SAND2007-0839P

The Design Process for a Border Monitoring System

Ruth Duggan

Global Security Programs (GSP)
Sandia National Laboratories

March 2007

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Role of Technology in Border Monitoring

- Detect illegal border crossings
  - Terrorists
  - Smugglers
  - Illegal immigrants
- Detect threats to fixed sites
  - Military outposts and bases
  - Other infrastructure
- Reduce risk of accidental conflict
- Potential to enhance bilateral or regional confidence

Considerations in a Monitoring System

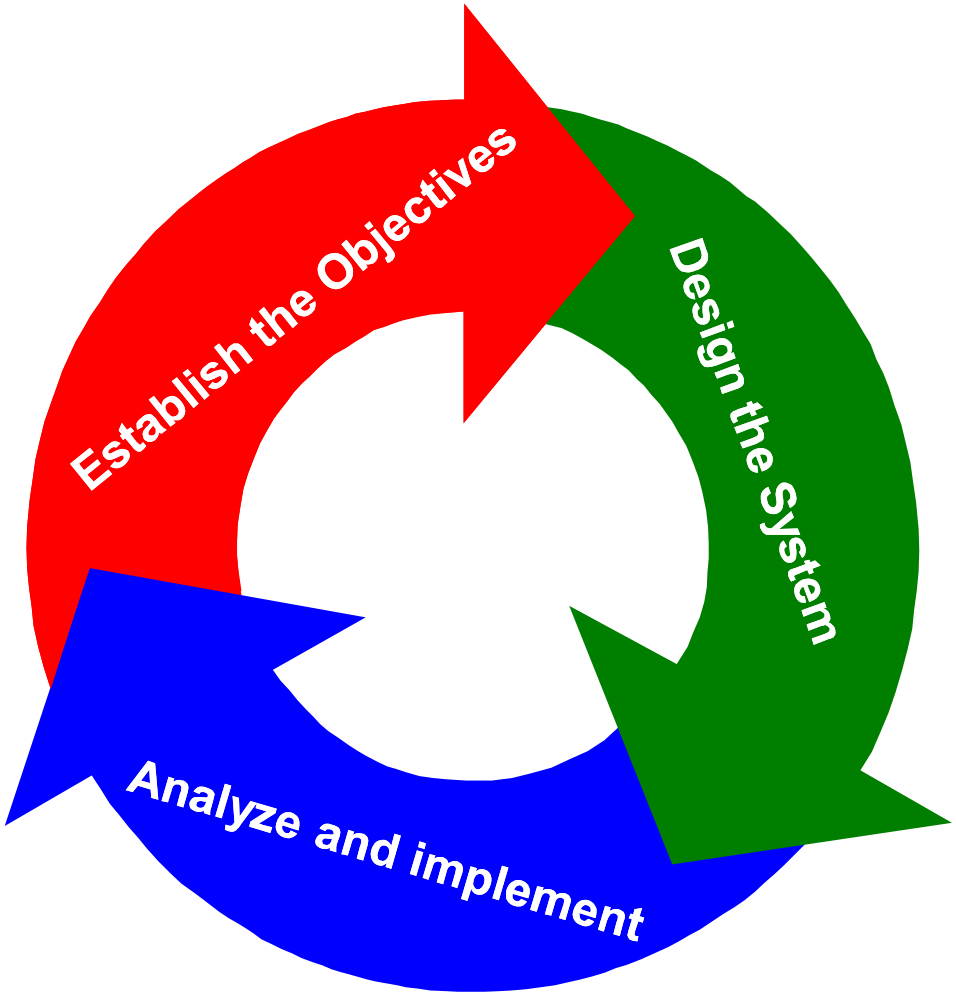
- Technologies and procedures must be evaluated from a systems perspective - understanding their benefits and limitations within the context of the threat being addressed.

- Effective system operation is a complex problem
  - It is not just an equipment problem; it is also a procedural and operational problem
  - Detection and deterrence will not be effective if the equipment is not adequate or if the operations, procedures, and response are not adequate
  - A monitoring system must be sustainable
    - Infrastructure
    - Maintenance and training

The Value of a Systems Approach to Design

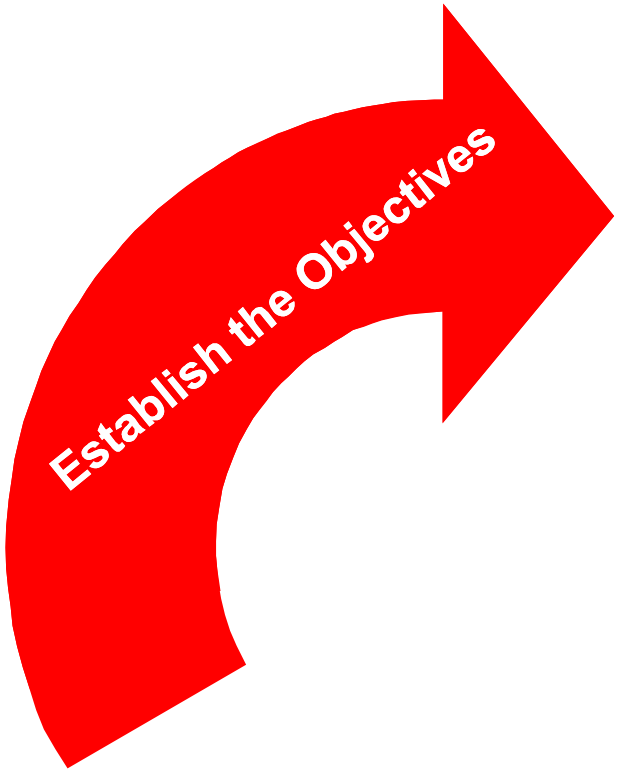
- **Without a systems approach:**
  - **Objectives of a system are not clearly defined.**
  - **Solutions may solve the wrong problem.**
  - **Solutions may provide little or no reduction in risk.**
  - **Cost effective solutions may be overlooked.**
  - **Resource allocations or resource requests are difficult to make and justify.**

The Monitoring System Design Process



Sandia National Laboratories

The Monitoring System Design Process



Sandia National Laboratories

A formal assessment of the threats provides the basis for security system design

- Threat assessment
  - An analysis that documents the credible motivations, intensions, and capabilities of potential adversaries that could cause undesirable consequences
- The value of defining a “Design Basis Threat” (DBT)
  - Making and justifying potentially expensive decisions
  - Establishing functional goals for the monitoring system
  - Evaluating the adequacy of the monitoring system
  - Provides a rational basis for:
    - Testing
    - Determining the need for countermeasure modifications
    - Identifying organizational responsibilities

Developing a DBT: Nine Steps

1. Identify the roles and responsibilities of all organizations
2. Develop the assumptions for use with the Threat Assessment
3. Identify categories of external and internal threats
4. Identify what we need to know about the threat
   - motivations, intentions, and capabilities
5. Identify sources of threat-related information
6. Collect and organize threat-related information
7. Formalize the threat assessment and gain consensus among participants
8. Define a DBT from the threat assessment
9. Introduce the DBT into border security operations

An Example Threat Assessment Matrix

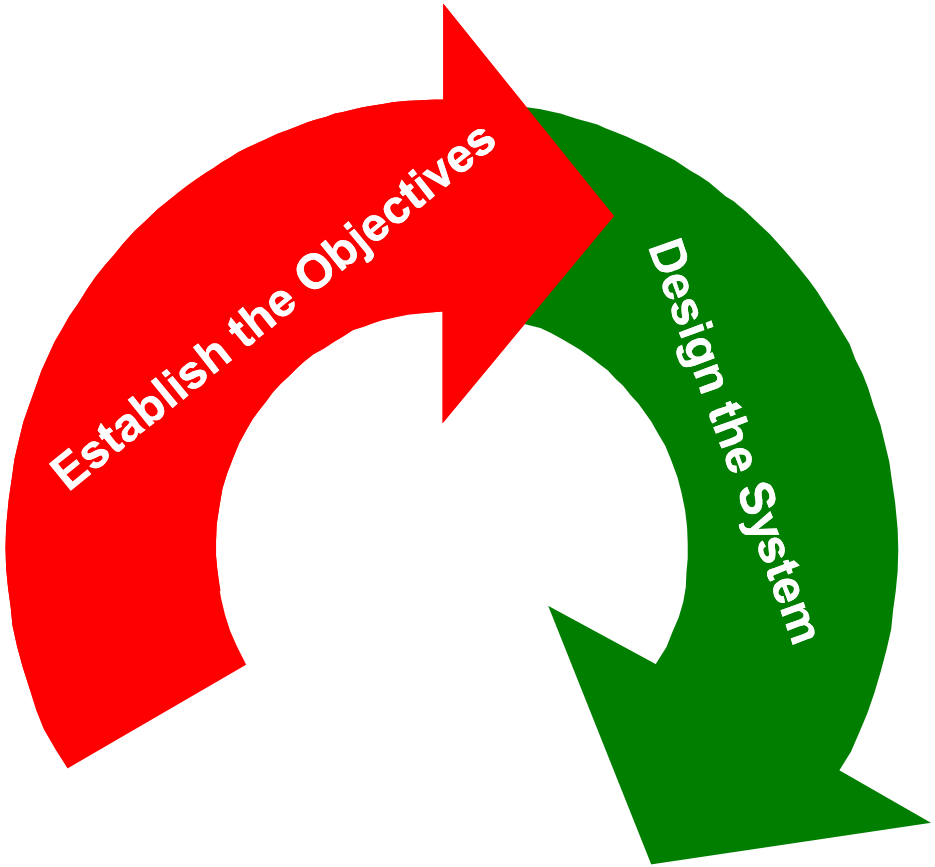
	EXTERNAL THREAT		
	Protestors	**Terrorists**	**Criminals**
MOTIVATION			
INTENTIONS Theft or Sabotage			
CAPABILITIES			
NUMBERS			
WEAPONS			
EXPLOSIVES Type & amount			
TOOLS Power or hand tools			
TRANSPORTATION Ground, air, water			
TECHNICAL SKILLS			
FUNDING			
INSIDER COLLUSION			
SUPPORT STRUCTURE			
OTHER			

Fundamental Questions:

How does my design balance risk?

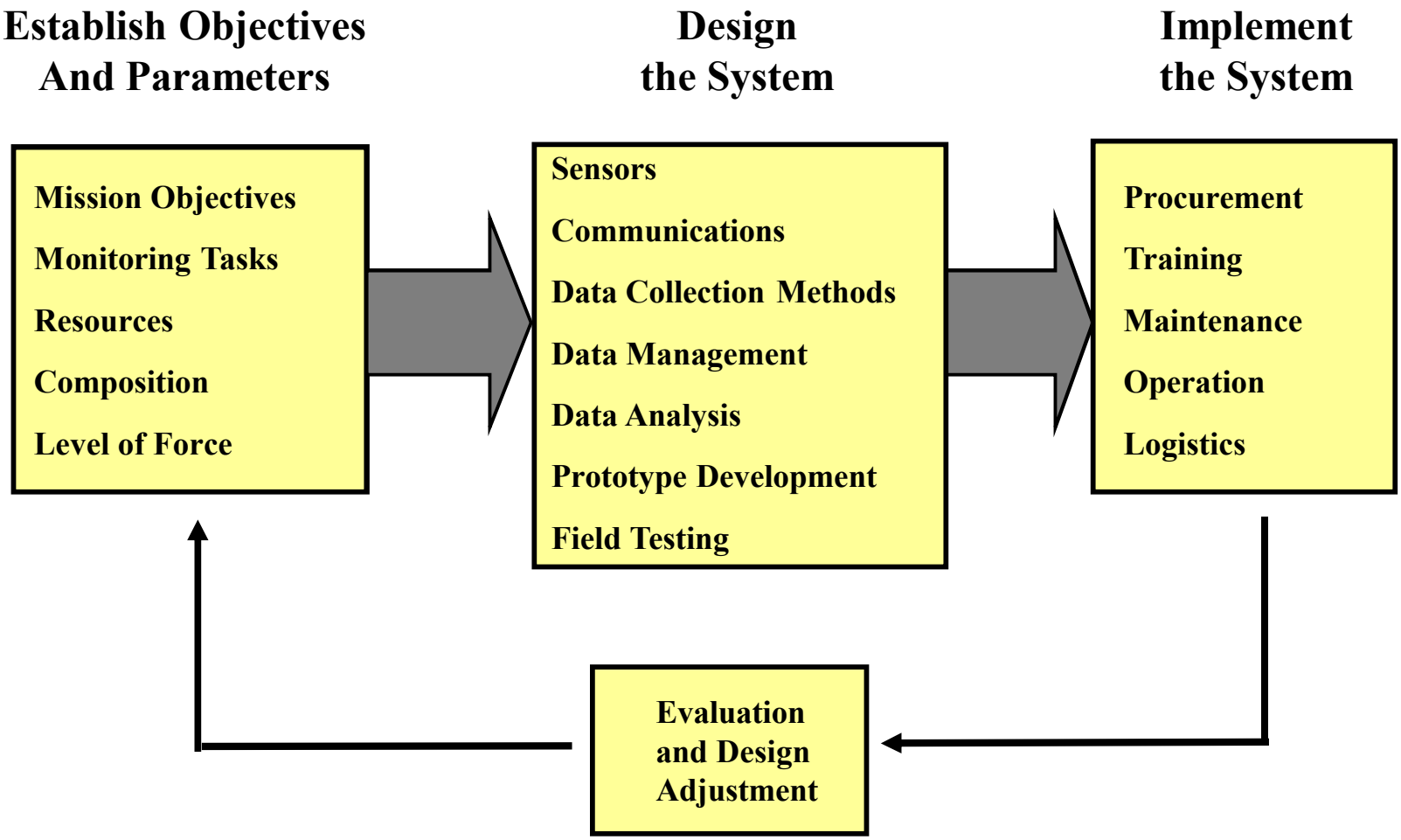
How to conduct operations?
How much to spend?
What to buy?

The Monitoring System Design Process



Sandia National Laboratories

System Design and Implementation



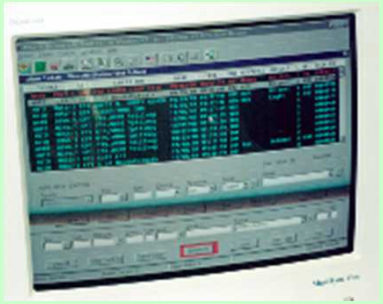
Elements of a Monitoring System

Sensor Systems

Site-Specific Monitoring System

Communications Systems

Video Systems

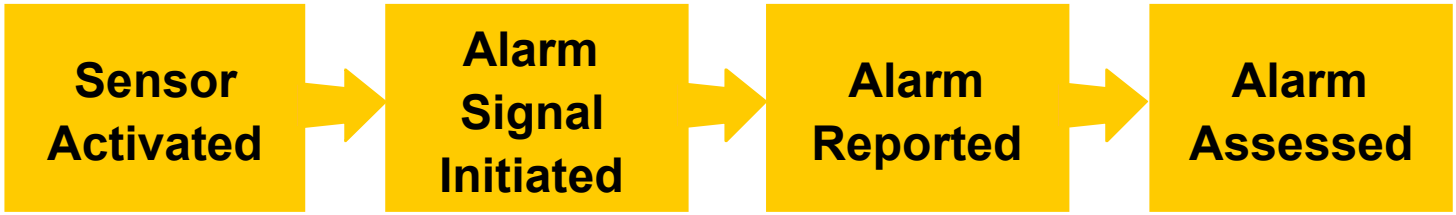


Data Management Systems

Command Center

Systems Integration of all Elements

Functional Steps in a Security System: Detection



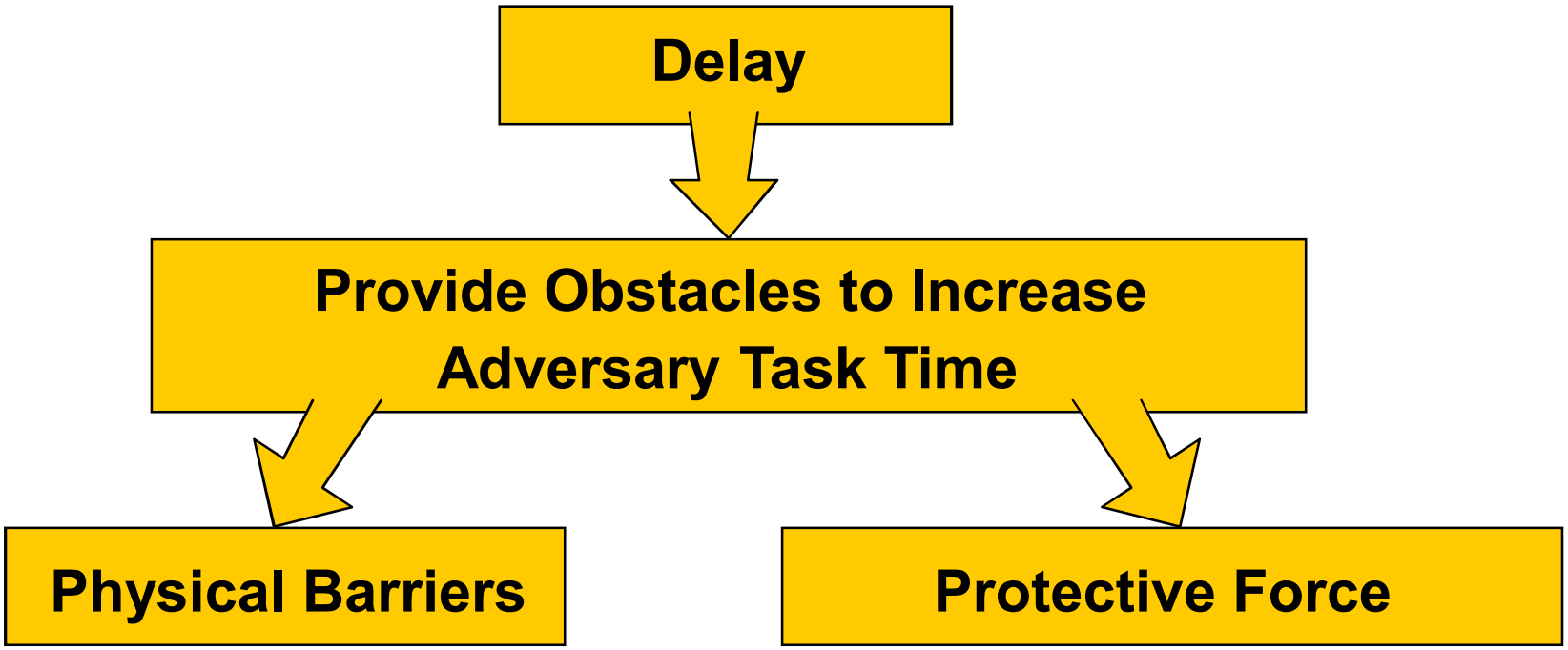
- Performance Measures
  - Probability of detection
    - Time for communication and assessment
    - Alarm without assessment is not detection
  - Frequency of nuisance alarms / false alarms
  - Vulnerabilities

Where in the sequence below does detection take place?

- Sensor alarm signal is generated
- Alarm signal is transmitted to console
- Operator is alerted by the incoming alarm
- Operator scans detection zone of alarming sensor for the cause (either visually or with video)
- In searching for the cause of the alarm, the operator observes an unauthorized person in the area
- The operator notifies the response force, describing the nature and location of the intrusion
- The security response force interdicts the intruder

Functional Steps in a Security System: Delay

- Performance measure: Increase time available to defeat threat
  - Create delay and/or increase early warning of intrusion



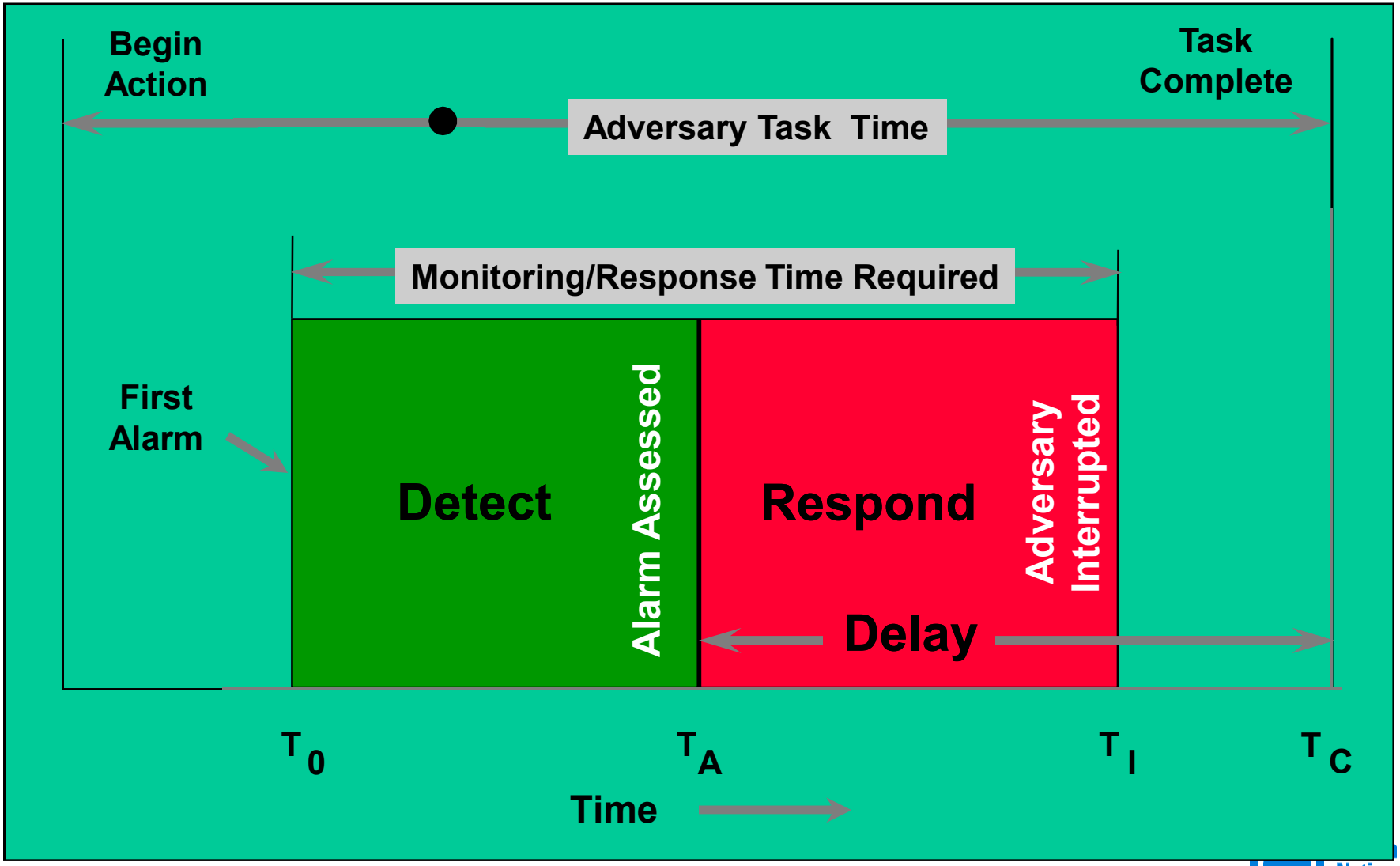
Delay Test Video

Sandia National Laboratories

Functional Steps in a Security System: Response

- Performance measures
  - Probability of communication to response force
  - Time to communicate
  - Probability of deployment to adversary location
  - Time to deploy
  - Response force effectiveness

Adversary Task Time vs. Monitoring/Response System Time Requirements



Monitoring System Design Requires a Balance of Priorities to Select Options

- Number and Skill Sets of Personnel Required to Run a System

- Communication and Power
  - Availability
  - Reliability
- Cost of a System
  - Installation and Operation

- Maintenance
  - Appropriate access
  - Reliability

- Confidence in System
  - Timeliness of Report
  - Redundancy

Sandia National Laboratories

Site-Specific Monitoring Systems

Integrated sensor systems to meet specific monitoring goals.

- **Use multiple complementary sensor types**
- **Sensors functions: detection, screening, assessment**
- **Sensor Characteristics**
  - **Probability of Detection**
  - **Nuisance alarm rate**
  - **Vulnerability to defeat**
- **Appropriate resolution of information collected**
  - **Geographic Area**
  - **Specificity of measurements**
- **Role of security personnel**

Operational Considerations in the Design of Monitoring Systems

- **Area Characterization**
  - Terrain and weather
  - Wildlife and vegetation
  - Normal activity at location

Sandia National Laboratories

Functions of a Monitoring Station

Data collection and information management

- **Data display and review**
  - **Text-Based**
  - **Graphical**
  - **Real-Time or Delayed Retrieval**
- **Data analysis and decision support**
- **Archiving of data**
- **Initiation of response to event**

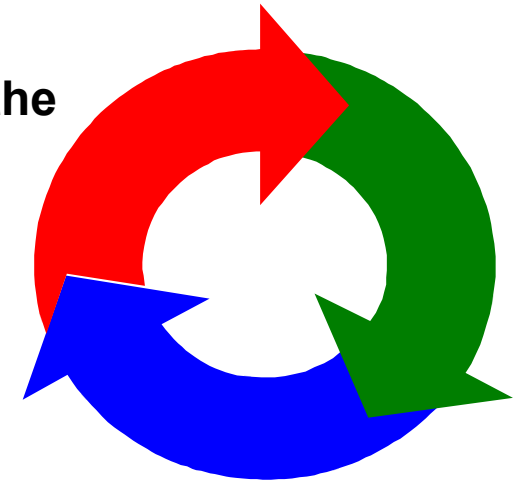
Communications Systems

Ensure the timely flow of information.

- **Types**
  - Remote access
  - On-site

- **Modes**
  - Direct connection by wire or fiber
  - Telephone - wire or cellular
  - Radio Frequency (RF)
  - Wireless Networks
  - Satellite
  - Internet
  - Combinations of above

Analyze, Implement, Analyze



- **Analysis:**
  - Functional Performance Testing
  - Field Testing
  - Performance Analysis
  - Vulnerability Analysis
  - Cost-Benefit Analysis
  - Modeling and Simulation

- **Implementation:**
  - Procure
  - Install
  - Test
  - Commission
  - Operate

A General Strategy for Border Monitoring

- Assess threats and set operational objectives
- Undertake systems approach to meet objectives
- Focus on significant activities and high-risk areas
- Balance cost with benefit
- Coordinate with various security systems
- Blend technical and non-technical types of monitoring
- Monitor in depth

Observations on Border Monitoring

- Monitoring technologies enhance the ability to detect cross-border movements
- A balance of human and technological solutions are needed
- Various sensor types are available for different applications, terrain and climate
- Using a combination of sensors to measure different signatures increases system effectiveness
- A systems approach to design is necessary to meet border security objectives
- Understanding the threat, your objectives, and operational constraints are key starting points in a systems design process
- Cooperation can enhance effectiveness of a system by providing early detection and greater response time as well as building confidence between parties on both sides of the border.

Analysis Slides

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Testing Methodology

- Evaluation Categories
  - Ease of installation
  - Adequacy of documentation
  - Detection capability
  - Nuisance and false alarms
  - Vulnerability to defeat
  - Adaptability
  - Maintenance required
  - Special requirements
  - Manufacture's support

  - Suggest changes is appropriate

Functional Testing Methodology

- **Functional Type Test (FTT)**
  - Evaluate “as built” specifications
  - Conduct bench tests to verify nominal performance
  - Use national Standards as applicable
  - Explore environmental limitations using laboratory facilities
  - Evaluate ease of installation/use
  - Examine documentation sufficiency
  - Produce preliminary gap analysis
    - What is the system missing to meet requirements?

Performance Testing Methodology

- **Performance Type Test (PTT)**
  - FTT completed
  - Use national Standards and system performance requirements
  - Test in representative operational environment such as Outside Test Facility
  - Determine performance such as
    - Probability of Detection (P_D)
    - Nuisance Alarm and False Alarm (NAR/FAR)
    - Degradation factors
    - Operational environmental effects
  - Test and assess defeat mechanisms
  - Amend gap analysis as appropriate
    - Again, what is the system missing to meet requirements?

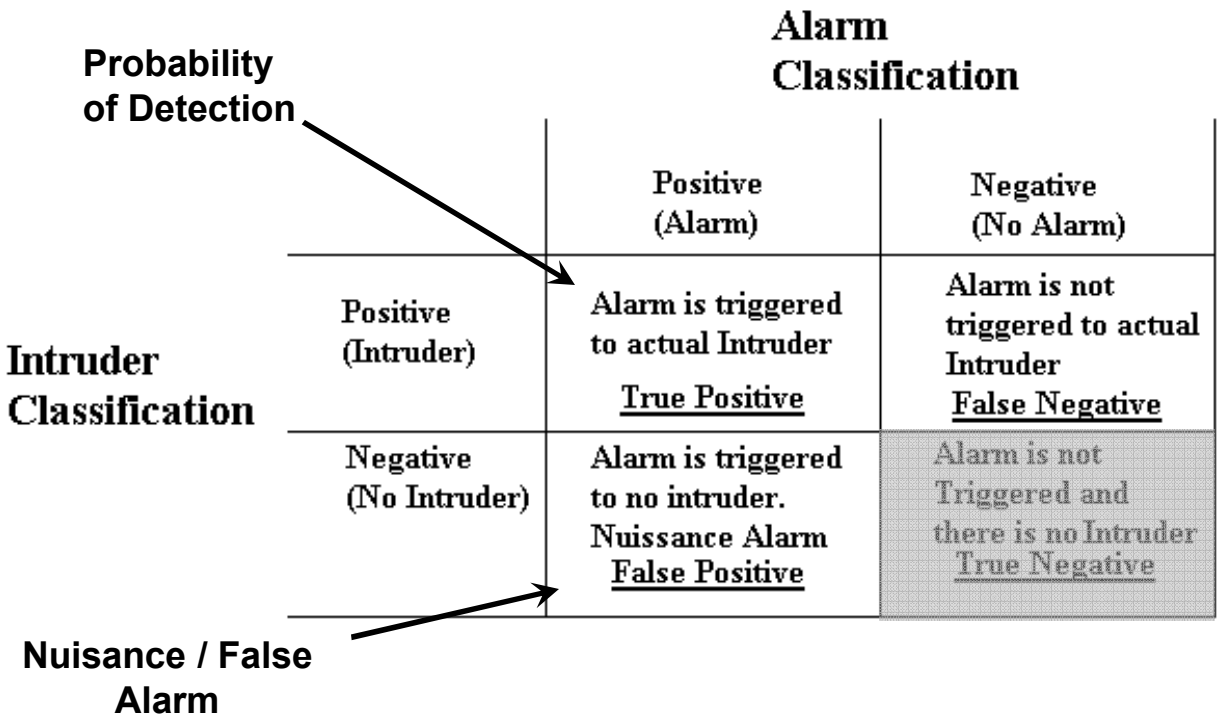
Performance Testing Methodology (continued)

- **Performance Testing**
  - ***Probability of Detection* (Pd)**
    - **Provides an indication of sensor performance in detecting intruder within sensor coverage**
    - **Involves characteristics of the sensor, environment, method of installation, method of installation and the assumed behavior of an intruder**
  - ***Nuisance / False Alarm Rate* (*NAR/FAR)***
    - **Indicates the expected rate of occurrence of alarms which are not attributable to intrusion**
    - **A *nuisance alarm* is an alarm event which is not caused by an intruder. Alarm is triggered by both natural and industrial environments**
    - **A *false alarm* is a nuisance alarm that is generated by the equipment itself (poor design, inadequate maintenance, or component failure)**
  - ***Vulnerability to Defeat***
    - **Bypass – all sensors have a limited detection zone, any sensor can be defeated by going around its detection volume**
    - **Spoofing – any technique that allows the intruder to pass through the detection zone without generating an alarm.**

Testing Methodology

- System Type Test (STT)
  - FTT/PTT complete
  - Place in system suite for full scale tests
    - Fit and form
    - Interoperability
    - Compatibility
    - Usability by border security personnel at operational locations
  - Evaluate for conformance to overall system design

Data Analysis & Probability of Detection



$$\text{Probability of Detection (Pd)} = \frac{[\text{True Positive}]}{[\text{True Positive + False Negative}]}$$

True Positive: Amount of actual alarms activated
False Negative: Amount of alarms that did not activate when there was an intruder

Completed Test
Seismic Sensor System

Statistical data on Seismic Sensors:	
Total Test run on Seismic Sensors:	260
Probability of Detection ($P_{d\text{-}Ideal}$):	85.34%

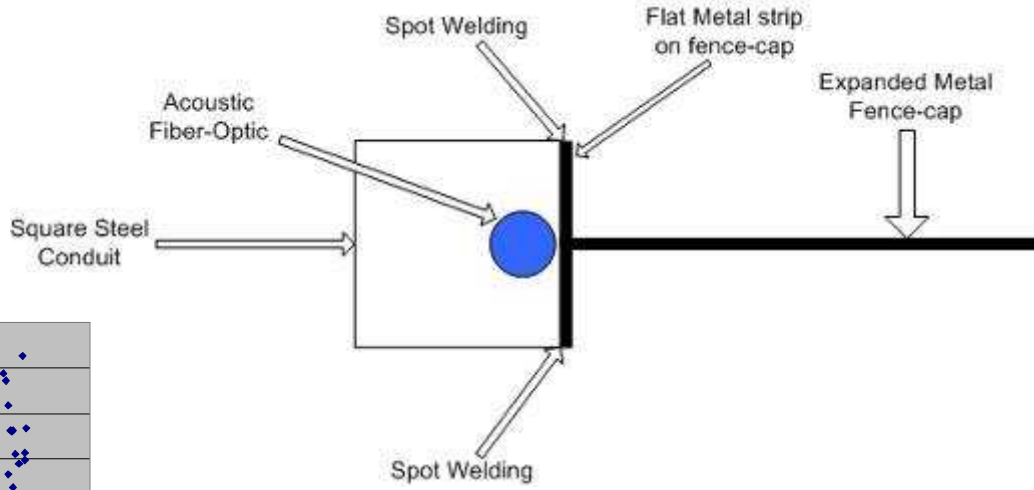
Average Circle of Detection:	
Human Walking:	6.14 meters
Human Running:	14.14 meters
All Terrain Vehicles:	19.25 meters
Truck:	22.67 meters

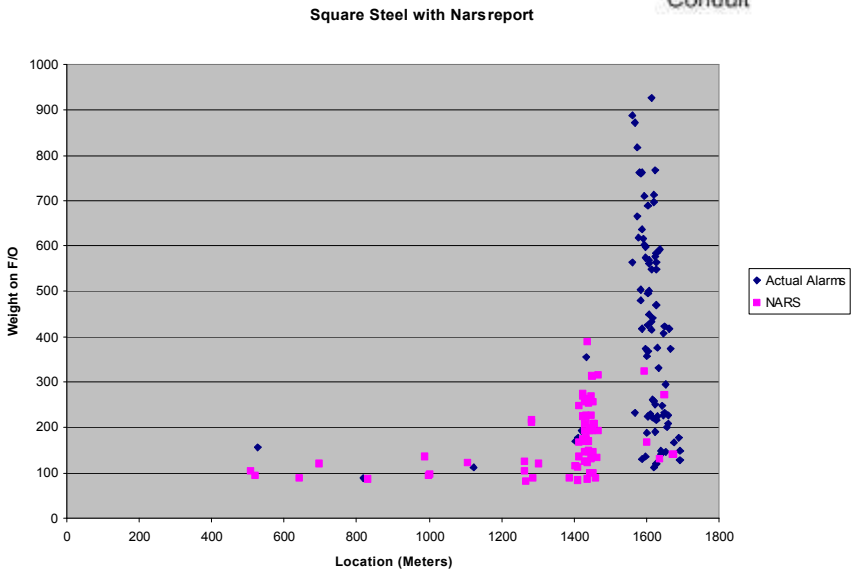
Completed Test
Acoustic Fiber-optic Sensor on Fence-Line

Square Steel on Border Patrol Fence:

Statistical data on Chain-Link Fence Configuration:	
Total Test run:	120
Probability of Detection ($P_{d\text{-}Ideal}$):	92.31%
Average Nuisance Alarm Rate	44%

Location capability:	
Location for Alarm	1579 Meters
Standard deviation from Actual Alarm	162 meters





Sandia National Laboratories

Field Trials Along US-Mexico Border

Installation of fiber optic sensor system on barrier wall in Nogales, AZ POE

Sensor installation with USBP

Camera testing with USBP

Sandia National Laboratories

Video - Assessing the Alarm

Discrimination Categories

1. A discrimination level of **DETECT** indicates that the presence of an object is verified.
2. A discrimination level of **RECOGNIZE** indicates that the class to which the object belongs can be verified (light vehicle, heavy vehicle, personnel)
3. A discrimination level of **IDENTIFY** indicates that the object can be discerned with sufficient detail and clarity that the type can be specified. (car, truck, armed man vs unarmed child)

HLR	Observable Identification
3	No identification of movement within the FOV
7	Minimum Identification of movement within the FOV. Will not be able to identify between Vehicle, Animal, or Human. Will only be able to see movement within the area
10	Identification between vehicle and Human/Animal (Will not be able to identify between Human and Animal)
13	**Minimum Identification difference between Human and Animal. Identification of Vehicle Type (I.E. truck or small vehicle)**
16	Identification of Human clothing and Animal type. Identification of Vehicle model type and color.
20	Identification of Human characteristics – Male or Female.
23	Identification of Human characteristics – Gender, clothing, prominent facial features.
26	Identification of Human characteristics – Gender, Features and characteristics that can be used as evidence, and specific clothing types
30	Identification of Human characteristics – Identification of marks (tattoos) and clothing types (leather jack or cloth shirt)

System Compatibility

- Meet national communication requirements and compatibility
- Survive and work in various environmental conditions
  - Temperature ranges
  - Humidity
  - Rain
  - Snow
  - Elevation
  - Wind
  - Blowing sand

- Survive and work after transport
  - Ground, rail, air
  - Vibration, mechanical shock, acceleration,
- Security of the equipment / sensors
  - Covert installation
  - Protective measures to delay intruder from stealing or destroying before response force arrives
- System Reliability, Availability, Maintainability (RAM)
  - What is the Reliability of the system
  - Availability
    - Are there readily available spares
  - Maintainability
    - Mean Time Between Failures (MTBF)
    - Mean Time To Repair (MTTR)
- Life Cycle costs
  - How often need to replace system components

Sandia National Laboratories