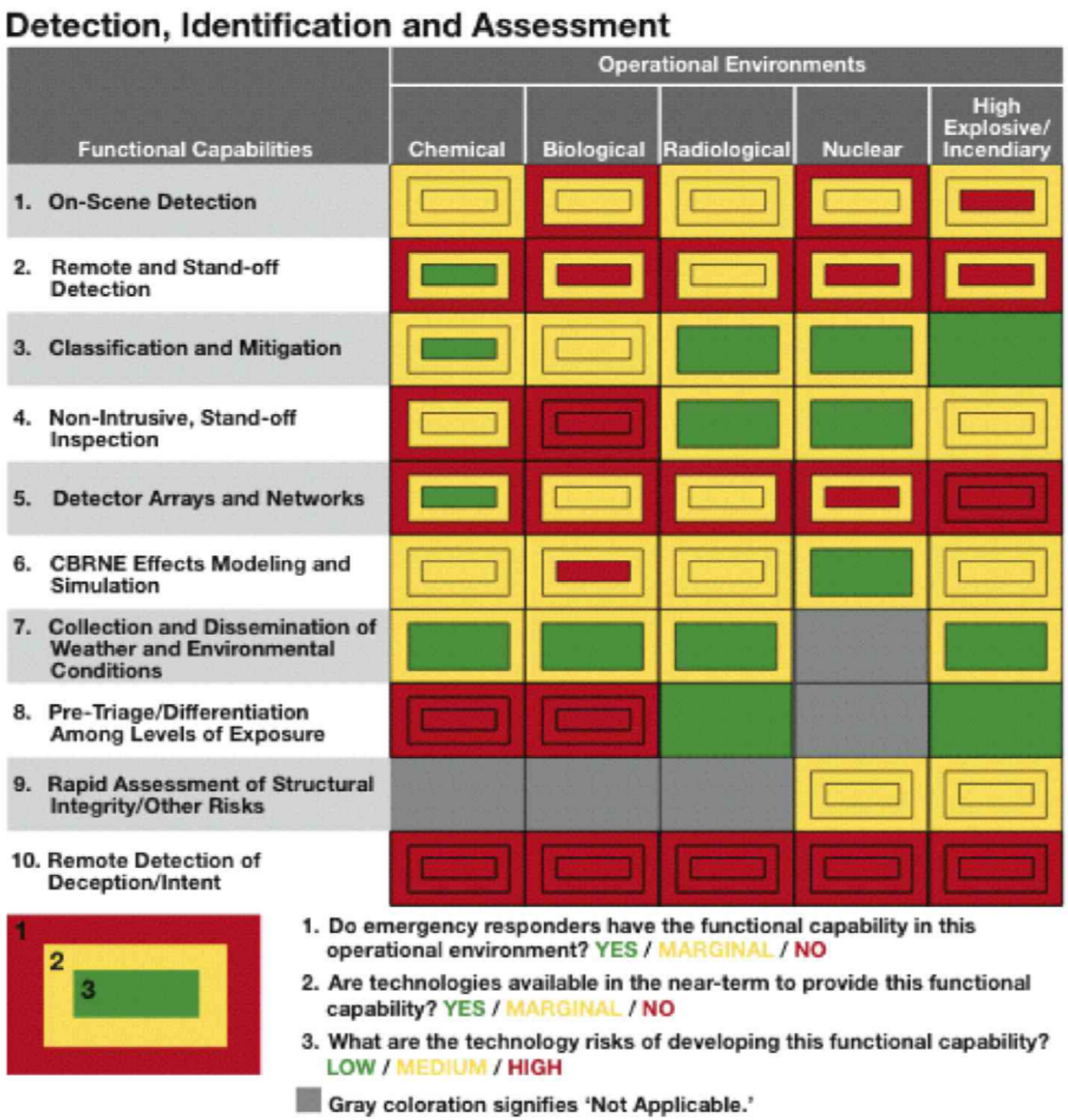
How complex is it?
Project Responder

- First Responders provided requirements
  - Multiple workshops
  - Scientists & Responders interacted to produce results
- 12 Chapters covering all aspects of detection, protection, prevention, response, & remediation

Project Responder:

Summary of detection technology readiness for 1st responders

Critical point: Wide range of threats, sensor technology, & level of maturity.

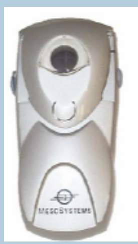


Example Layers of Bio-Defense Equipment & Users

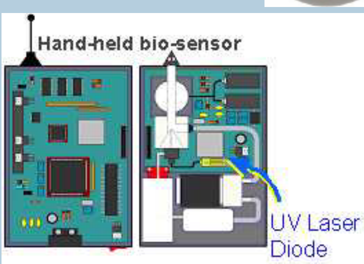
Layer 1: Manportable -
- GPS tracking of movers
- Wireless communications
- Field Processing Capability
- Response time ≥ .75 hr*

Layer 2: Vehicle portable -
- Automatic processing
- GPS tracking of movers
- Wireless alerts
- Response time ≥ 15 minutes*

Layer 3: Fixed location
- High throughput
- High confidence
- Response time ≥ 3 hrs*



Mesosytems Personal Sampler



DARPA Bioalert trigger (future option)

Research International SASS RAPTOR

Idaho Technology RAPID field portable PCR analysis kit

DFU or Rsch Intl SASS 3000

Applied Biosystems ABI 7900 HT high throughput, high sensitivity PCR

*Response times can be increased in low threat conditions

The Current Fielding Strategy

- Solution by parts & pieces
  - Focus on individual technology stovepipes - e.g. nuclear detectors
- Simplified scenarios & threats
- Heavy emphasis on testing at prepared sites - e.g. Yuma, Little Baghdad for IED
  - Controlled variables
  - Emulation of real scenarios
- Minimal attention to CONOPS & Force integration

Sensor centric approach:
Field ‘em if you got ‘em

Consider: Testing the Untestable

Problem 1 - Deception Detection

- Problem: find the hijacker at the airport
  - Proposed solution: remote detection of deception - lie detectors at 10 feet
  - Research - find the “golden signature” of deception
- How to test?
  - Current strategy - get cooperative test subjects to deceive in controlled environment
  - Develop ROC* curve prior to fielding
    - Question: is this realistic?
- How do you verify that emulated deception accurately represents real-world deception?
- Is validation costlier than the solution?

*Receiver operating characteristic - probability of detection vs false alarm rate

Consider: Testing the Untestable

Problem 2 - Nuclear Detection Network

- Problem: find the nuke in transit before it blows
  - Proposed solution: sensors & network
  - Research - Optimized network architecture
- How to test?
  - Current strategy - sensor testbeds
  - Data collections in urban environments
  - Develop sensor ROC* curve prior to fielding
  - Architecture studies in parallel
- How do you determine the best architecture? How do you test CONOPS under various threat conditions? How many variables do you control? How long can we afford to study this?

*Receiver operating characteristic - probability of detection vs false alarm rate

Consider: Testing the Untestable

Problem 3 - Tracking movers

- Problem: monitor the motion of sensors in vehicles
  - Proposed solution: GPS tracking with wireless, real-time reporting of user whereabouts
  - Research - none, solved problem, right?
- How to test?
  - Current strategy - run cooperative test subjects in controlled environment
  - Measure coverage, link security, accuracy
    - Question: is this realistic?
- How do you assess responders reactions to being tracked? Will behavior change?
- Is it easier to simulate, emulate, or measure human response? Operational testbed may be most accurate.

Advantages of Real-World Testbeds

Operational testbeds solve many problems

- Source of realistic data:
  - Careful collection yields the best data
    - E.g. prob. 1 - airport data easy to get
    - Algorithms & software can be developed & tested on the same data.
  - Ground truth possible
    - E.g. nuclear detection - repeat vehicles useful
- Costs for complex systems reduced by combining development, testing, & fielding phases
- Time to field is reduced dramatically since the test articles are tested on the job
  - Manpower for Homeland Security is in place

OJT - on the job training of responders & software

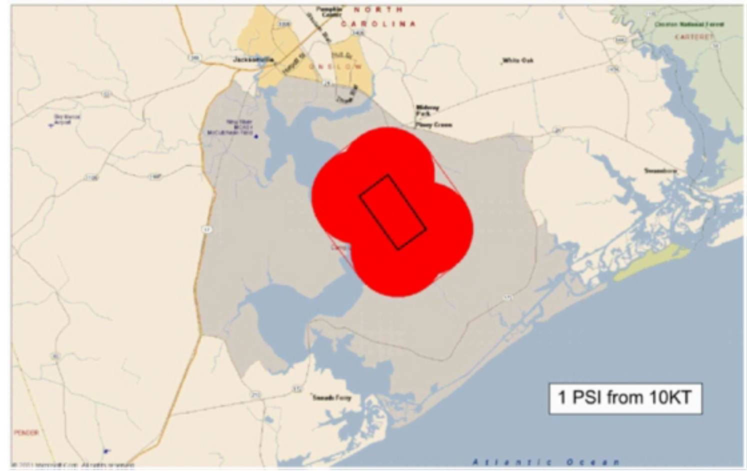
Approach to Real-World Testbeds

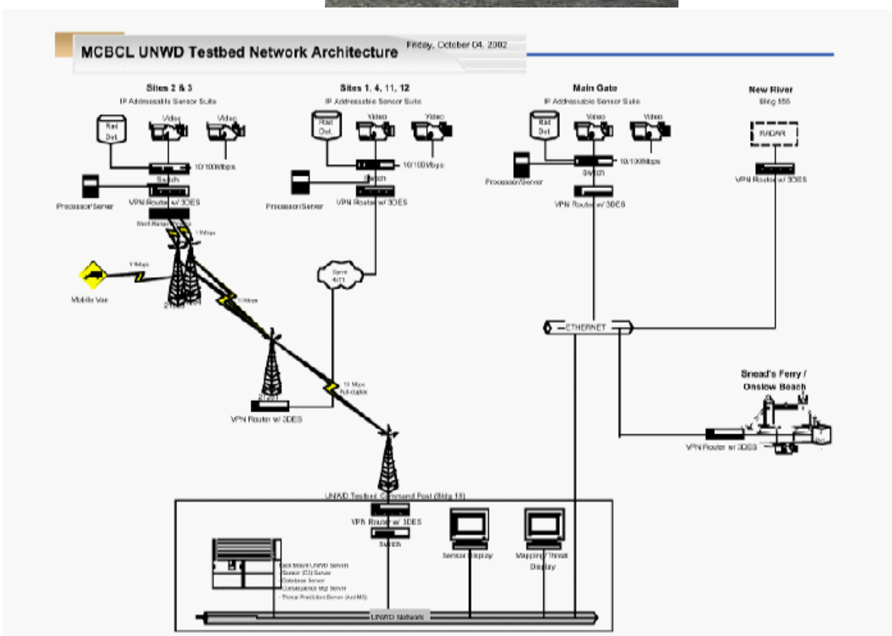
- Pick one or a few places
- Field sensors, network, & software
  - Enough to test the full operational range
- Field strawman response protocol & decision tree
- Collect & analyze volumes of data (in parallel with OPS)
  - Showstopper: Pay for analysis of the data or don’t bother to create the testbed
  - Compare testbed results with predictions from simulations - correct either or both as needed
- Conduct real-world exercises in series of graduating difficulties
- Test & operate as if your life depends on it - it probably does
  - Red team everything
- Be flexible - there is surely more than one solution
  - Don’t wait for perfect sensors & networks

Case Study: Unconventional Nuclear Warfare Defense (UNWD): an evolving testbed

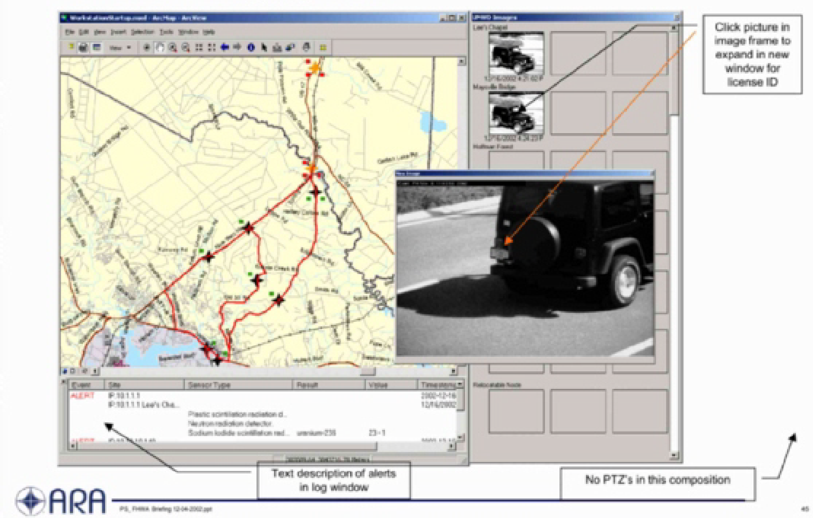
- July 2001, Defense Science Board (DSB) Report on Unconventional Nuclear Warfare Defense (UNWD) recommendation:
  - Deploy sensors and systems in test bed to protect critical DoD installations

Protection Zone





Off-Base Display View



Camp Lejeune Testbed Scorecard

Utility high but full potential not realized

- Ongoing:
  - Sample threats - fake
  - Data on stream of commerce both staged & real
  - Excellent exercise environment with local & base assets
  - Decision tree evolving
  - Network in place, static detection strategy (chokepoints)
- Needed:
  - After the fact ground truth
    - Analysis of commercial & medical traffic
      - Access to local isotope usage information
      - Traffic analysis - repeat cars & trucks
  - Actual threats in covert pass through
  - Greater variety of detection strategies
  - Measured ROC curve

RN Detection Testing - Many Variables

Detection Array

Short Range Detectors (1-3 m)
~ button to smoke detector class
Personnel & Vehicle-Mounted & Fixed

Medium Range Detectors (3-10 m)
~ brief case class
Fixed & Mobile

Longer Range Detectors (>10m)
~ trunk class
Vehicle-Mounted & Fixed

Data/samples

Mix of devices
Large urban area
GPS tracking
Wireless Links
Computer Controls

Confirmation
Fixed, high speed screening and analysis

Wire(less) data

Commands

"BRAIN"

Assessment & Controlled Response System (ACRS)

- Network control
- Array control
- Alert Processing
- False Alarm Management
- Response Initiation
- Response Monitoring

Experimental results

- Parametric trades
- Optimization:
  - Moving vs fixed mix
  - Mixed detection processes
  - Design to budget mixes
  - Operational cost optimizations
  - False alarm management trades
- General Design rules

RN Detector Deployment Options

- Button & smoke detector class
  - Proliferate in buildings, entrances (fixed locations)
  - Police use in traffic enforcement, random checkpoints
- Briefcase detector class
  - Various trusted vehicles on the streets and highways
    - Opportunistic moving detections
  - Harbor security - boats, tugs, etc.
  - Responsive to Small or Large Threats
  - Police use in traffic enforcement, random checkpoints
- Trunk size detectors (or larger arrays)
  - Truck weighing stations (fixed)
  - Water choke points
    - Marinas, canals
- Covert & concealed, decoyed, fixed and moving

What mix is best?

Summary: Real-World Testbeds

- Make the world a lab
- Real-world testing needed for complex WMD defense systems of systems
  - When do they work? When do they break?
- Some real-world properties cannot be simulated or emulated
  - Human response is hard to measure in controlled scenarios
  - Number of variables prohibits exhaustive testing
- Solution
  - Develop, field, test, & train in operational testbeds
  - Pay for the analysis