SAND2006-3171P

System Engineering & Networked Sensors:

Tying the Pieces Together

Carolyn Pura

University of Nevada – Las Vegas
"Nuclear Threat and Detection for Homeland Security"
May 4, 2006

Sandia National Laboratories

Tonight's Lecture

- Status of network development for radiation detection
- System engineering & network design principles
- An example of the network design process
- Some considerations for future work in this area

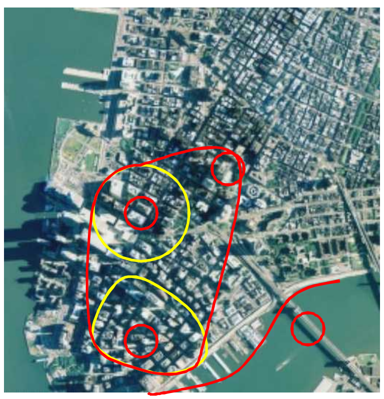
On the Road to Comprehensive Detection System Deployments

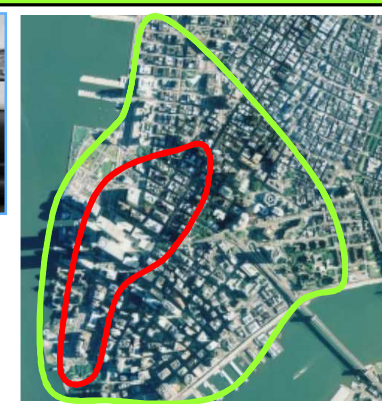
- Earlier applications – domestic safeguards, limited force protection, intelligence, arms control/nonproliferation
- 9/11 forced the radiation detection community to refocus
- Problems call for extensive, comprehensive, & integrated solutions
- DoD, DOE/NNSA, DHS have been demonstrating capabilities required
  - Studies & Simulations
  - Mobile Detection Systems
  - Networking Information & Communications
  - Customs Port of Entry (POE) deployments
  - Department of Homeland Security (DHS) CounterMeasures Testbeds (CMTB)
  - Department of Defense (DoD) Testbed

Project Haystack Study

Evaluated the feasibility and effectiveness of a wide area detection system architecture to protect dense, high-value targets from unconventional delivery of a nuclear device.

November 2000 – March 2002





<u>Target</u> Analysis

<u>Threat</u> Analysis, Incl. <u>Source</u> & <u>Scenario</u>

Evaluation of <u>Current Technology</u>

<u>System Concepts & Performance</u>

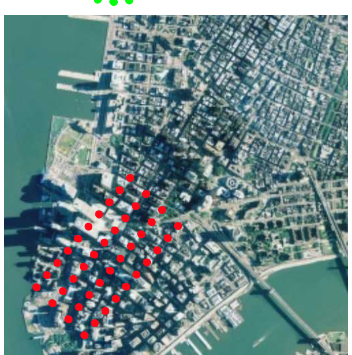
<u>Recommendations</u>

Sandia National Laboratories

Five Detection System Architectures were Considered

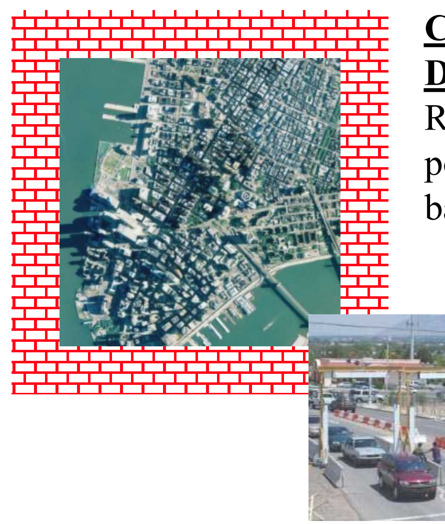
Distributed Defense
Detectors are uniformly distributed beyond the target area for early warning

Concentric Defense
Greater probability that the threat will pass by more than one detector node



Terminal Defense
Immediate target area is densely covered with detector nodes to discover a threat as it reaches the target

Mobile Defense
Detectors deployed on existing infrastructure of law enforcement vehicles, etc.

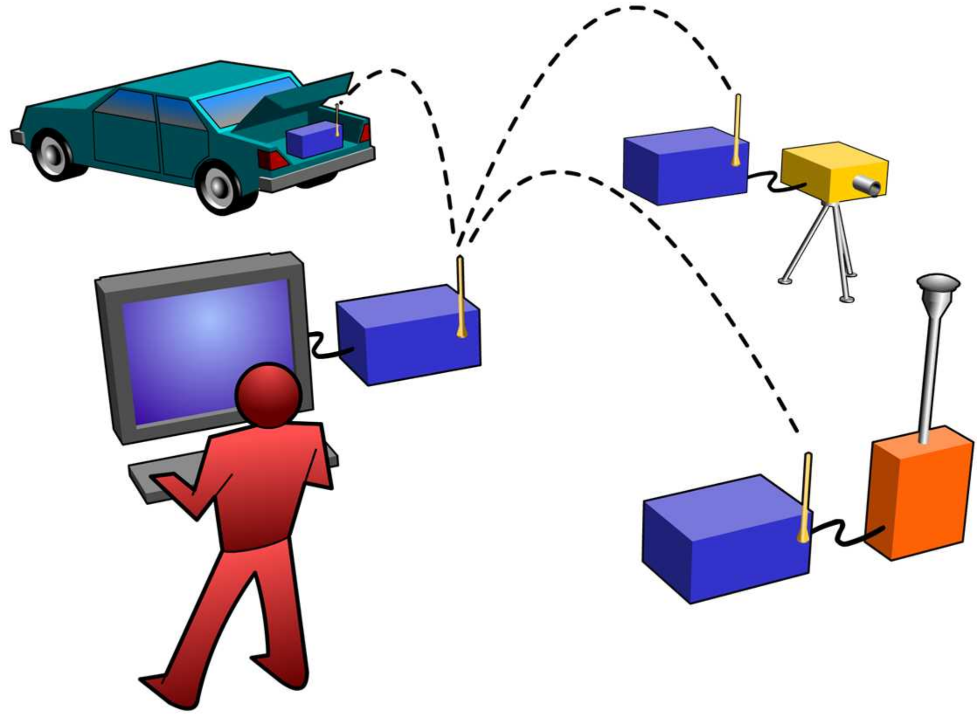


Controlled Access Defense
Restricted ingress, portals and physical barriers

Sandia National Laboratories

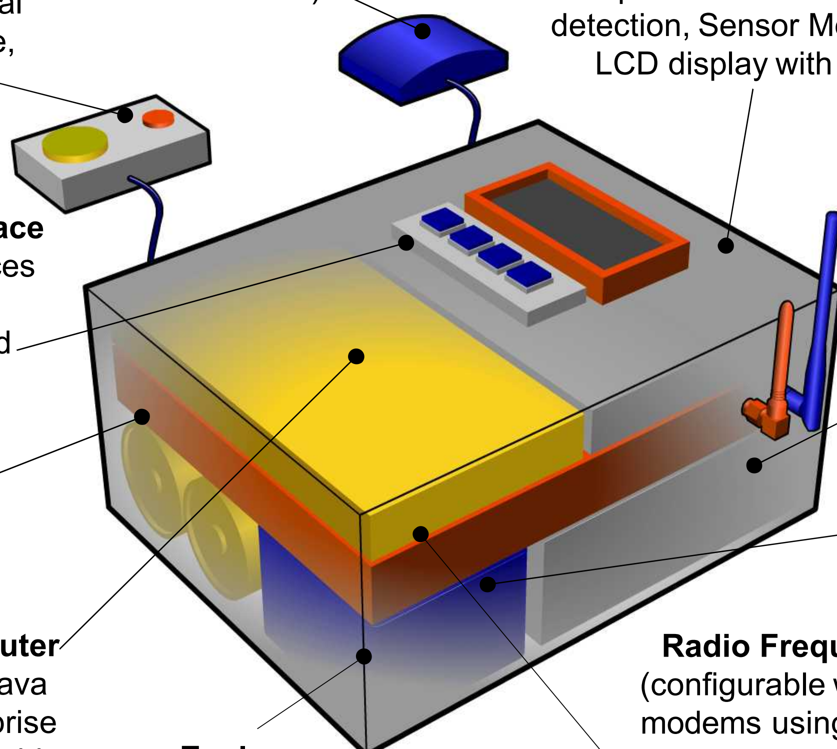
Sensor Management Architecture (SMA): ISM Based Sensor Network

– ISMs utilize an innovative combination of embedded computation, noise immune spread spectrum wireless intercommunication, real-time telemetry for integrated and interfaced sensor and detection systems, and a distributed software framework for data aggregation and visualization.



– ISMs are aggregated to provide a scalable architecture (based on node density and transmission range). ISMs can intercommunicate, and can seamlessly join, leave and rejoin ISM node subpopulations.

Intelligent Sensing Module (ISM): Hardware



Sandia National Laboratories

Networking Information & Communications

- Data Highway for Comprehensive Set of Homeland Security Sensors
- Distributed Access with Multi-Level Security, Information Fusion, and Common Operational Picture
- Ultra-High Level of Reliability, Survivability, and Security
- Scalable Across State, Local and Federal Governments

DHS Test Bed Objectives

- Test and evaluate COTS and advanced systems
  - Common test bed for benchmarking
  - Determination of requisite system characteristics
  - Real world environment
- Mold technology development with operational experience
- Guide forthcoming regulations
- Gather data on radiological characteristics of routine commercial traffic
- Train response personnel

Test Bed Includes all Modes of Transportation

Marine: Cargo Containers

Aviation: International Cargo

Land: Bridges, Tunnels and Terminals

Rail: PATH and AirTrain

DoD Testbed Objectives

- Recommended by the DSB 2000 Summer Study & approved by Congressional funding legislation
  - Deploy nuclear protection systems at DoD bases
  - Provide an integrated sensor test bed network for base/force protection
  - Leverage law enforcement, DoD Force protection and DOE technology
  - Integrate, if/where possible, other types of chemical/biological/explosives sensors into the network

Unconventional Nuclear Warfare Defense Baseline Demonstration

RIS III at a Military Base

RIS III at a Military Base

Marine RIS on the inter-coastal waterway

Marine RIS on an ocean bay

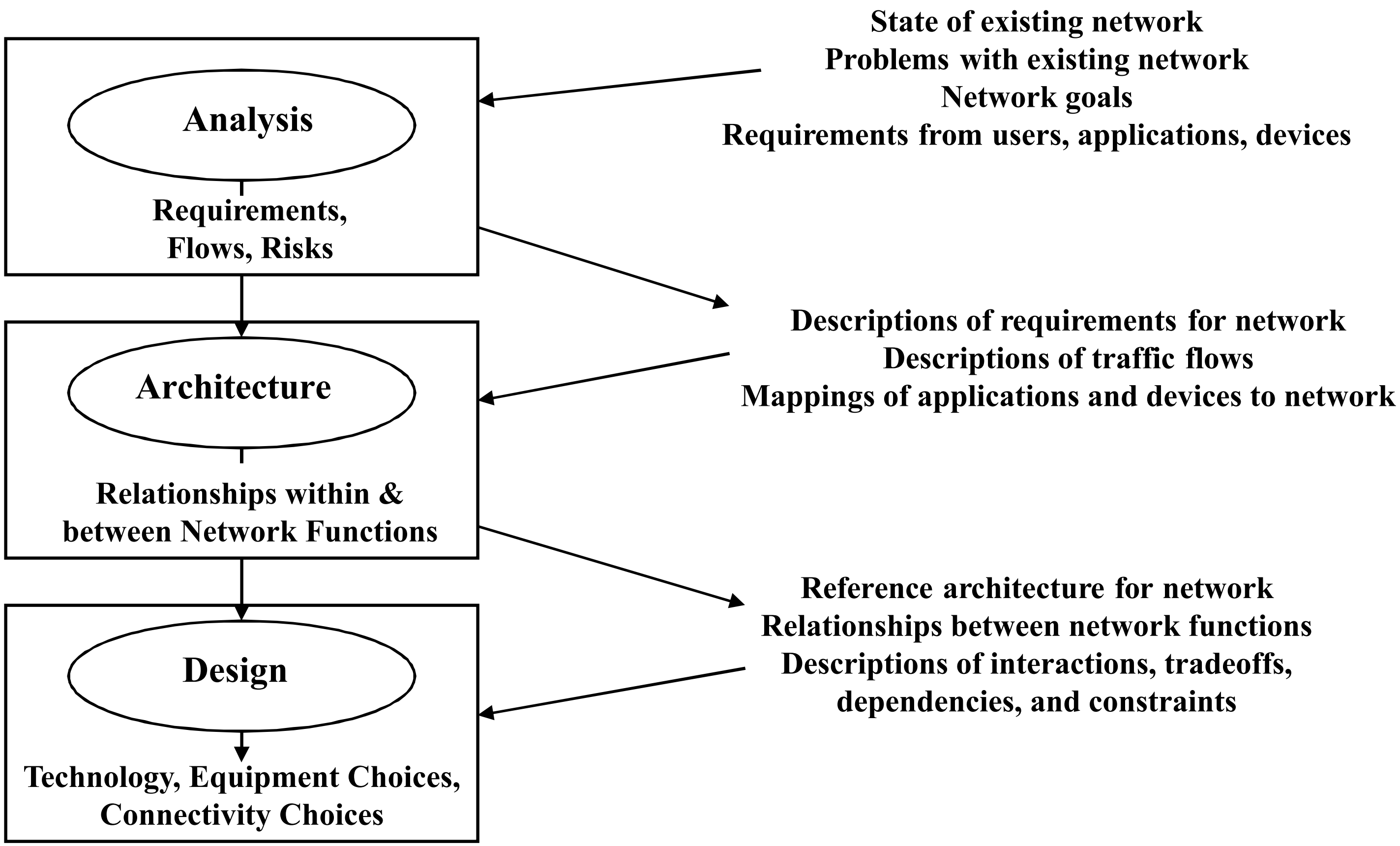
Sandia National Laboratories

Characteristics of a Good Network Design

- Delivers the services requested by its users
- Delivers acceptable throughput & response times
- Within budget & maximizes cost efficiencies
- Reliable
- Expandable without requiring a major redesign
- Manageable & maintainable by support staff
- Well-documented

Reference: "Data Networks: Routing, Security, and Performance Optimization" by Tony Kenyon

Network Analysis, Architecture, & Design Process



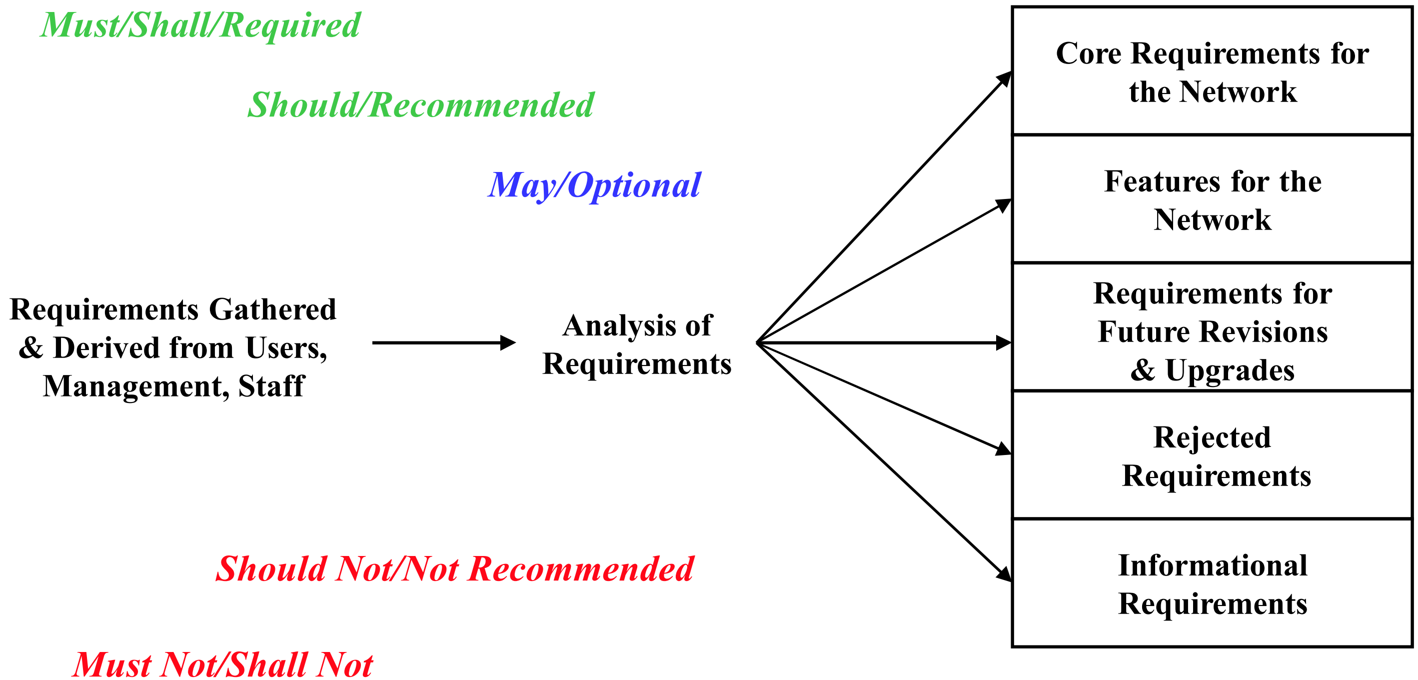
Reference: "Network Analysis, Architecture, and Design" by James D. McCabe

Requirements Analysis: Process

- Gathering & Listing Requirements
  - Determining Initial Conditions
  - Setting Customer Expectations
  - Working with Users
  - Taking Performance Measurements
  - Tracking & Managing Requirements
  - Mapping Location Information

Reference: "Network Analysis, Architecture, and Design" by James D. McCabe

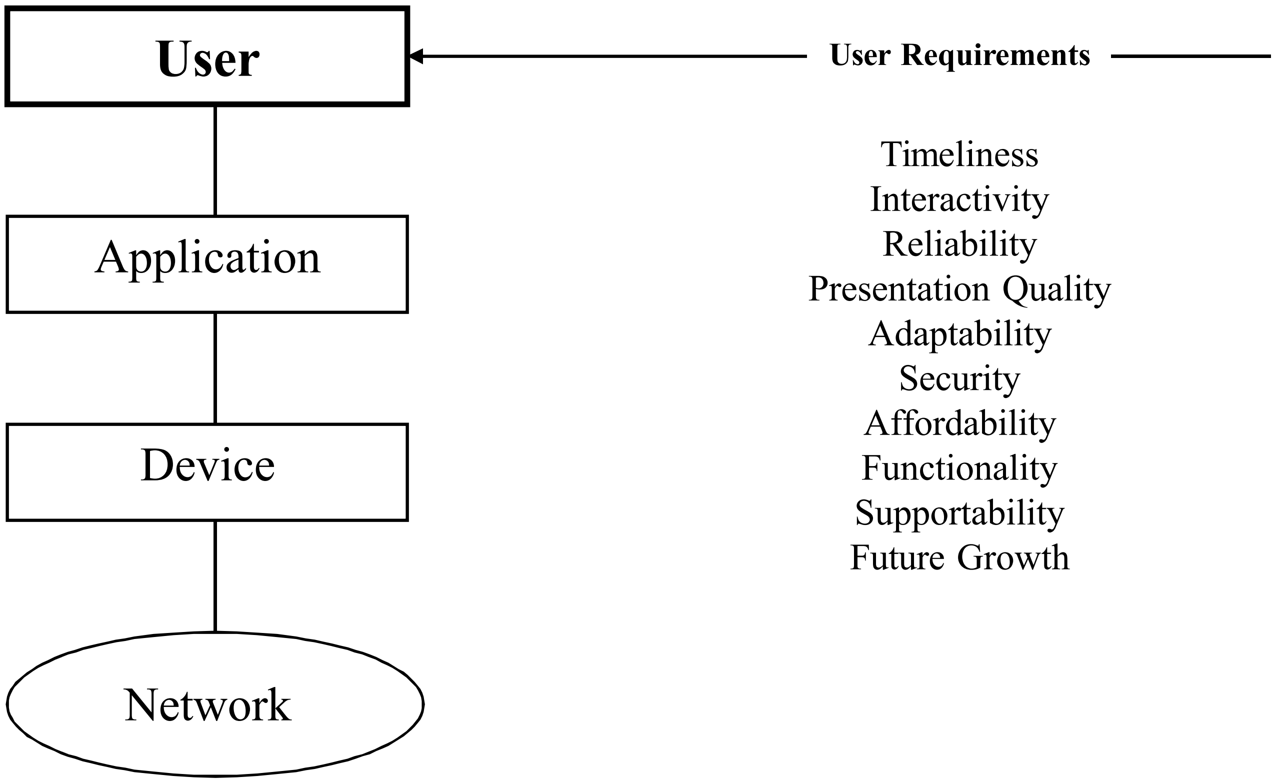
Requirements Analysis: Concepts



Reference: "Network Analysis, Architecture, and Design" by James D. McCabe

Sandia National Laboratories

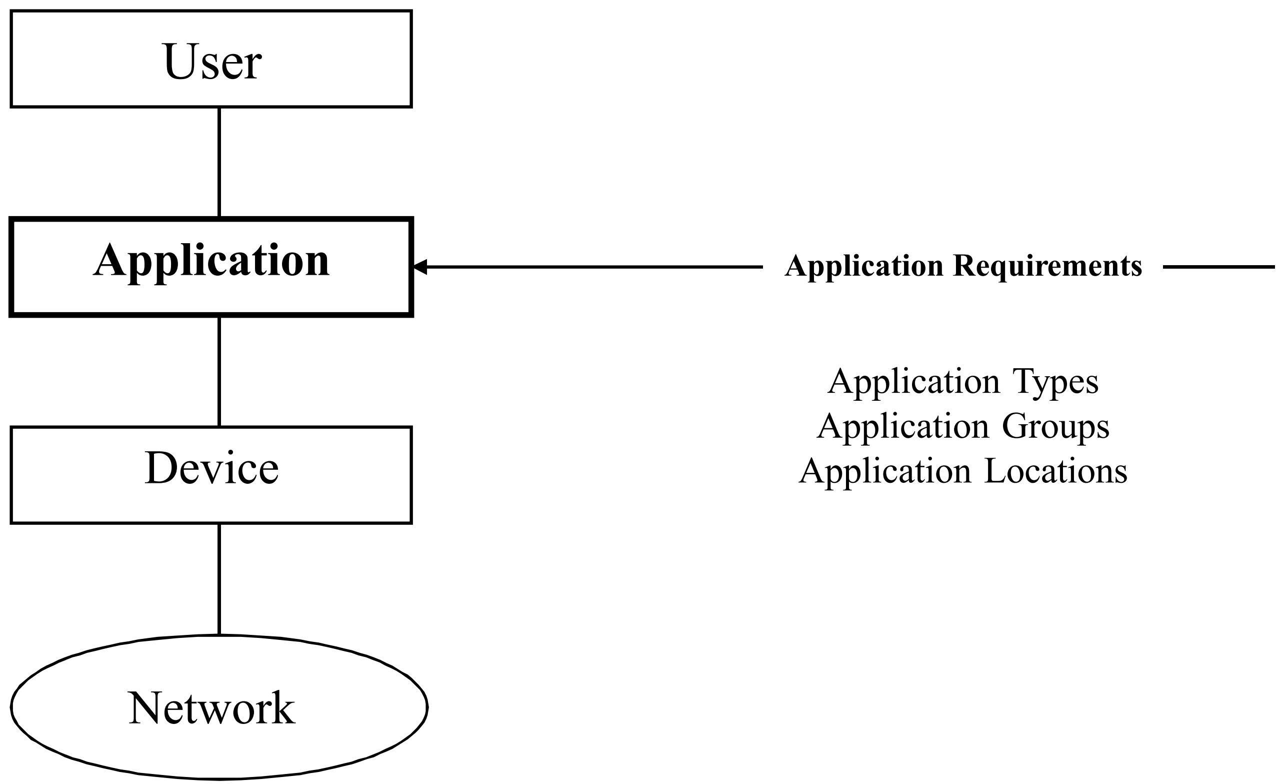
User Requirements



Timeliness
Interactivity
Reliability
Presentation Quality
Adaptability
Security
Affordability
Functionality
Supportability
Future Growth

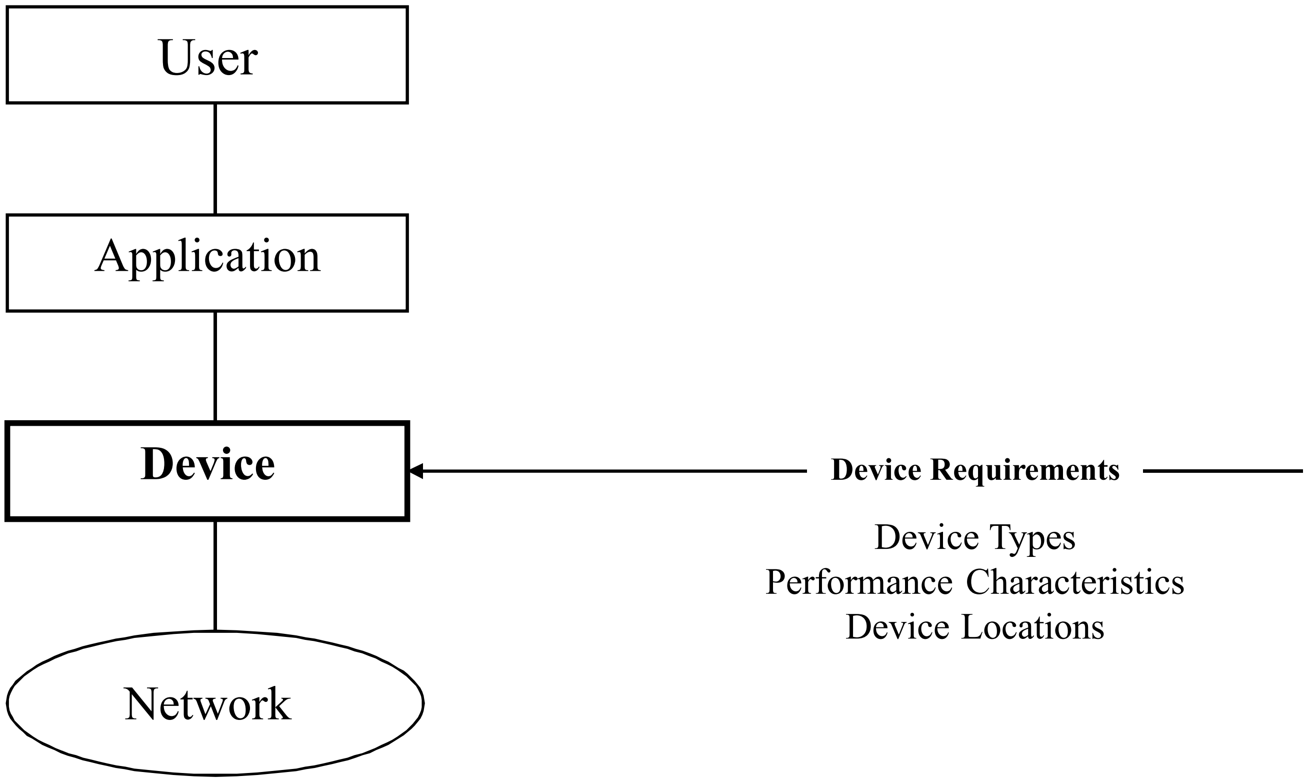
Reference: "Network Analysis, Architecture, and Design" by James D. McCabe

Application Requirements



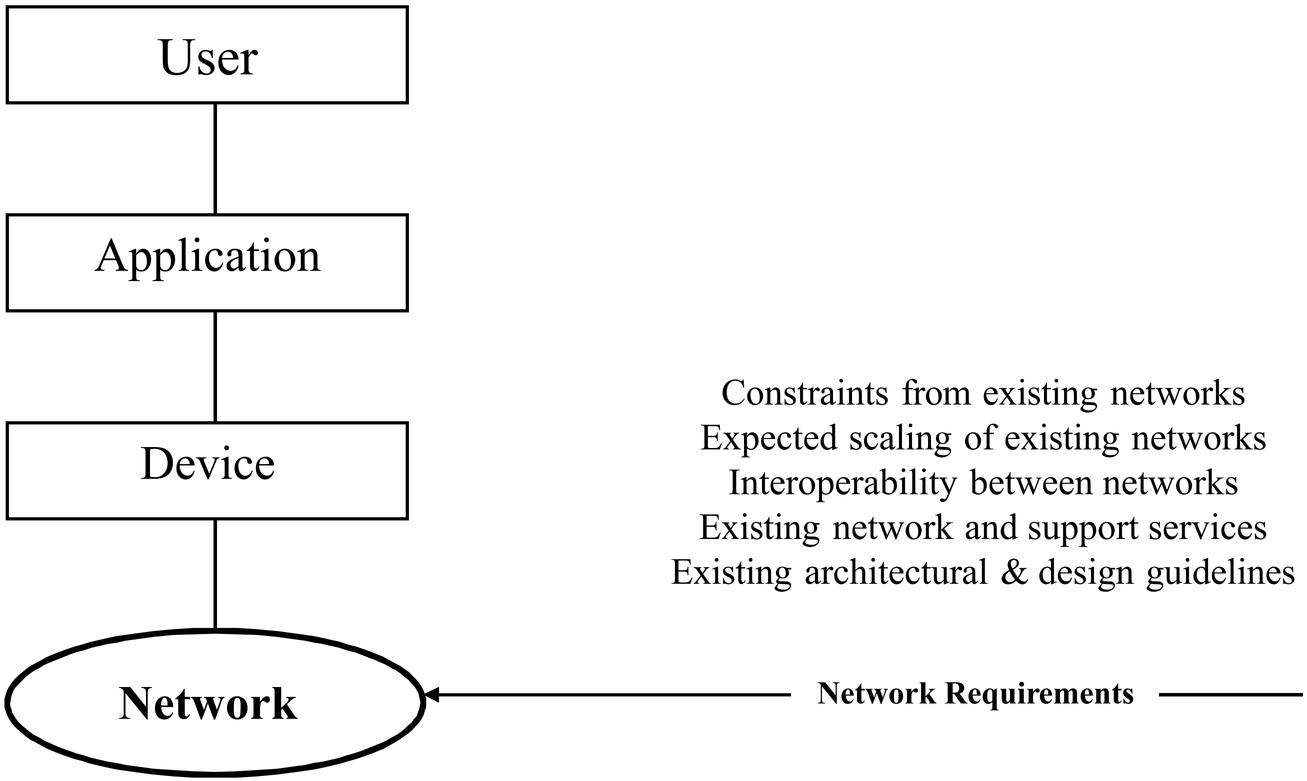
Reference: "Network Analysis, Architecture, and Design" by James D. McCabe

User Requirements



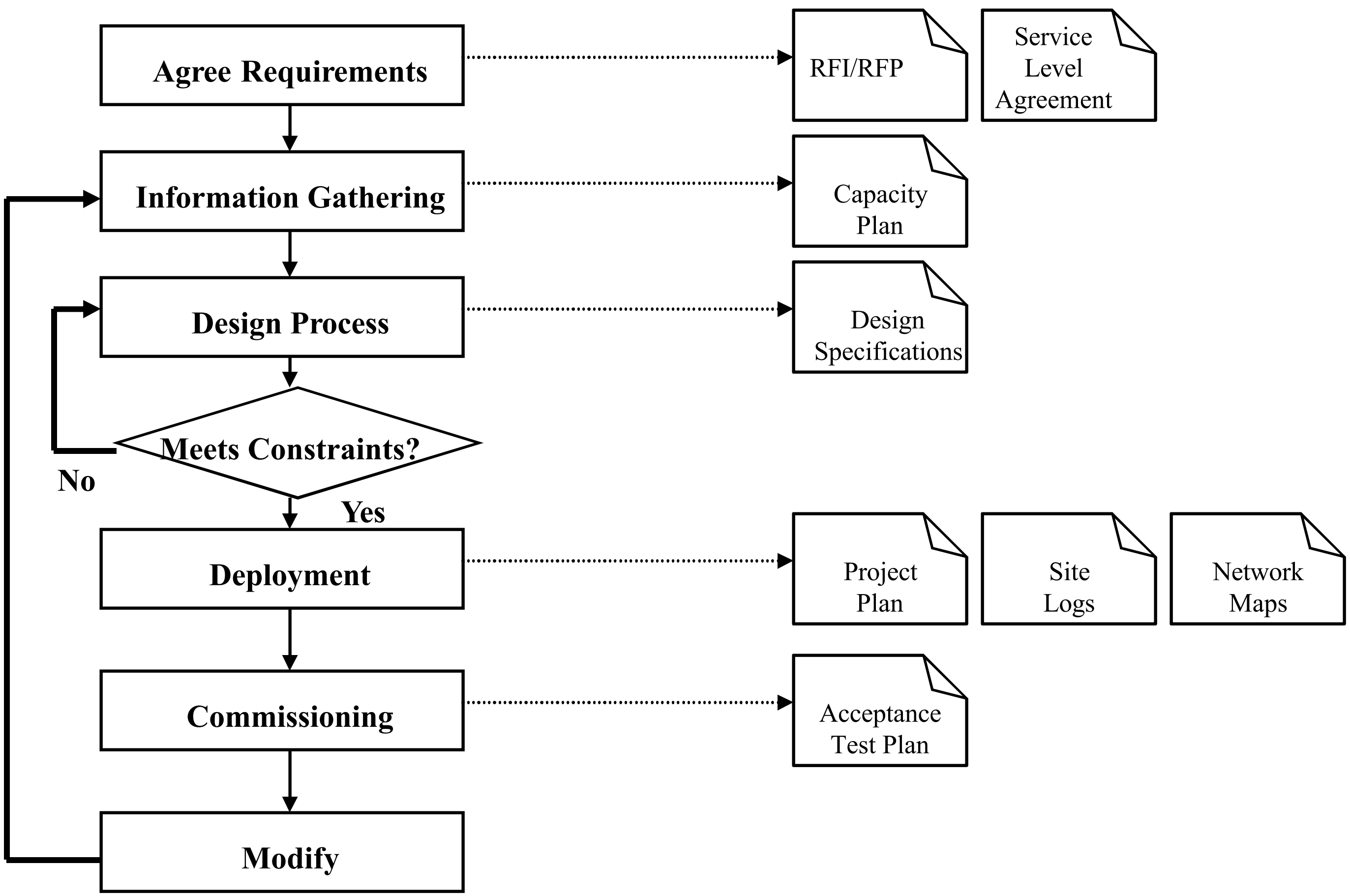
Reference: "Network Analysis, Architecture, and Design" by James D. McCabe

Network Requirements



Reference: "Network Analysis, Architecture, and Design" by James D. McCabe

The Lifecycle of a Design



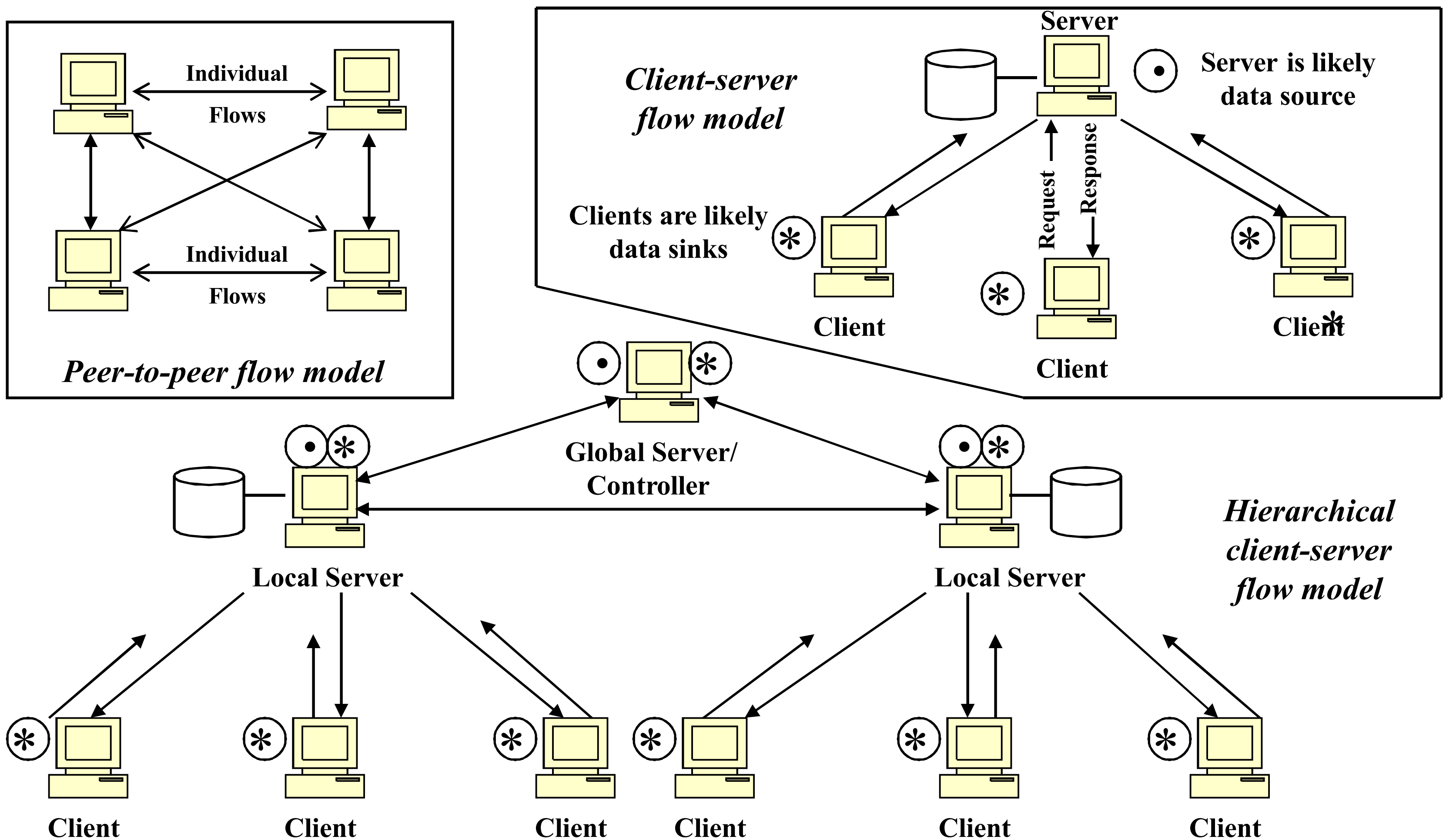
Reference: "Data Networks: Routing, Security, and Performance Optimization" by Tony Kenyon

Building Blocks for the Design

- Building Block 1: The Framework
  - Standards organizations – e.g., International Organization for Standardization (ISO)
- Building Block 2: Applications
  - Centralized, decentralized, client/server, distributed (Common Object Request Broker Architecture – CORBA, Enterprise Java Beans - EJB)
- Building Block 3: Protocols
  - TCP/IP vs. older network protocols such as AppleTalk or IBM SNA
- Building Block 4: Hardware
  - Sensors, servers, system integration
  - Scalability, convergence, traffic optimization
- Building Block 3: Physical Connectivity
  - Low-speed direct vs. dial-up vs. wireless vs. Ethernet vs. satellite
  - Performance, bandwidth, Quality of Service (QoS)

Reference: "Data Networks: Routing, Security, and Performance Optimization" by Tony Kenyon

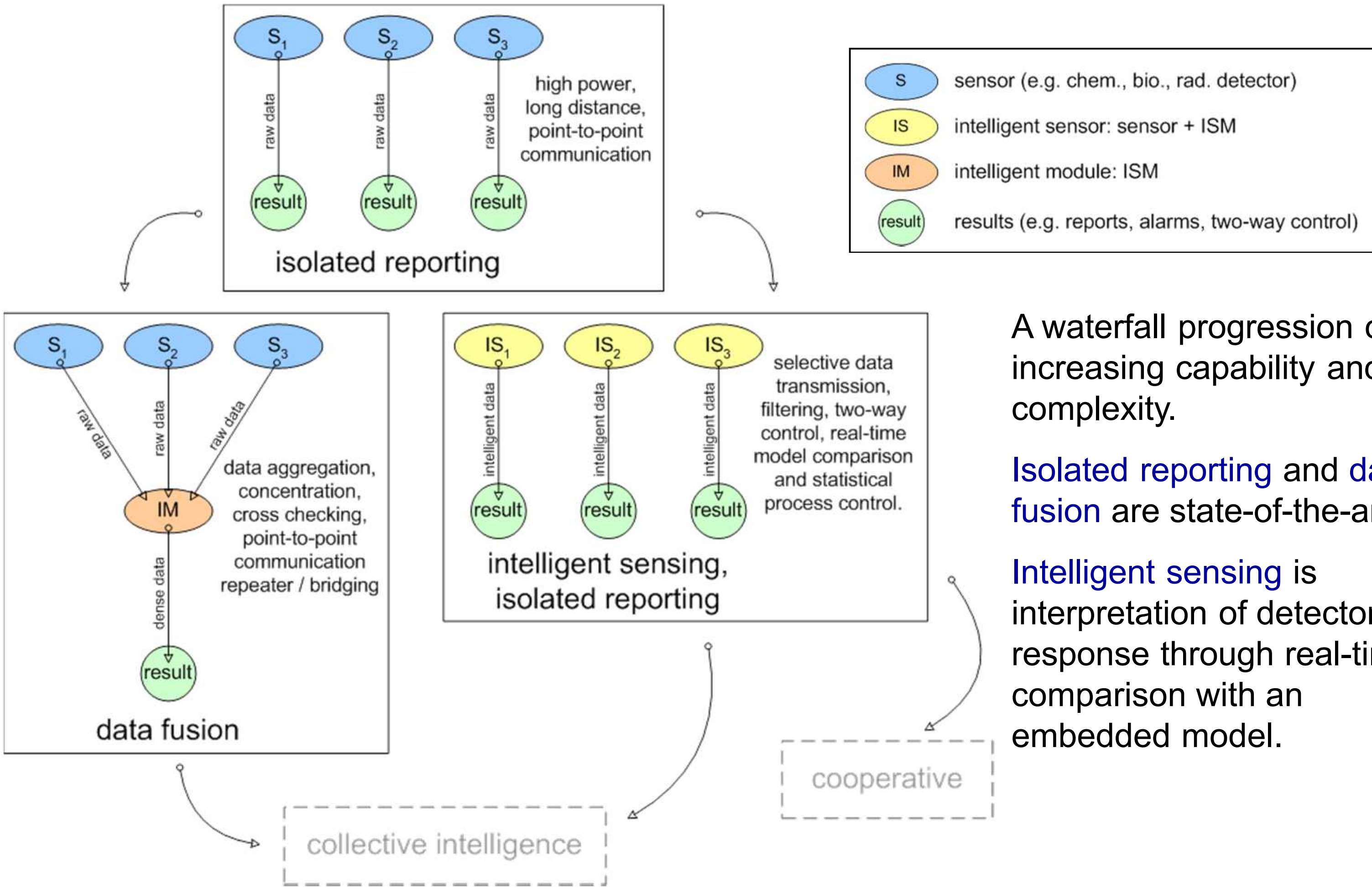
Flow Models



Reference: “Network Analysis, Architecture, and Design” by James D. McCabe

Sandia National Laboratories

Adding Data Fusion to the Picture



A waterfall progression of increasing capability and complexity.

Isolated reporting and data fusion are state-of-the-art.

Intelligent sensing is interpretation of detector response through real-time comparison with an embedded model.

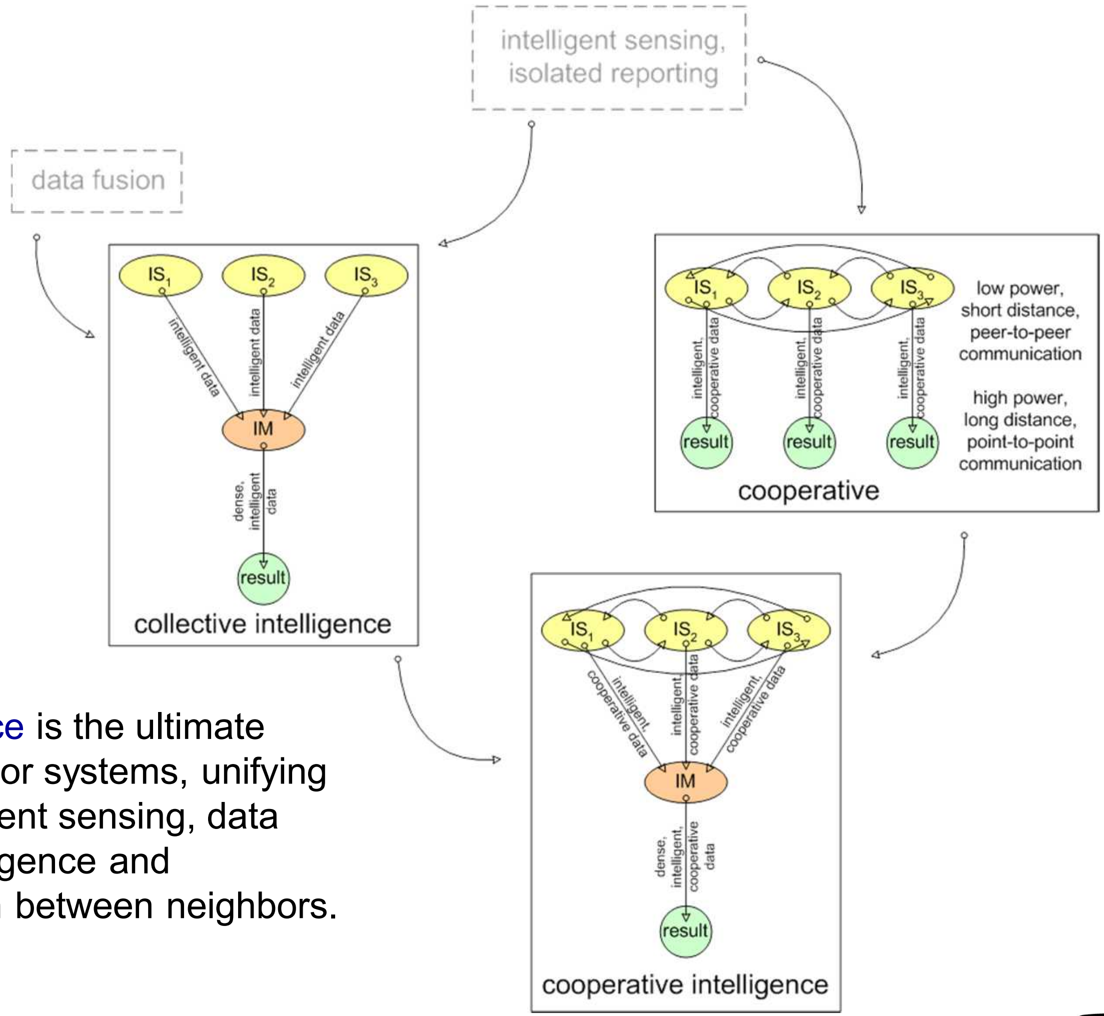
Sandia National Laboratories

Cooperative Intelligence

Collective intelligence supports decentralized conclusions through tiered data fusion.

Peer-to-peer communication where detection systems cooperate and benefit from neighbor input (e.g. change set points based on local input).

Cooperative intelligence is the ultimate goal of advanced sensor systems, unifying the concepts of intelligent sensing, data fusion, collective intelligence and immediate cooperation between neighbors.



Sandia National Laboratories

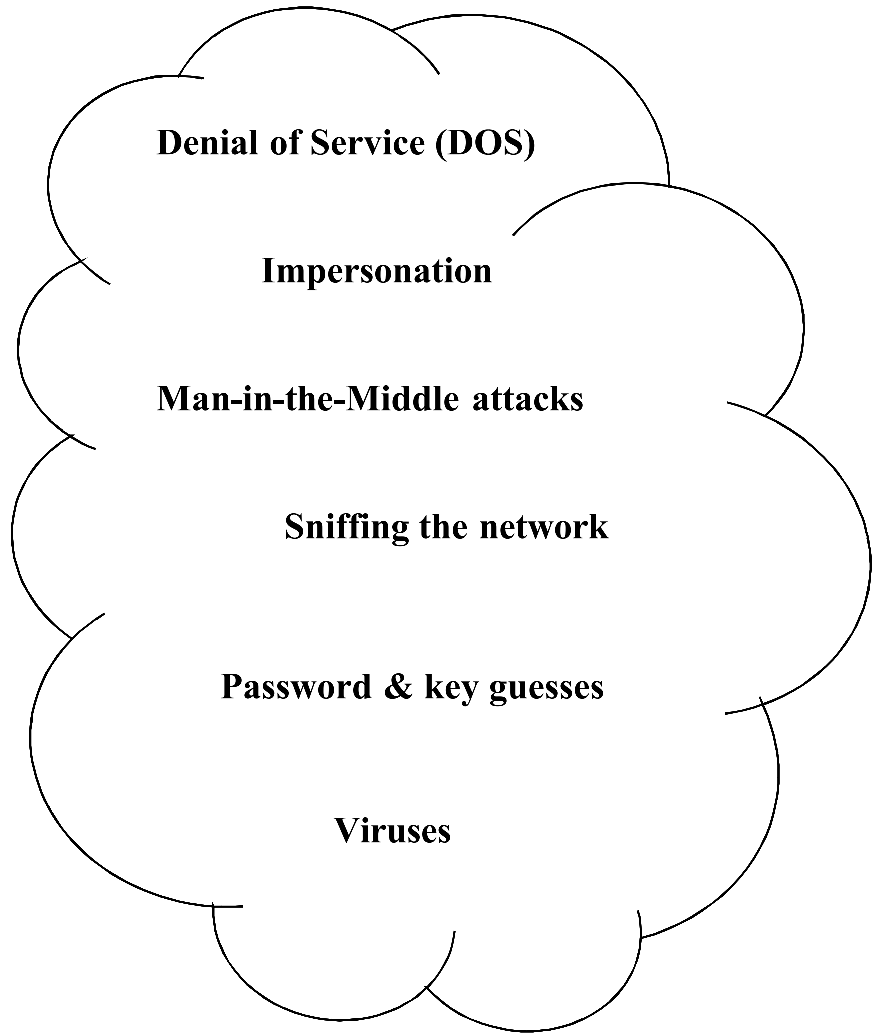
Some Important Details

- Characterizing Behavior
  - Modeling & Simulation
  - User Behavior
  - Application Behavior
- Developing RMA Requirements
  - Reliability - MTBF
  - Maintainability - MTTR
  - Availability – MTBF/(MTBF + MTTR)
  - Thresholds & Limits

Reference: "Network Analysis, Architecture, and Design" by James D. McCabe

Design for Security & Anticipate Attacks

- Authentication
- Access Control
- Confidentiality
- Integrity
- Nonrepudiation



Reference: "Data Networks: Routing, Security, and Performance Optimization" by Tony Kenyon

Planning for Failure

- **Failure –** observed behavior of a system differs from its specified behavior
- **Single Point of Failure – SPOF –** network can be rendered inoperable or significantly impaired by the failure of one single component
- **Multiple points of failure –** network can be rendered inoperable through a chain or combination of failures
- **Fault tolerance –** every component in the chain supporting the system has redundant features or is duplicated
- **Fault resilience** – at least one of the modules or components within a system is backed up with a spare
- **Disaster recovery –** process of identifying all potential failures, their impact of the network as a whole, & planning the means to recover from such failures

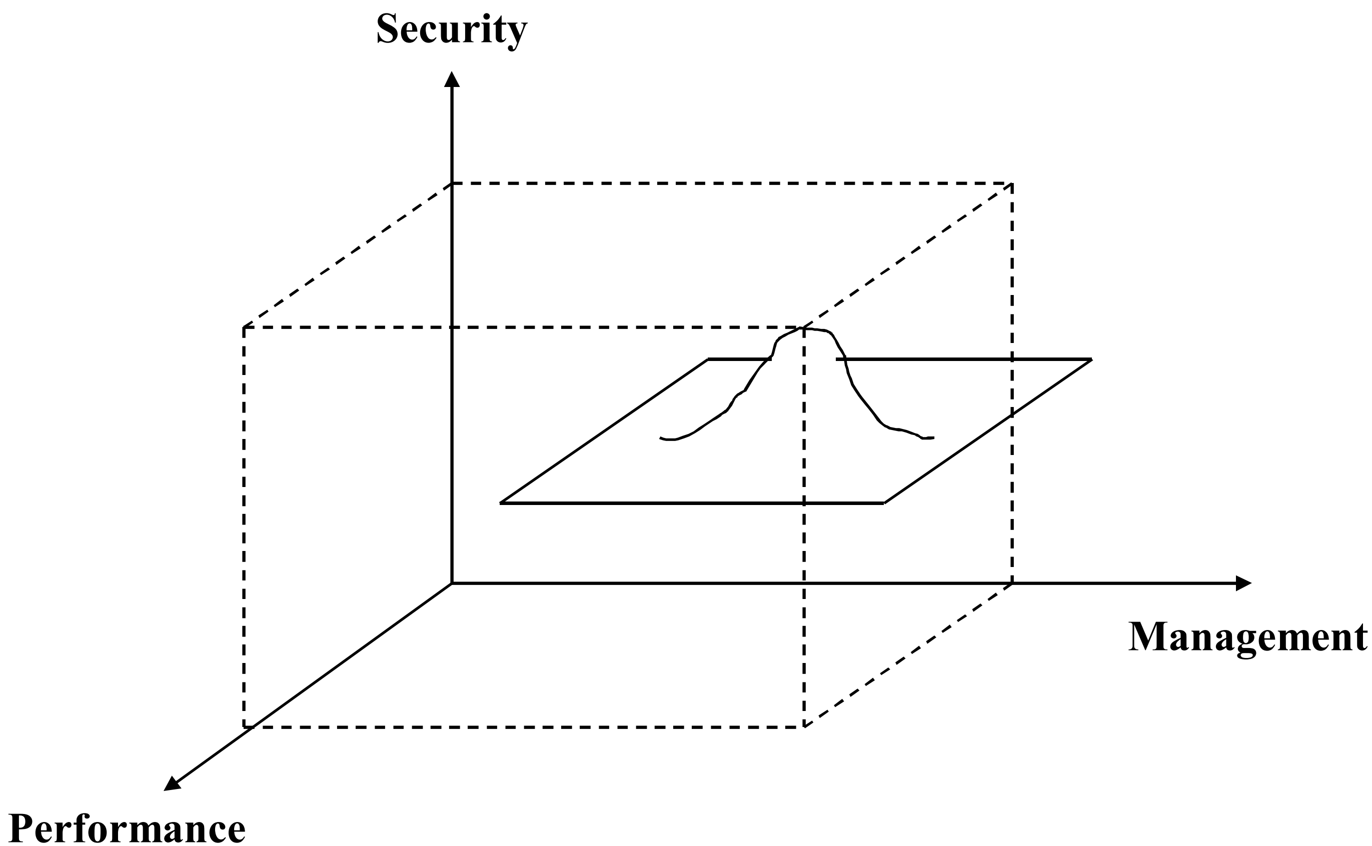
"Whatever can go wrong will go wrong at the worst possible time and in the worst possible way…" – Murphy

"Expect the unexpected." – Douglas Adams,
The Hitchhikers Guide to the Universe

Reference: "Data Networks: Routing, Security, and Performance Optimization" by Tony Kenyon

Sandia National Laboratories

Architecture & Design Solutions are Multidimensional



Reference: "Network Analysis, Architecture, and Design" by James D. McCabe

Implementation: A Phased Approach

- Educate
  - Demo to senior user reps
  - Training operators in equipment & CONOPS
- Pilot Test
  - Be prepared for bugs & glitches
- Acceptance
  - Comprehensive test to prove intended performance
  - Use as benchmark for fine-tuning & optimization
- Deployment
  - Sufficient support in place
  - Fallback plans

Reference: "Data Networks: Routing, Security, and Performance Optimization" by Tony Kenyon

References for Future Use

- **James D. McCabe, "Network Analysis, Architecture, and Design," Second Edition, 2003, Morgan Kaufman Publishers: An Imprint of Elsevier Science, San Francisco**

  An excellent overview of the design process and how to go about it by the Network Architect for BeamReach Networks, consultant, teacher, and recipient of multiple NASA awards and patents

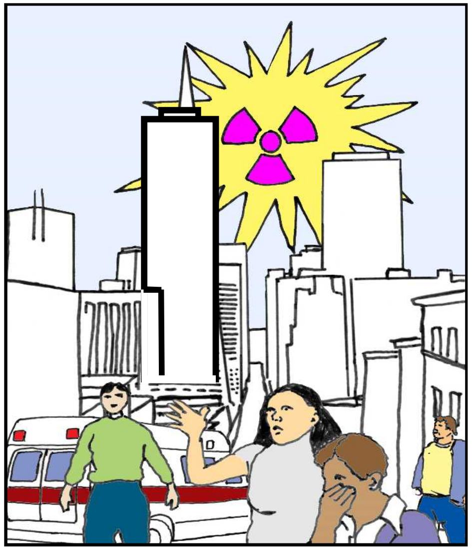
- **Tony Kenyon, "Data Networks: Routing, Security, and Performance Optimization," 2002, Digital Press: An Imprint of Elsevier Science, Woburn, MA**

  A very good overview of advanced topics and performance optimization by the Chief Technical Officer of Advisor Technologies in the UK, designer of several international communications networks and an award-winning network design suite of modeling tools

Wireless Sensor Network (WSN) for Radiation Detection

- We will explore some of the WSN requirements as we follow the developmental path of the Hybrid Emergency Radiation Detector (HERD) project.
- The HERD project provides one potential solution to the detection of radiation fallout after a dirty bomb attack in an urban terrain.

The initial set of requirements for HERD come from an analysis discussion with potential customers and with radiation experts.

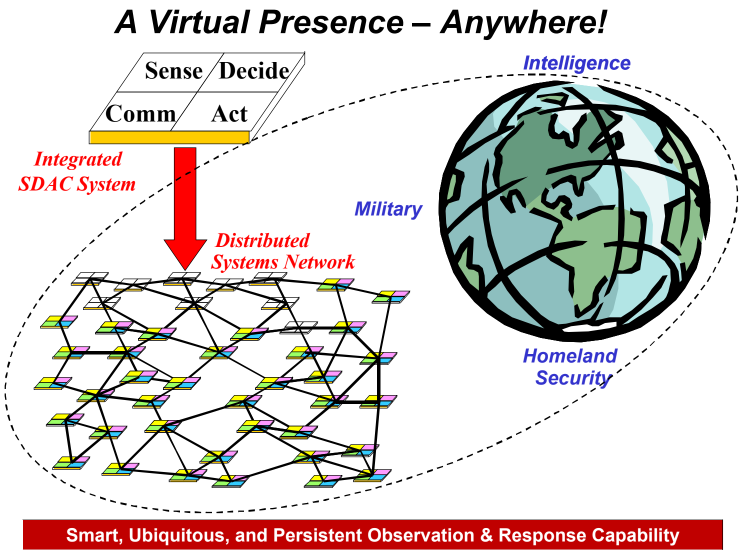


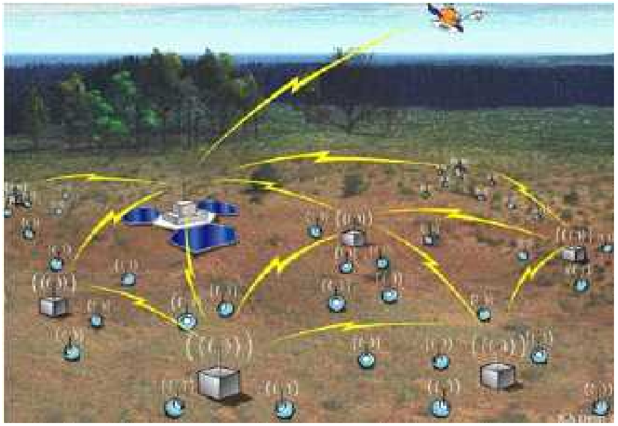
Wireless Sensor Networks (WSNs)

What is a WSN? Collection of sensor nodes, each node is a system containing

- 0 to any number of sensors
- Wireless transmitter/receiver(s)
- Microprocessor on board
- Dense intelligence embedded with local perception

Collectively nodes make up a system of systems of sensors enabling distributed, fine-grained surveillance not previously feasible.





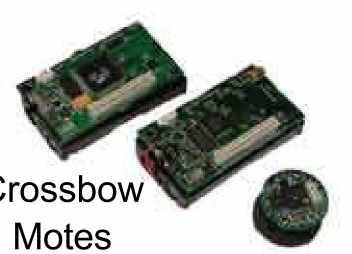
Vision

WSNs represent a hierarchical problem domain with clusters of WSNs each containing other WSNs and ending with individual wireless sensor node(s). Each level of the network can be conceived as a system of systems.

Sandia National Laboratories

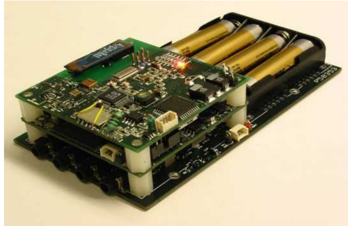
Wireless Sensor Network (WSN)

Wireless sensor networks are a unique integration of hardware and software, forced into small and medium sized boxes. Both technologies depend on each other and neither can stand alone.

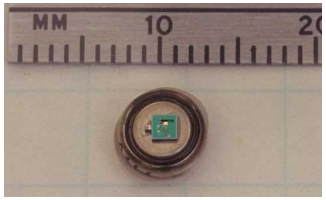


Crossbow Motes

Sensoria



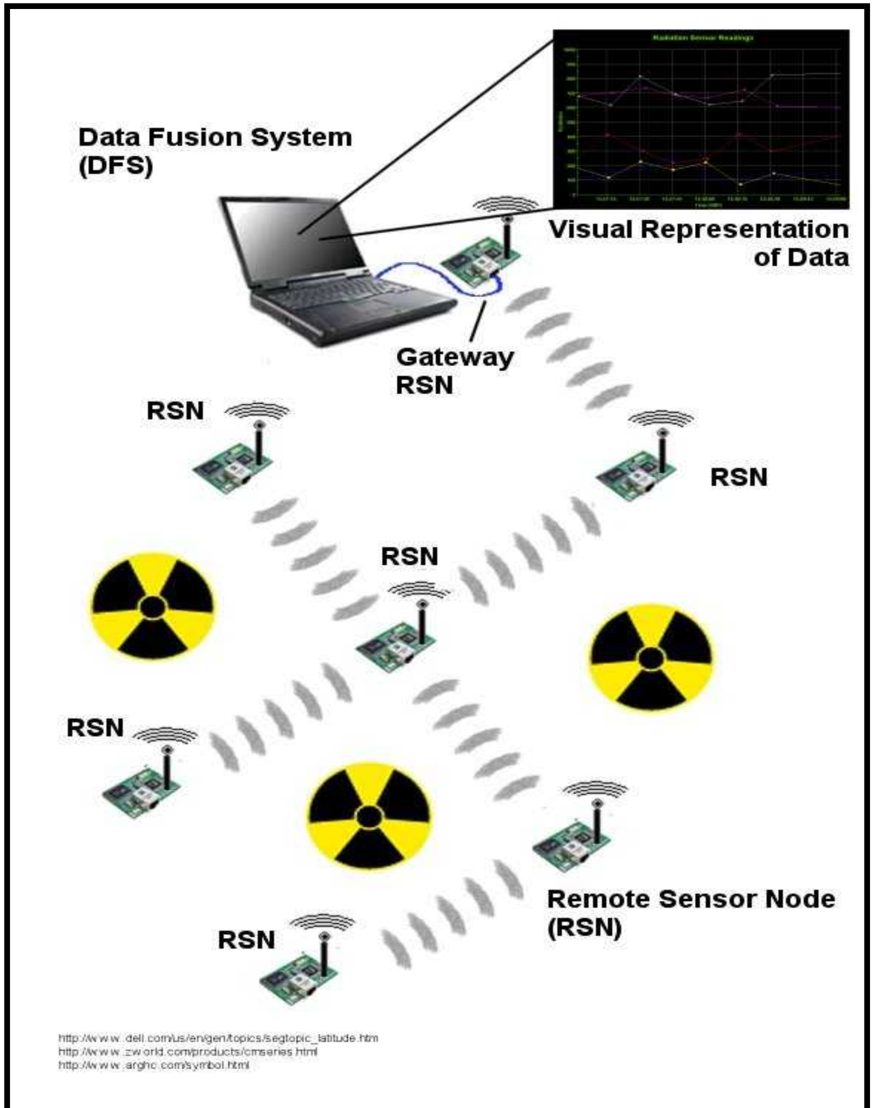
MIT uAMPS:



Dust

There are general sets of requirements for WSNs that assist the developers and end-users in selecting the best configuration of the sensor node and supporting network software.

Overview of HERD Sensor Network



Network is a collection of wireless sensor nodes that:

1. Are distributed across explosive area
2. Form polled ad-hoc network
3. Nodes are polled by Data Fusion System (DFS)
4. Nodes report back to DFS via the gateway node
5. Gateway is used to connect laptop/base station to the node network
6. DFS software provides GIS visualization for user to see node results

Potential capabilities or requirements for high-level sensor technology include: mission space, physical sensor, imaging sensors, environmental sensors, communication, tags, emplacement or mobility, power, control, data processing, networking, and algorithms

Sandia National Laboratories

Parameters for WSN

- Based on system considerations and requirements the following parameters are important to the low level sensor networking "components"
  - Power Consumption
  - Security
  - Network Latency
  - Network Throughput
  - Algorithmic Resolution
  - System Flexibility
  - Per Node Cost
  - Size
  - Network Bandwidth
  - Network Fairness
  - Network Reliability (QoS)
  - Communications Range
  - Node Density

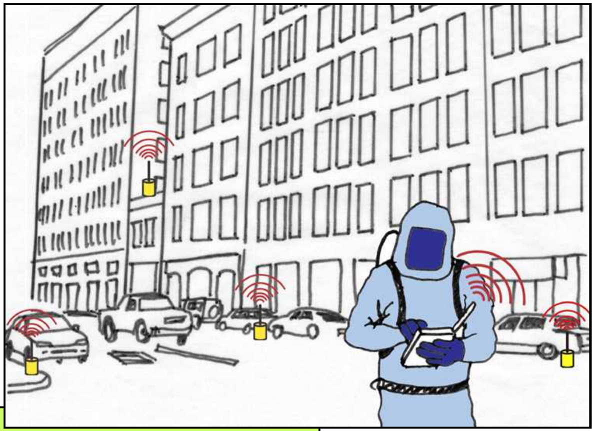
Characteristics of Networking for WSN

Some fundamental characteristics are desired from all WSN in varying degrees:

- High throughput – the ability to transmit large amounts of data per time
- Low latency – the ability to quickly transmit data
- Reliability – durability in hostile environments
- Security – resistance to human interception or disruption efforts
- Convenience – low complexity and easy implementation interoperability

Requirement Considerations

- Mission Space
  - Operational Life
  - Environment
  - Response time (real-time/delay)
  - Covert
  - Persistence



HERD

Operational Life: 1 week to 1 month, reply 10 sec, extend to 30 min….

Estimated length of severe contamination, more can be gained with more battery power.

Environment: Urban terrain

Terrorist will explode dirty bomb where it will cause most panic.

Response time: Real-time

User wants to know up to date information for given radiation node.

Persistence: Data held fixed timeframe

Node will replace data on a cycle or upon request.

Sandia National Laboratories

Requirement Considerations

- Sensors
  - Physical: Acoustic, magnetic, seismic, meteorological
  - Environmental: biological, radiation, chemical/explosive
  - Imaging: optical, thermal, 3-D optical radar, penetrating radar

- Tags
  - Passive or active
  - Chemical tags

HERD

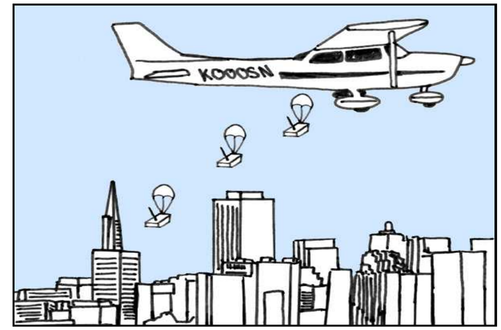
Environmental: Gamma

Easiest initial sensor to build and deploy for node from air.

Sandia National Laboratories

Requirement Considerations

- Communication
  - **Communication links: local RF, long haul RF, range**
  - **GPS**
  - **Authentication**
  - **Encryption**
  - **Antenna (distributed array)**
- Emplacement/mobility
  - **Airdrop**
  - **Ground mobility**
  - **Air mobility**



HERD

Communication: Local RF

Node-to-node communication, supporting multi-hops to get from node A to node B. 100-300 meters

GPS: yes

Node location and clock time taken from satellite.

Antenna: Variable lengths

Nodes to talk between 100-300 meters, may very for different radiation sensor attachments.

Emplacement: Airdrop

Ease of fast deployment over the blast zone.

Requirement Considerations

- Data Processing, Networking, Algorithm, Control
  - Low false positives
  - Beam forming
  - Power cycling
  - Reprogrammability, adaptability
  - High level processing
  - Biometric recognition
  - Routing

HERD

False positives: Users provides range of acceptable readings.

Ranges vary for different radiation fallout and system must support these variations.

Power cycle: Separate radio board and power off main processor, also known as distributed processing.

Unit must live 16 days on 2 AA batteries. Separating radio control means application processor is off unless processing needed. Radio remains on for routing.

Adaptability: Change the rate of testing environment.

User wants to be able to change the rate the node will test the environment.

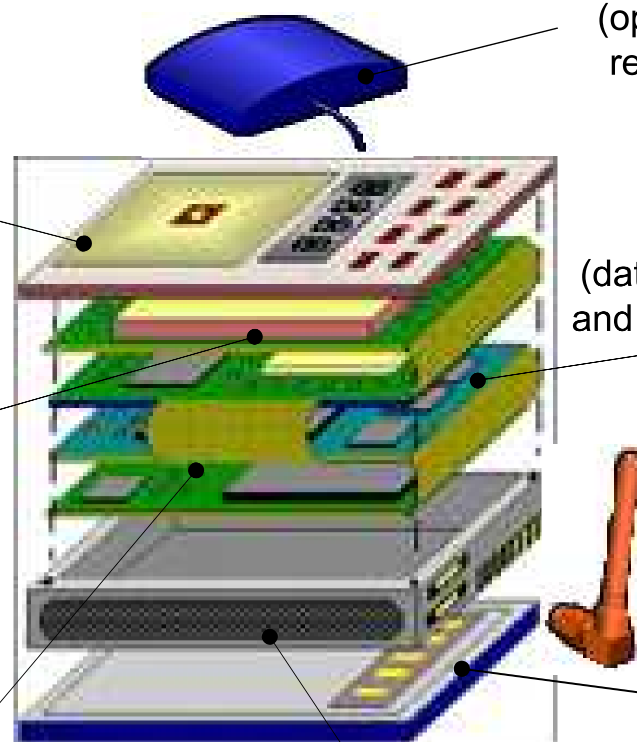
Routing: Hybrid Source Routing

Users require ability to probe single node.

Design Specifications

- **Cost** - inexpensive ($100-$150) (currently~$1000)
- **Size** - small for greater portability, easy deployment
- Range - 100-300 meters (affects size and power)
- Lifetime – 1 week to 1 month (current ~2 weeks w/ 400mw gamma detector)
- Data Rate – Counts every 15-120 min for 1 min.
- Rugged - air drop deployable, land or sea, outside environmental conditions
- **Modular** - Adaptable to other sensor types (i.e. bio/chem detectors)

Decompose of Sensor Node



GPS Antenna
(optional, tethered, remotely located)

Sensor Module
(environmental sensor, temperature, pressure, humidity, light intensity, motion, tamper detection, etc…)

Device Management
(data acquisition, sensor data fusion and integration, display with controls)

Device (Detector) Interface
(external device interfaces, including chemical, biological and radiological detection systems)

Radio Frequency Modem(s)
(configurable, spread spectrum, high bandwidth, low power, long range transmission)

Single Board Computer
(Embedded Linux, Java J2ME, ad-hoc wireless networking)

Battery Pack
(multiple day runtime)

Building Blocks – The Sensing Systems You've Heard About

- Gamma-Ray Spectroscopy
- Gamma-Ray Imagery
- Neutron Detection
- Active Interrogation
- Room Temperature Semiconductor Detectors

Network Design Considerations

- Extent & Coverage
- Performance
- Communications
- Aggregation of Info
- Cost
- National Security
- Decision & Response Process
- Timing
- Concept of Operations
- Policy

Real World Limitations in the Homeland Security Environment

- Many people and commodities generate radiation at levels similar to a nuclear weapon (~1:1,000 people and commodities)

- Significant quantities of some materials can be shielded &/or packaged in compact forms

- Technologies that can discriminate benign radiation sources from radiological and nuclear threats are expensive and not ready for extended deployments

- The National Laboratories have pilot deployments of advanced hardware and software in cooperation with DHS, local governments, and technology companies to develop the next generation of rad/nuc security technologies and procedures

Sandia National Laboratories

Typical Alarm Results

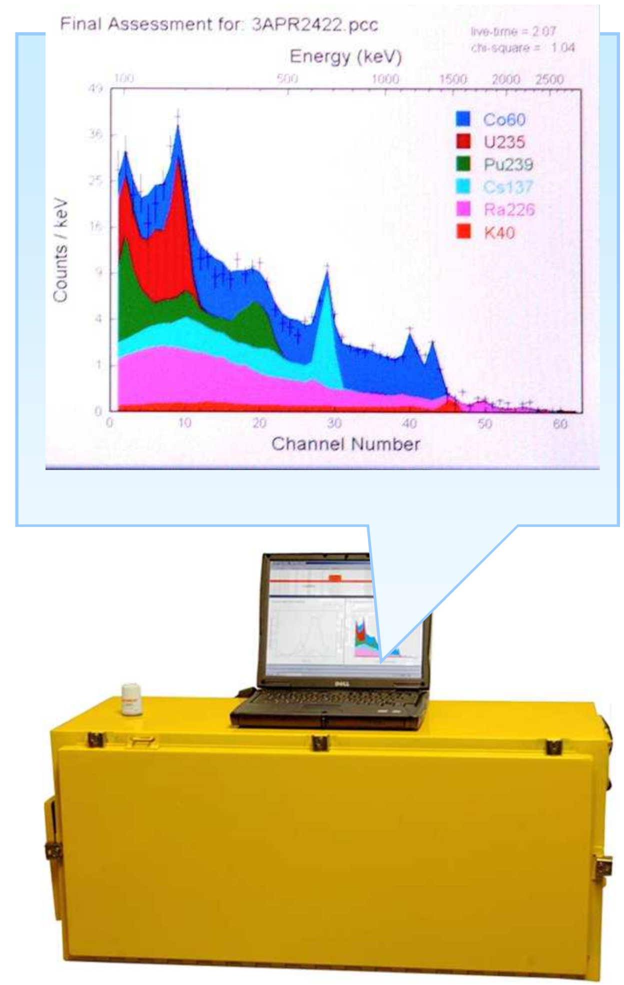
Alarm Rate is typically 1% to 2%

Alarms are from containers, vehicles and people

- 23% – Not Specified
- 18% – Kitchenware/tableware
- 11% – Ceramic Tiles
- 6.6% – Sinks & Toilets
- 6.6% – Stoneware
- 5.1% – Ceramics (Unspecified)
- 4.4% – Medical
- 4.4% – Pottery
- 3.7% – Porcelain Dishes
- 2.9% – Furniture
- 2.9% – Decorative Items
- 2.2% – Chinaware
- 1.5% – Crystal/Glassware
- 1.5% – Toys
- 1.5% – Granite/marble
- 0.7% – Potassium containing chemicals
- 0.7% – Soil Density Gauge
- 0.7% – Pencils
- 0.7% – Fireworks
- 0.7% – Industrial Products
- 0.7% – Arts & Crafts
- 0.7% - Food

SMART System for Radiation Detection and Analysis

- Detects gamma-ray and neutron emitting materials passing within a few meters of the detector
- Automatically identifies the isotope(s), including mixed sources, in near real time
- Indicates the probability that the material is Special Nuclear Material (low, fair, high, or very high)
- Video imager captures image of person or vehicle carrying the radioactive material when the detector is triggered



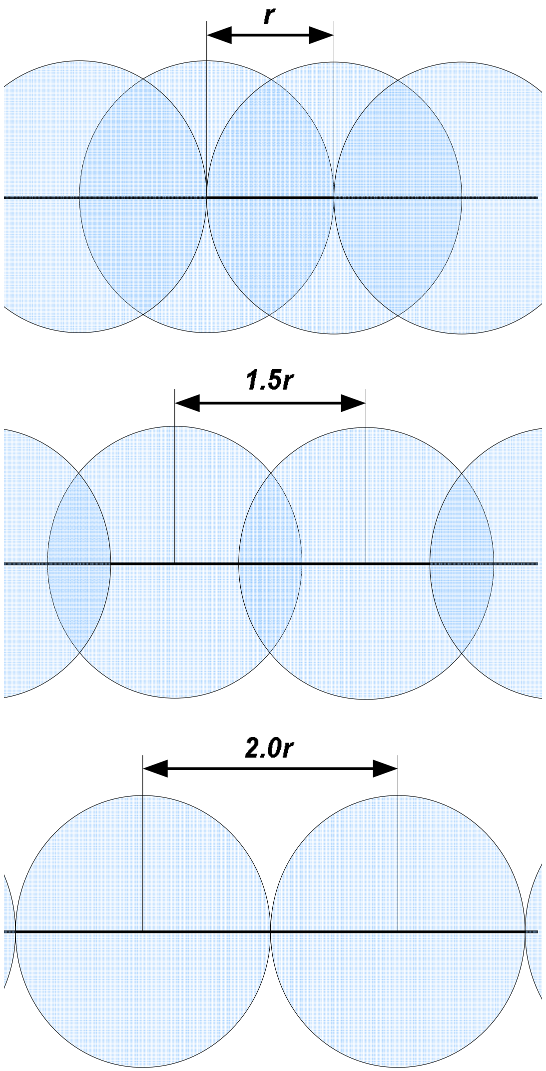
Smart Cart – Examining a Container

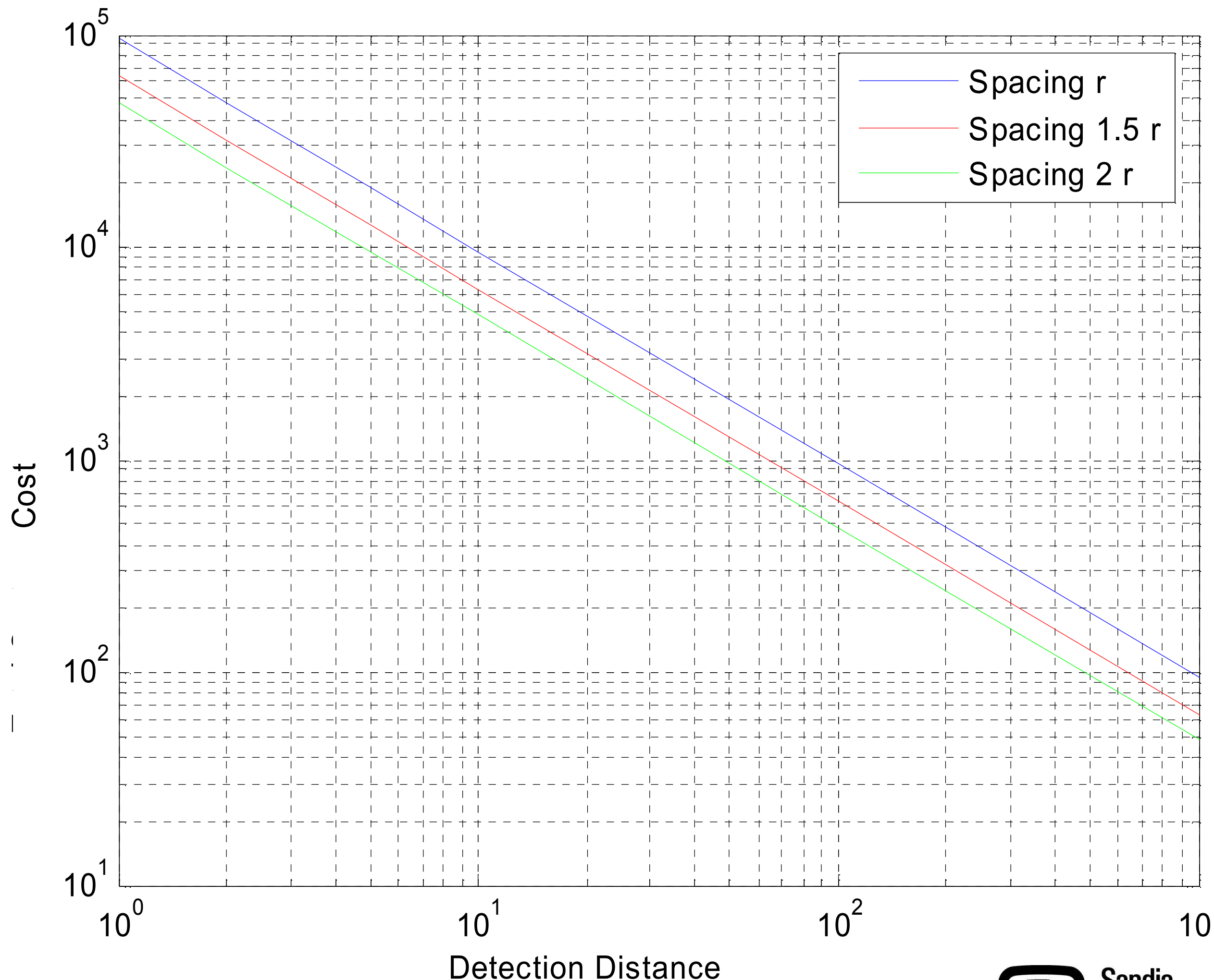
Smart Jeep – A More Robust Solution

Sandia
National
Laboratories

Taking data in traffic

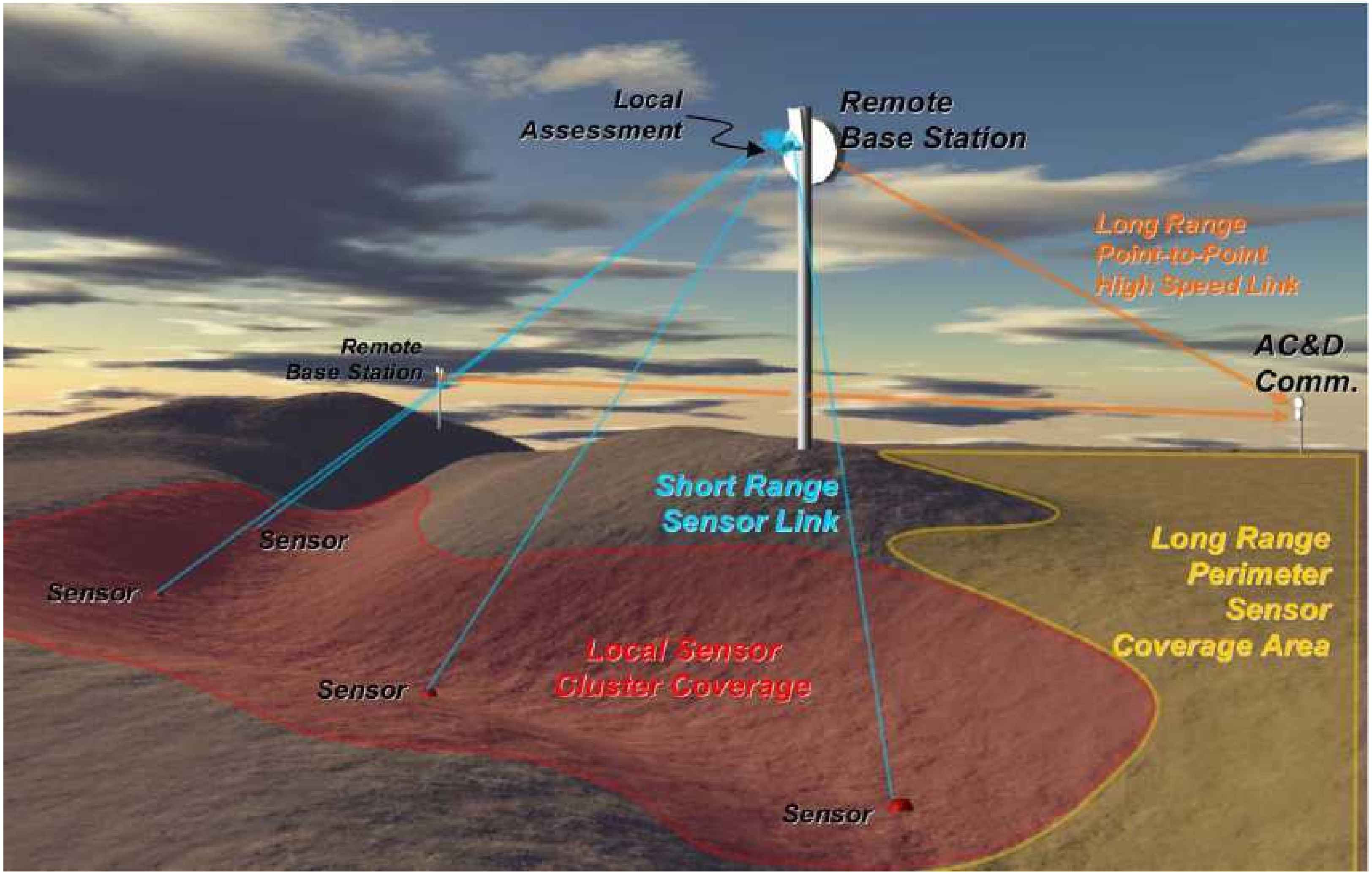
String of pearls style deployment is costly and difficult





Sandia National Laboratories

Creating Networks for Special Applications



Sandia National Laboratories

Sorting Out the Differences: Point versus Area Defense

- Point Defense Benefits
  - Controlled vehicle encounters optimize detector performance
  - Small number of sensors per site
  - Straightforward Concept of Operations (CONOPS)
  - Allows collection of real-world data in relatively controlled setting
  - Development of effective portal detection technology for POEs has wide applicability in overall national defense architecture

Sorting Out the Differences: Point versus Area Defense

- Point Defense Drawbacks
  - Does not rule out likely attack modes for unconventional nuclear threat
  - Must account for possible consequences of interdiction at the Port of Entry
  - Point defenses do not provide a foundation that can be built upon to protect nearby urban centers at times of heightened threat
  - Point deployments may be susceptible to deliberate reconnaissance by threat teams transporting legitimate radiation sources

Sorting Out the Differences: Point versus Area Defense

- Potential Area Defense Benefits
  - Provides some protection for extended areas against device smuggled into US across open border/coastland and transported overland to target
  - May allow threat detection well away from Desired Ground Zero (DGZ)
  - Reduces the danger associated with interdiction

Sorting Out the Differences: Point versus Area Defense

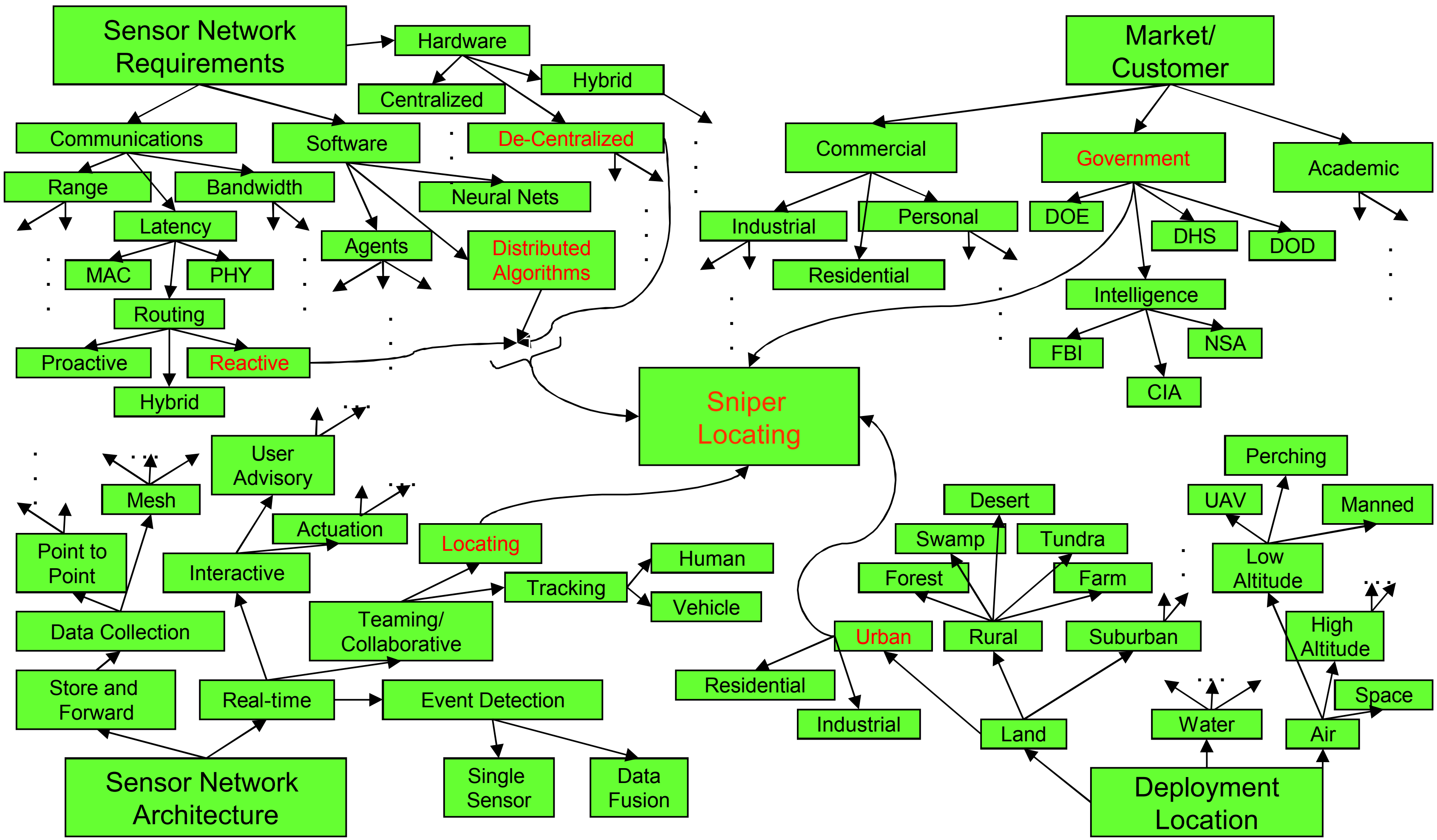
- Area Defense Drawbacks
  - Detectors must operate unattended for extended periods
  - Detector performance uncertain in a demanding application
  - CONOPS for wide area defense has never been tried
  - Ownership/list of participants less clear

On the Road to Comprehensive Detection System Deployments

- Problems call for extensive, comprehensive, & integrated solutions
- DoD, DOE/NNSA, DHS have been demonstrating capabilities required

  - Studies & simulations → Comprehensive
  - Mobile detection tests → Deployable
  - Information linkages → Extensive
  - Extensive DHS POE deployments → 24/7
  - DHS testbed → Integrated DHS solutions
  - DoD testbed → Integrated DoD solutions

Tracking Down a Sniper



Sandia National Laboratories

An Application to Pursue

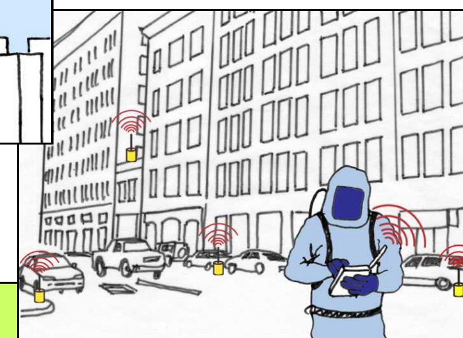
Sandia National Laboratories

Some Days the Real World Bites

Backups

Requirement Considerations

- Mission
  - Operational Life
  - Environment
  - Response time (real-time/delay)
  - Covert
  - Persistence
- Communication
  - Communication links: local RF, long haul RF
  - GPS
  - LPI/LPS/authentication
  - Encryption
  - Distributed array antenna
- Emplacement/mobility
  - Airdrop
  - Ground mobility
  - Air mobility



<u>HERD</u>

Operational Life: 16 days

Environment: urban terrain

Response time: real-time

Communication: Local RF

GPS: yes

Emplacement: Airdrop

Distributed Processing

- **Tradition unattended ground sensors have a one CPU centralized architecture**
  - Processor must have enough performance to perform all task
  - Processor must be general enough to handle all functions
  - Memory requirements are larger to execute all code/tasks
- **Distributed processing: puts the processing where needed**
  - Processors are chosen and designed specific to the task
    - E.g. A sensor processor is quite different than a communications processor in architecture and design
  - Processors are optimized to save power locally
  - Processors tightly coupled to sensor to make sensing smarter
  - Smarter sensors can provide more useful information and filter bad data

Identify Taxonomy of an Application

- Each sensor network and application/scenario has a unique place within any choice of taxonomy

- Taxonomy depends on perspective
  - Sensor network requirements
  - Sensor network architecture
  - Deployment location
  - Market/Customer

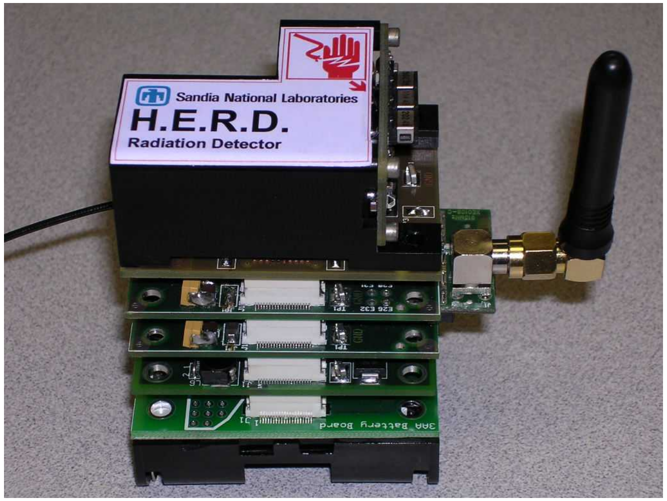
WSN Questions about Requirements

- The multitude of WSN makes it difficult for users and developers to decide what solution(s) are best for their application.
  - What architecture is most appropriate for a particular application/ mission space ?
  - How are the existing sensor architectures different from each other?
  - How to analyze the requirements of an intended application and match them with the capabilities of potential architectures?

Potential capabilities or requirements for high-level sensor technology including: mission space, physical sensor, imaging sensors, environmental sensors, communication, tags, emplacement or mobility, power, control, data processing, networking, and algorithms

HERD Sensor Node Specification

Multiprocessor, component based design – used to obtain low power
Low power – node must live 15-30 days
Extensible and flexible platform – desired for future development
Ad-hoc wireless network robust to failures – network permit user to probe specific node.



Node board stack from bottom to top of node:

Power supply – 2-AA's

Processing/GPS – application processing

Radio board – 915 MHz radio

Sensor board – gamma sensor

Sandia National Laboratories

Hybrid Source Routing

- Custom Ad-Hoc routing protocol for small embedded platform. Why?
  - Can’t fit standard algorithms in small embedded platforms
  - Didn’t require the features of these algorithms
  - Capitalize on the fact that the Data Fusion System/base station is the ONLY consumer of data and has substantial CPU resources, power
- How?
  - Offload route discovery to Data Fusion System/base station, all routes are held on these device(s)
  - Source routing down to sensor
  - Queued route in return path
- Very extendible, supports other routing algorithms

Networking is the Key

The deployment of sensor networks begins with understanding the large number of requirements and how they apply to the application.

The major key issues in the initial understanding of these systems are the **networks** that support retrieval and transmission of data and commands between the sensor nodes and the end-user(s).

Without established networks wireless sensor cannot be accomplished.

Networking Protocol Selection

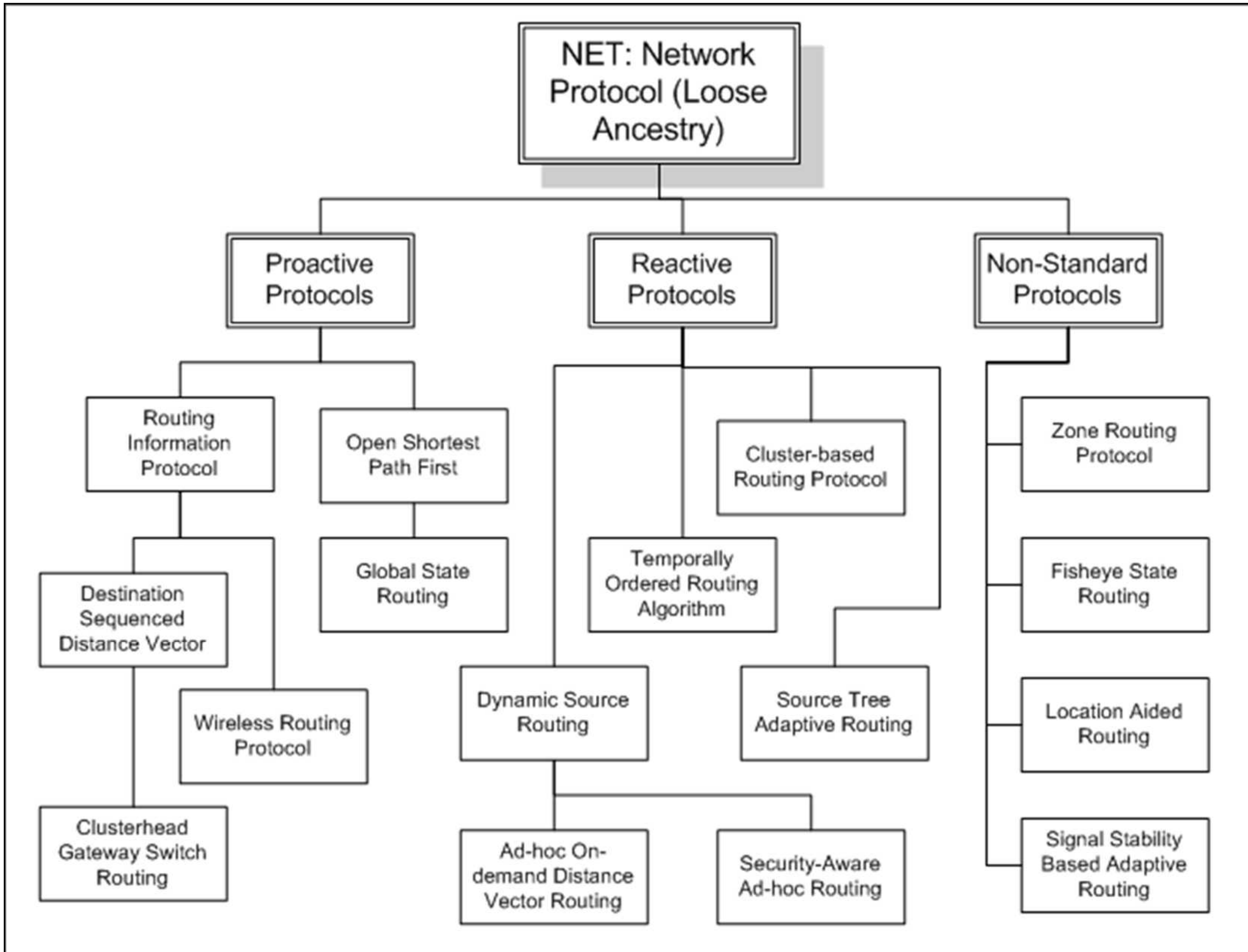
Routing protocols can be classified as proactive/ reactive

- Proactive protocol creates routes before they are needed
- Reactive protocols create routes in response to route requests

Additional categorized based on the method a protocol uses to construct routes

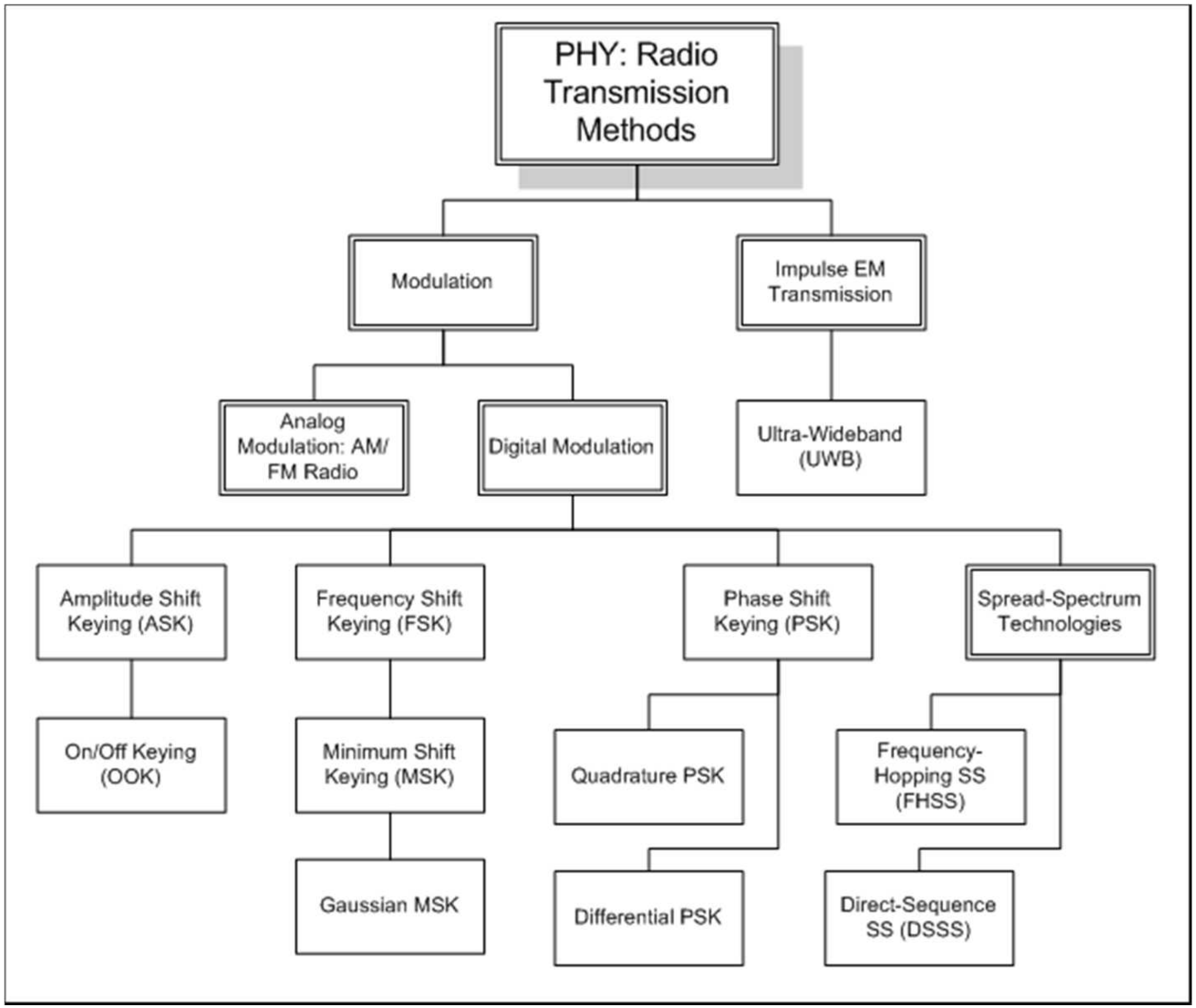
- Distance vector routing passing routes through the network for selection,
- Link-state routing passes neighbor-to-neighbor link status messages for each device to build a network topology and then create routes from it

Routing Protocols: Network Layer



Sandia National Laboratories

Physical Layer



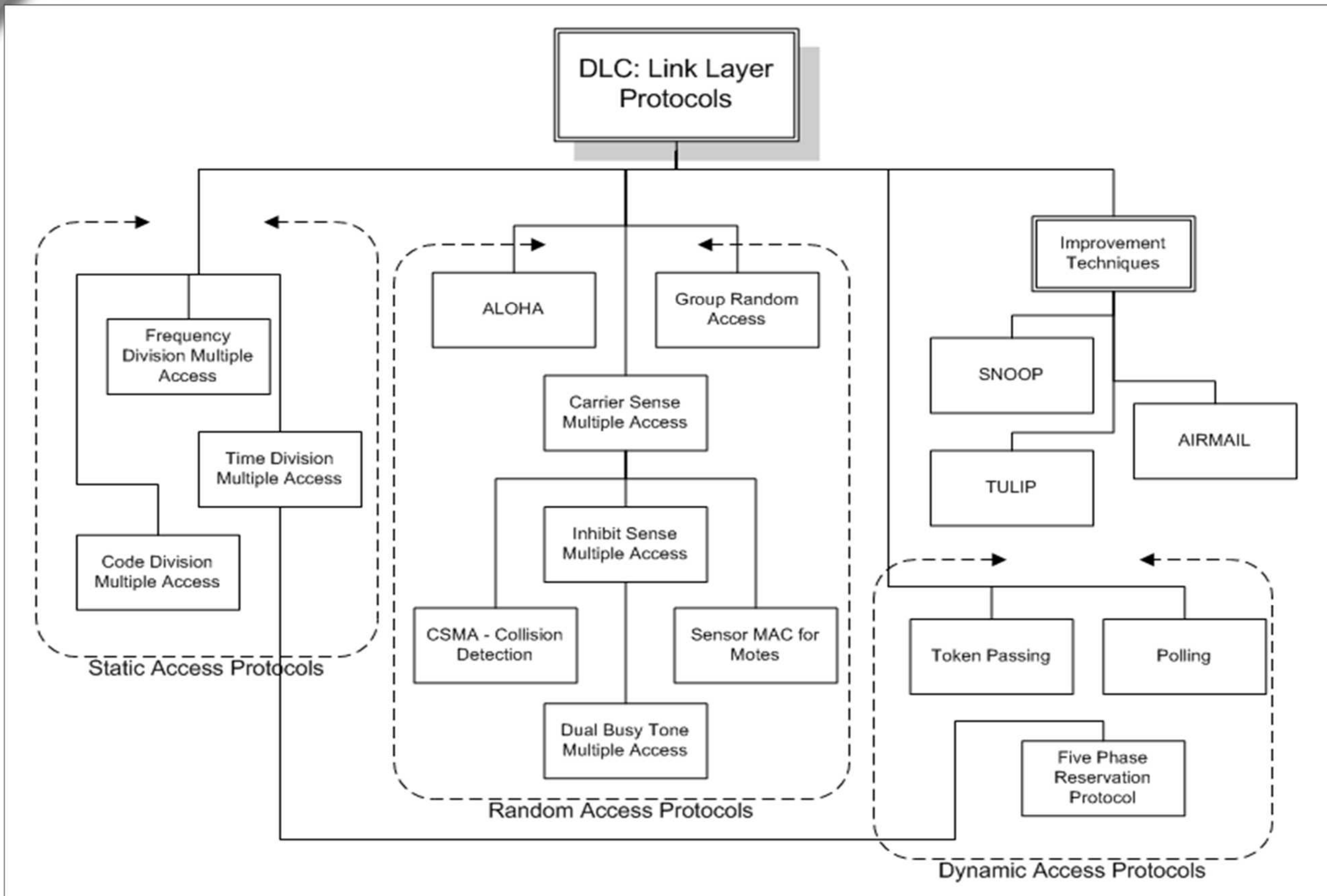
Sandia National Laboratories

PHY Layer Design Concerns

Selection and design of PHY layer are affected by:

- Power – efficiency, transmit distance, power per bit
- Bandwidth – range of frequencies used
- Interference – susceptibility to signal degradation
- Throughput – efficiency of data encoding and data rate
- Security– detection, interception, and jamming
- Implementation – physical and conceptual complexity, cost

Data Link Layer/MAC



DSL Layer Design Concerns

Selection and design of DSL layer are affected by

- Throughput – efficiency of channel utilization for data transmission
- Fault Tolerance – interference, collision, fading, or other problems
- Overhead – medium usage, computation, and storage
- Latency – data transmission time, average and maximum
- Security – may be inherent or designed in the node