SAND2010-1490P

Gathering Performance Data

11

April 30- May 19, 2006

Albuquerque, New Mexico, USA

Module Objective

- Identify the purpose and importance of different kinds of testing
- Describe probability of detection and confidence levels

Kinds of Testing

- Operability tests
- Performance tests
- Limited scope and whole system tests
- Evaluation tests

Operability Tests

- **Simple measure of integrity on a frequent basis**
  - Tests to check for significant malfunctions and continued operations
  - If the test fails, call maintenance and possibly take compensatory measures
- **Examples (each shift):**
  - Metal detectors
  - X-ray machines
  - One-quarter of the sectors in a perimeter

Performance Tests

- **Check equipment over planned range of operation**
- **Perform repetitive tests on a PPS element or sub-function to develop performance values and confidence levels**
  - Establishes or confirms the ability of a PPS element to meet a performance level
  - Provides comprehensive assurance of performance on a less frequent basis
  - Establish a baseline performance useful for design
  - Populate and validate analysis data

Performance Tests

- **When to do performance tests:**
  - On unknown equipment, to develop a baseline performance useful for a design
  - On critical system elements and sub-functions
  - After initial installation to verify element performance
  - After maintenance
    - New equipment has different characteristics
    - Control of spare parts may not be good
    - Documented to confirm performance
  - Periodically to verify element performance

Limited Scope and Whole System Tests

- **Used to determine or verify physical protection system performance**
  - Test sections of the system together
  - Conduct whole system tests
  - Done initially and when PPS design changes
  - Identify areas of weakness or substandard performance in relation to design standards

Limited Scope and Whole System Test Examples

- Response force times to a particular target
- Probability of detection of contraband items during vehicle searches
- Verifying that an alarm can be initiated, communicated, annunciated, and assessed
- Force-on-Force exercise

Evaluation Tests

- An independent or 3rd party evaluation to verify effectiveness of the physical protection system
- Regulatory Authority may conduct to verify the facility evaluation
- May be used as an element of licensing program

Test Categories vs. Application Level

	Component Level	Sub-System Level	System Level
Operability Tests	x	x	
Performance Tests	x	x	
Limited System/ Whole Systems Tests	x	x	x
Evaluation Tests 3rd Party Validation	x	x	x

x Reflects Emphasis of This Test Category

Testing Guidelines

- **Define the test objective**
- **Plan the test**
- **Control the test**
  - Ensure realism
  - Minimize variables
- **Collect the necessary data**
- **Safety and Security**

Planning Activities

- **Determine test objectives**
- **Document the plan and test procedures**
- **Obtain approvals and provide coordination**
- **Determine how to test considering**
  - Design Basis Threat
    - Adversary strategies and tactics
  - Simulation of adversary actions
  - Environmental conditions that may affect the test
- **Define Pass/Fail criteria**

Testing Criteria

- **How**
  - Type of test, specific testing techniques, test objective, realism, available resources
- **Where**
  - Test location may affect realism
- **When**
  - Time of test may affect realism
  - Operational hours versus non-operational hours
- **Number of each test**
  - Level of confidence in test results
  - Complexity of the test and the resources available

Obtaining Approvals and Providing Coordination

- **Performance tests may require**
  - Approval from appropriate management personnel
    - Facility
    - Response Force
    - Safety
  - Coordination with various organizations
    - Safety and health
    - Fire departments
    - Local police
    - Facility operations staff

Control Measures

- **Conducting an orderly and safe test requires the planning and enforcement of control measures**
  - Boundaries
  - Off-limit areas
  - Rules of conduct
  - Safety rules
  - Controller / trusted agent actions
  - Communications
  - Test initiation and termination
  - Site protection

Analyzing Test Results

- **Statistical analysis**
  - Probabilities and confidence levels
- **Subject matter expert judgment**
- **Lessons learned**

Determining How to Test

- **What factors affect testing?**
  - Performance will depend on
    - Adversary tactics, tools, and knowledge
    - Adversary size and speed
    - Environmental factors
    - Operational factors

Test scenarios must take these factors into account

Determining How to Test (cont'd)

- **What is the Design Basis Threat (DBT) and what defeat methods may be applied to this element?**
- **Categories of adversary action**
  - Run
  - Walk
  - Crawl
  - Use vehicle
  - Cut
  - Explosively penetrate
  - Deceive (falsify credential)

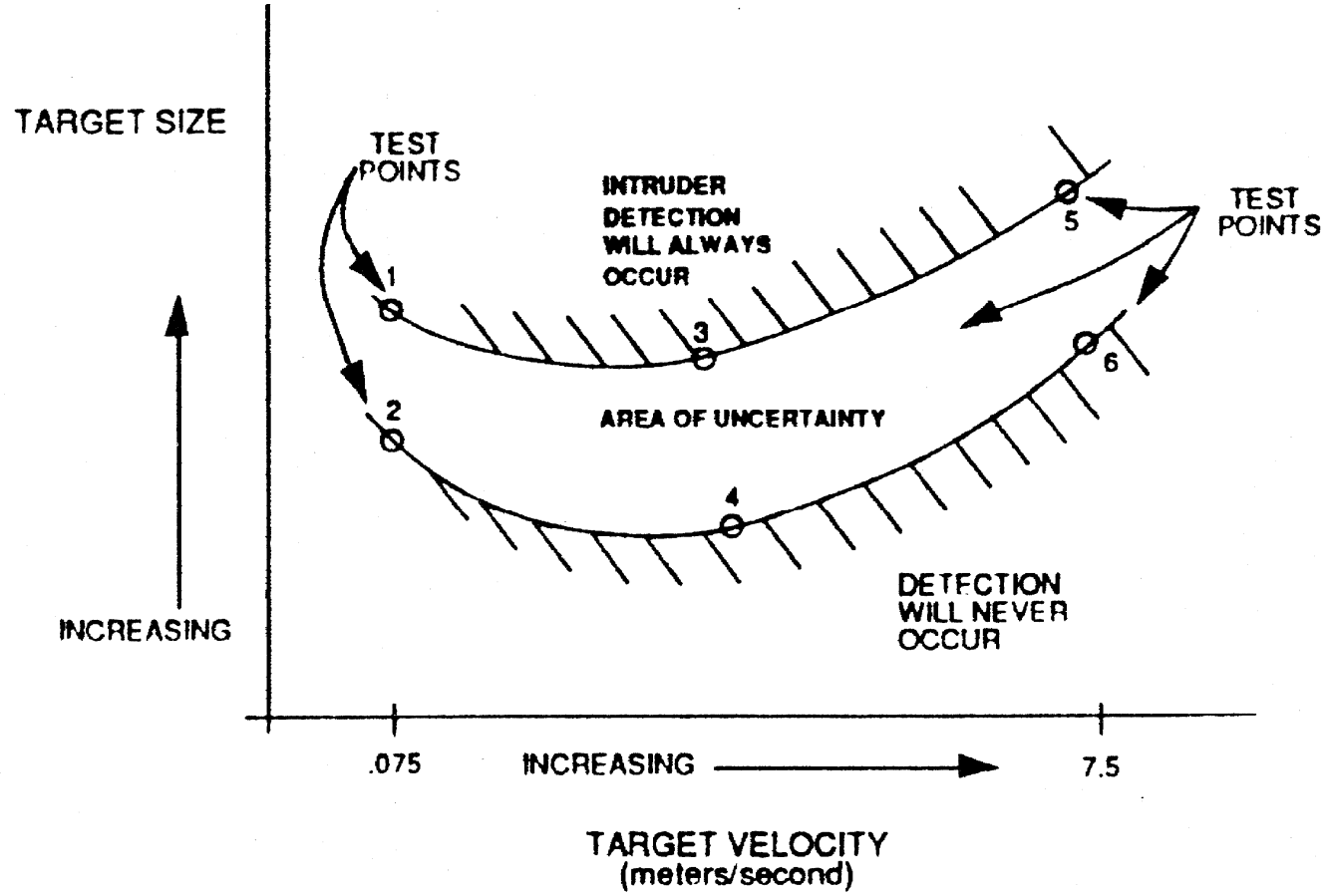
Determining How to Test (cont'd)

- **Conservative approach assumes skillful and cautious adversary**
- **Model and simulation of adversary actions**
  - Some actions can be directly modeled (e.g., runs and walks)
  - Some actions can be simulated by providing the sensor with a stimulus equivalent to the adversary action
    - cut top links of fence
    - hit the fence with a calibrated fence tester
    - aluminum sphere used for microwave crawl simulation

Determining How to Test (cont'd)

- **Environmental conditions**
  - Nuisance alarm sources and rates must be collected
  - Certain environmental conditions may be expected to degrade performance and should be tested
  - Examples:
    - Day/night, weather, vegetation, animals

Exterior Microwave Sensor Testing



MW Test Target

What Settings to Use

- Device calibration is a compromise between the following:
  - PD
  - Nuisance Alarm Rate
- The sensor or detector should be set at the lowest gain setting that provides the required performance

Detection and Confidence Levels

- **Testing strategies**
  - Set an acceptable performance standard
  - Set an acceptable confidence level
  - Conduct a reasonable number of tests
    - Importance of system element
    - Amount of time and resources available
  - Plan for one or more stopping points in the testing when reasonable P_D cannot be achieved

Probability of Detection Definition (P_D)

- **The likelihood that an intruder will be detected under a well defined set of conditions**
- **Example conditions:**
  - Intruder size is specified
  - Mode is specified:
    - Running, jumping, crawling, walking
  - Direction
    - Parallel or tangential to the detection volume
  - Speed range is given

Confidence Level

More testing provides a higher confidence in the accuracy of the results of the test

Usually expressed as a percentage

Detection and Confidence Levels

If a test plan assures a minimum 85% probability of detection with 95% confidence

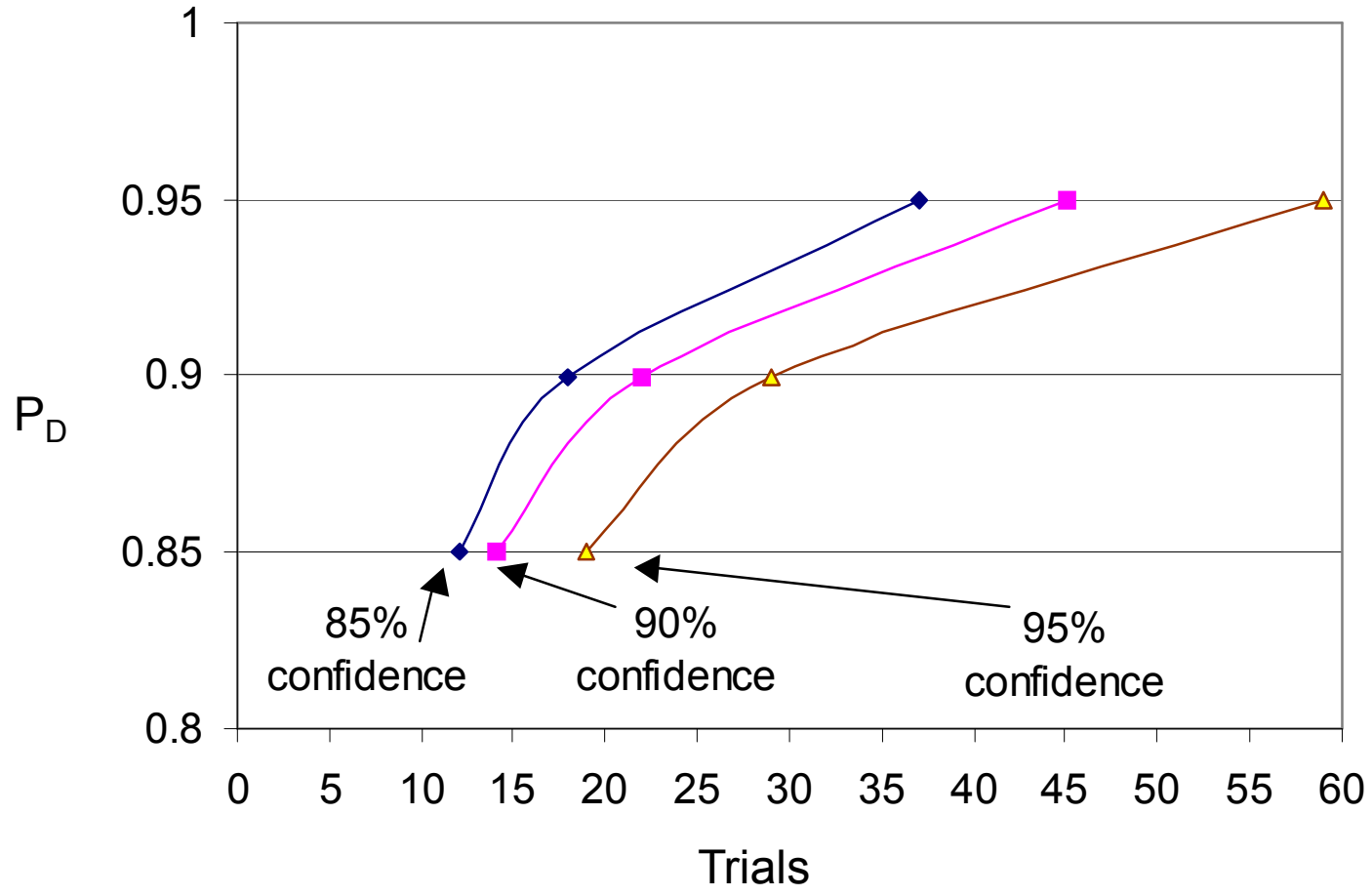
- **Then under the following conditions:**
  - Consistent conditions for a set of tests
  - Equipment is properly installed and maintained

Under these test conditions, the equipment successfully detects at least 85% of the attempts and will fail to detect no more than 15% of the time

The confidence that the equipment meets the criteria is 95%

(This means that 95% of the times we conduct this set of tests, the results will show at least PD of 85%)

Lower Bound for the Probability of Detection vs. Number of Trials (No Misses)



Detection (yes / no) vs. Signal Measurement

Yes/No Data

5 Consistent tests

4 Alarms (works)

1 No alarm

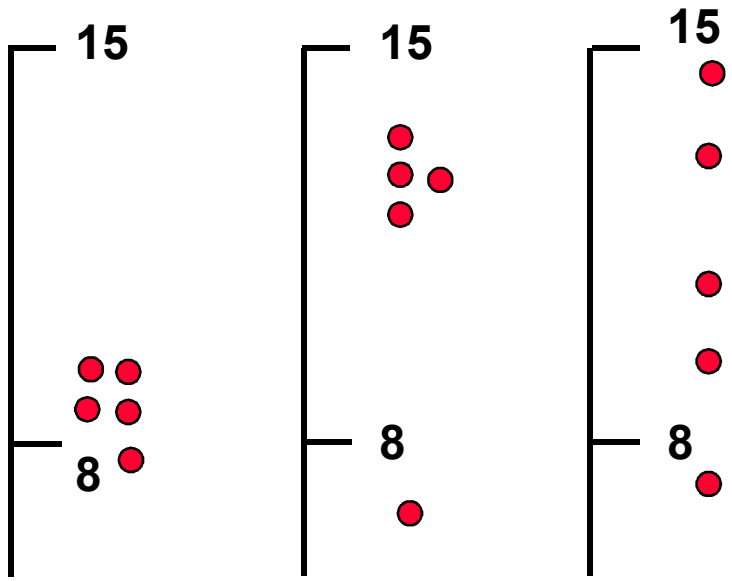
Estimate:

Works 80% of the time

95% Confidence – 34% P_D

90% Confidence – 42% P_D

Signal Measurement

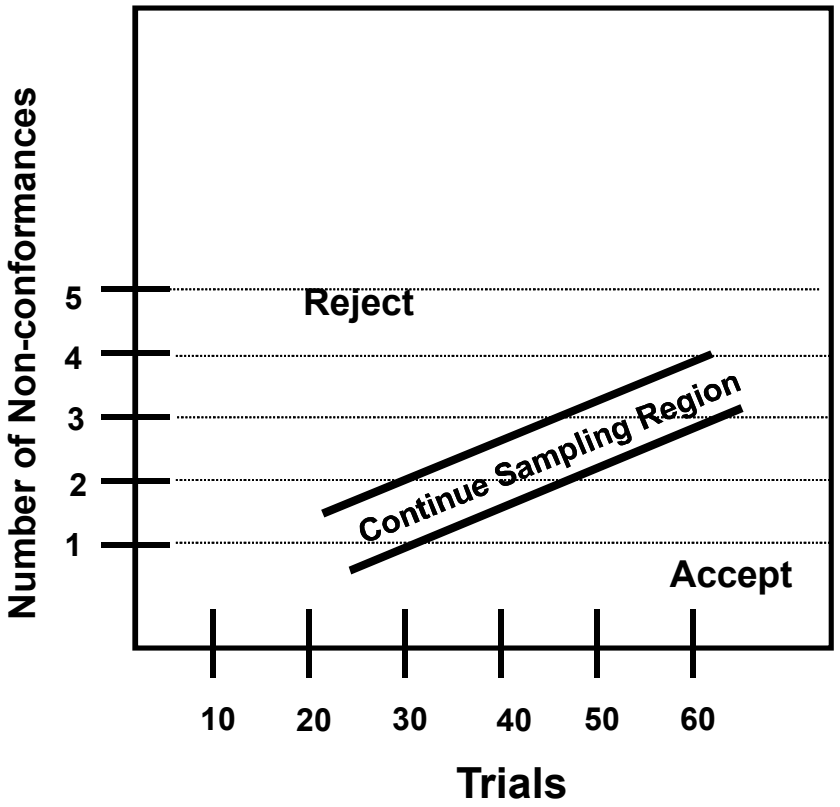


Detection (yes / no) vs. Signal Measurement

- **Detection**
  - requires more testing
  - treats equipment as “black boxes”
- **Signal measurement**
  - provides better assurance of performance quality
  - allows an assessment of the margin of conformance to requirements
  - allows better correlation between test conditions
  - makes alarms easier to analyze

Types of Detection (yes / no) Sampling

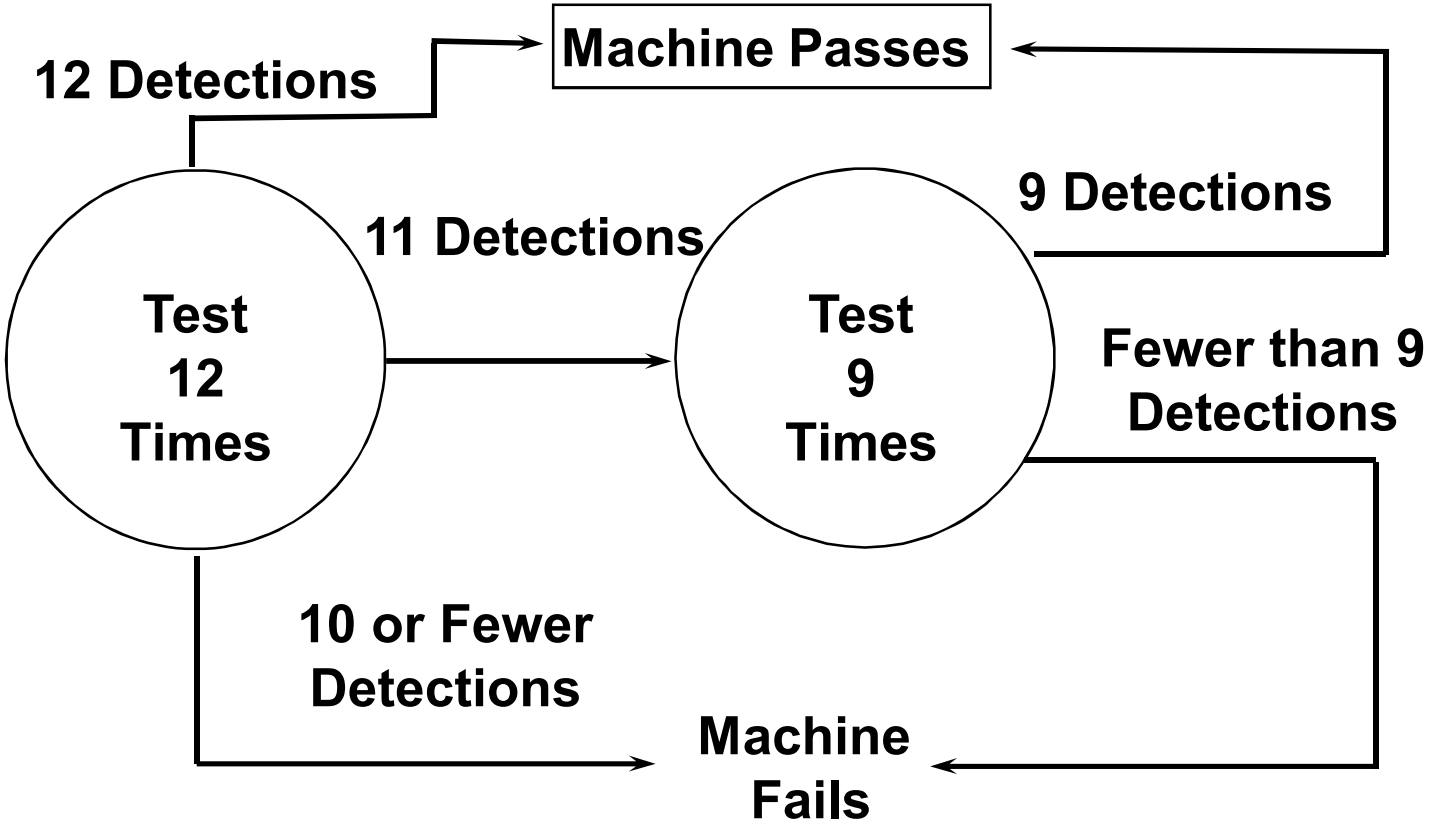
- **Single sampling**
  - Sample size
  - Acceptance number
- **Double sampling**
  - First sample size
  - Second sample size
  - Acceptance number for first sample
  - Acceptance number for both samples
- **Multiple sampling**
  - Extension of double sampling parameters



Single Sampling Tests Needed

Single Sampling Plan, No Failures Allowed									
P_D	**.85**	**.90**	**.95**	**.85**	**.90**	**.95**	**.85**	**.90**	**.95**
Confidence Level	**.85**	**.85**	**.85**	**.90**	**.90**	**.90**	**.95**	**.95**	**.95**
Sample Size	**12**	**18**	**37**	**14**	**22**	**45**	**19**	**29**	**59**
Single Sampling Plan, One Failure Allowed									
P_D	**.85**	**.90**	**.95**	**.85**	**.90**	**.95**	**.85**	**.90**	**.95**
Confidence Level	**.85**	**.85**	**.85**	**.90**	**.90**	**.90**	**.95**	**.95**	**.95**
Sample Size	**21**	**32**	**66**	**24**	**37**	**76**	**30**	**45**	**93**

Double Sampling Plan
(85% P_D at 85% Confidence Level)



Summary

- Performance testing is critical to a performance-based evaluation of a physical security system
- Adequate planning and effective execution ensure successful data collection
- Provides data for analysis tools

Back Up Slides

Samples of Variables, Test Matrices, and Results

Example 1: Radar System Test Variables

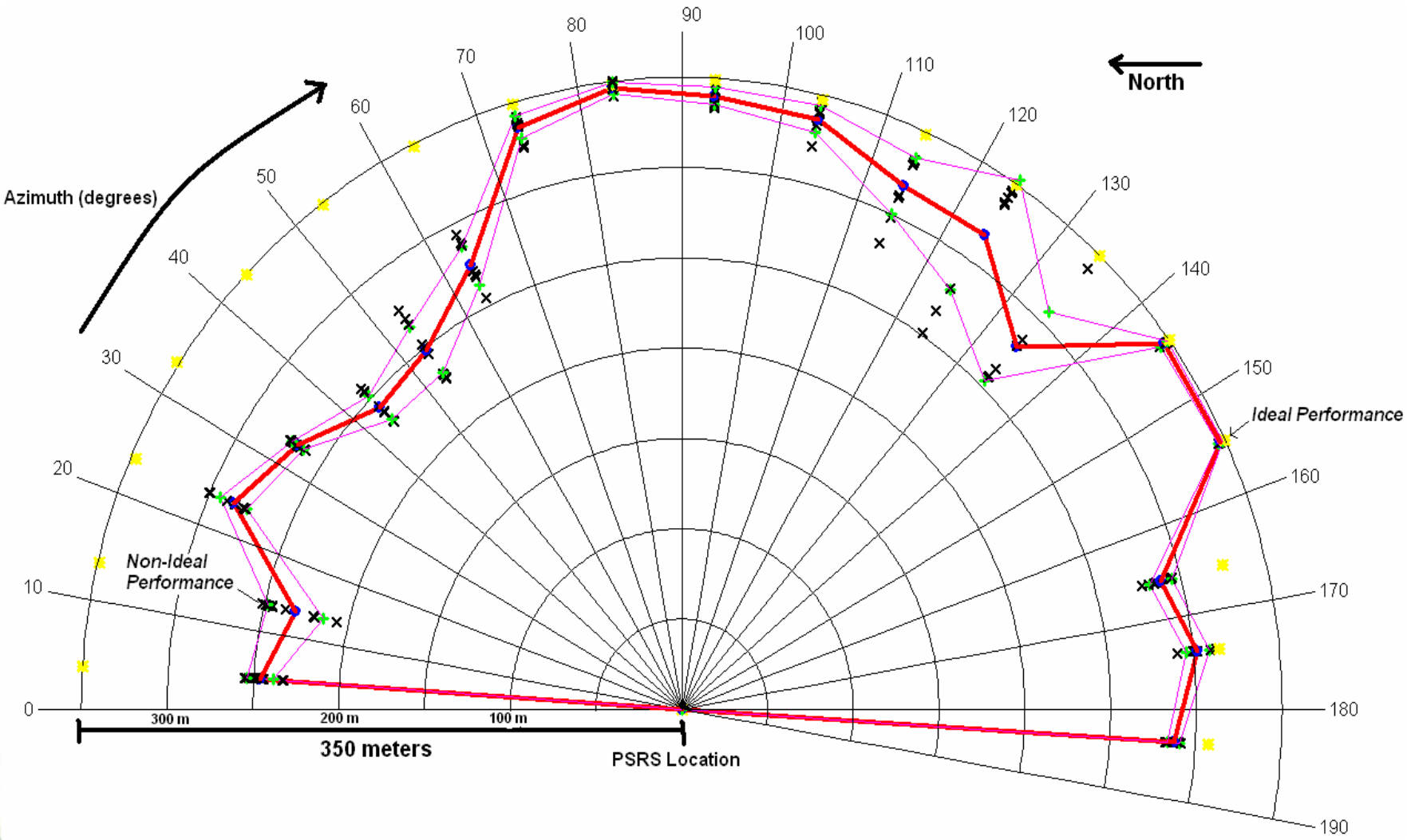
Variable – Controlled	
Threat Characteristics	at 2 feet per second (radials only) All-Terrain Vehicle (ATV) at speeds as fast as achievable in terrain (on likely paths approved by environmental survey) Vehicle (Sports Utility Vehicle) at 35 and 60 mph (on paved or packed roads) Note: the three subjects also represent differences in size, which can affect the radar cross-section.
Threat Vector	Radial test grid with radial paths every 10° Note: Tangential paths were not included in the test matrix.
Variable – Not Controlled	
Weather Conditions	Clear, rain, wind, hail (varied over time)
Terrain	Flat, mountainous, ravines, arroyos (varied with test location)
Foliage	Shrubs, Joshua trees, grass (varied with test location)
Fixed Parameters	
Radar Installation Details	Mounting height Tilt or vertical azimuth Coordinates of radar
Radar Data Acquisition and Alarm Criteria	Operating frequency Scan rate Number of consecutive radar hits required to declare an alarm condition Range setting Rain setting (to reduce nuisance alarms during rain) Minimum and maximum target velocity criteria Constant false alarm rate feature Spacial gain distribution Alarm threshold value

Example 1: Radar Test Matrix

	0º	10º	20º	30º	40º	50º	60º	70º	80º	90º	100º	110º	120º	130º	140º	150º	160º	170º
	30	5	5	5	5	30	5	5	5	30	5	5	5	5	30	5	5	5
ATV	0	30	0	0	0	0	10	0	0	0	0	0	10	0	0	0	0	0
Vehicle	0	30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	180º	190º	200º	210º	220º	230º	240º	250º	260º	270º	280º	290º	300º	310º	320º	330º	340º	350º	Test Total
	30[a]	5[a]	5[a]	5[a]	5[a]	5[a,b]	5[a]	5[a]	30[a]	5[a]	5[a]	5[a]	5[a]	20[b]	10[b]	5	5	5	**320**
ATV	10	0	0	0	0	0	10	0	10	0	0	0	0	0	0	0	30	0	**110**
Vehicle	10	0	0	0	0	0	0	30	30	0	0	0	0	0	0	0	0	0	**100**

Example 1: Radar Test Results



Example 2: PIR Test Variables

Direction of Intruder Approach

1. Radial
2. Tangential

Speed of the Intruder Approach

3. 0.5 ft/sec
4. 1.0 ft/sec

Intruder Profile

5. Walking upright
6. Crawling

Target Stature

7. Small—4'11" and 100 pounds
8. Large –6'0" and 200 pounds

Number of Units Tested (same make and model)

9. Unit #1
10. Unit #2

Mounting Height

11. 8 feet to 25 feet

Range Setting

12. 10 feet to 35 feet

PIR Sensitivity

13. High
14. Low

Microwave Sensitivity

15. Resistance on the Microwave Potentiometer

Example 2: PIR Test Matrix

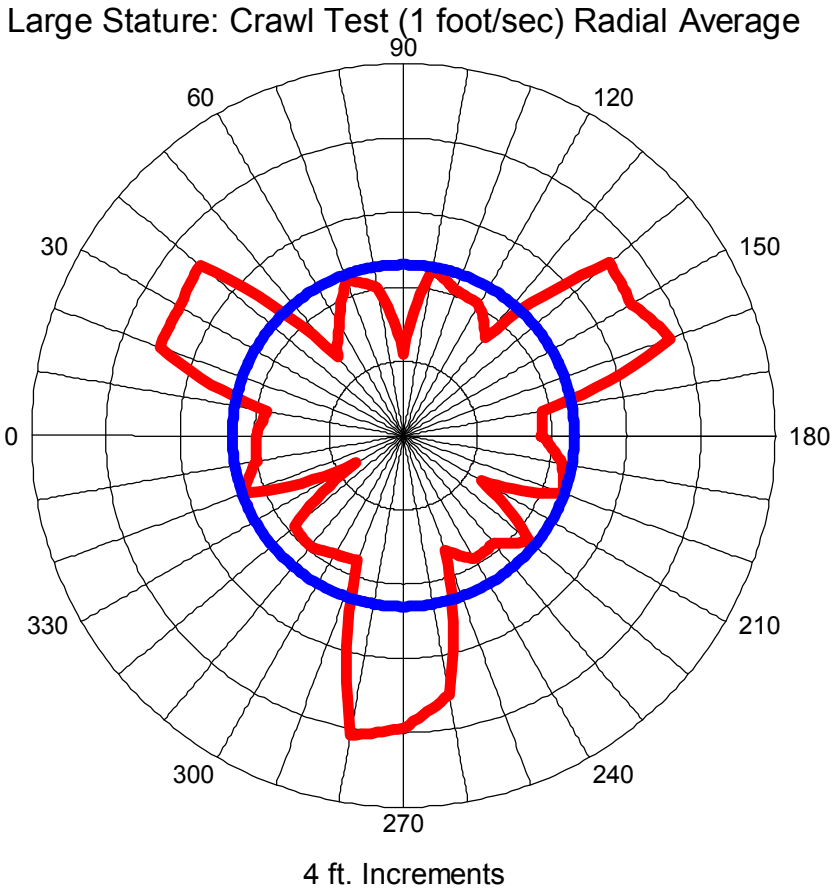
Radial Tests*	Unit #1		Unit #2		Total Number of Test Sets
	Small Stature	Large Stature	Small Stature	Large Stature	
0.5 ft/sec Slow Walk	10 sets	5 sets	4 sets	2 sets	21 sets
1.0 ft/sec Walk	10 sets	5 sets	4 sets	2 sets	21 sets
1.0 ft/sec Crawl	10 sets	5 sets	4 sets	2 sets	21 sets

* One set of radial tests consists of 1 test along each of the 36 radial transects, giving 36 data points.

Example 2: PIR Test Matrix

Performance Testing Allows Designers, Site Security Managers, and Decision Makers to make "Informed Decisions"

Average R = 9.2
Minimum R = 2.9
Maximum R = 16.4



Testing establishes performance characteristics not provided by the manufacturers

- *Degradation factors*
- *Vulnerabilities*
- *Nuisance and false alarm rates*
- *Reliability and maintenance Issues*

Backup Slides

Maturity Model

Maturity Model for Security Technologies

JR Russell

(505) 844-3865

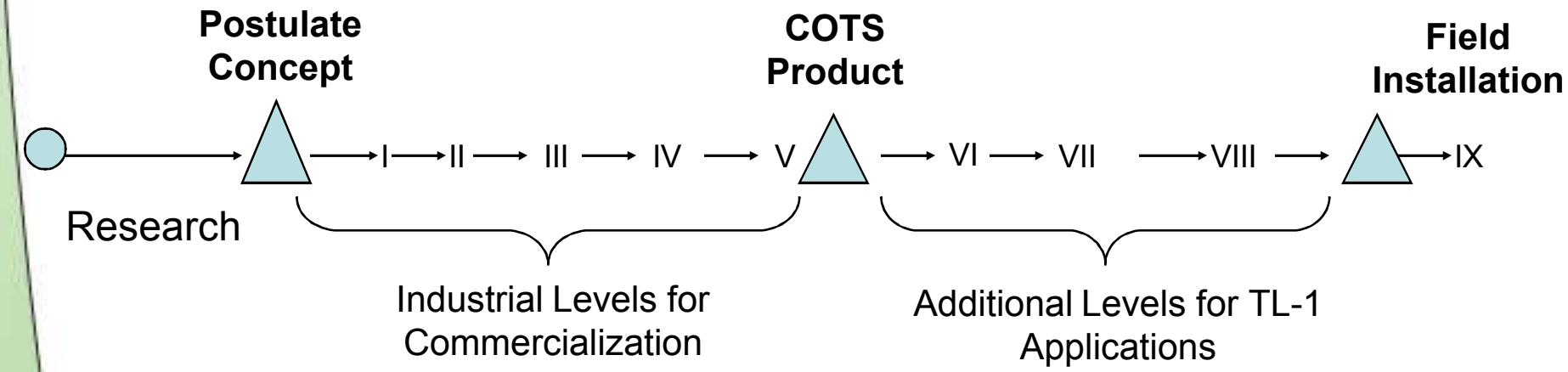
jlrusse@sandia.gov

Security Systems and Technology Center

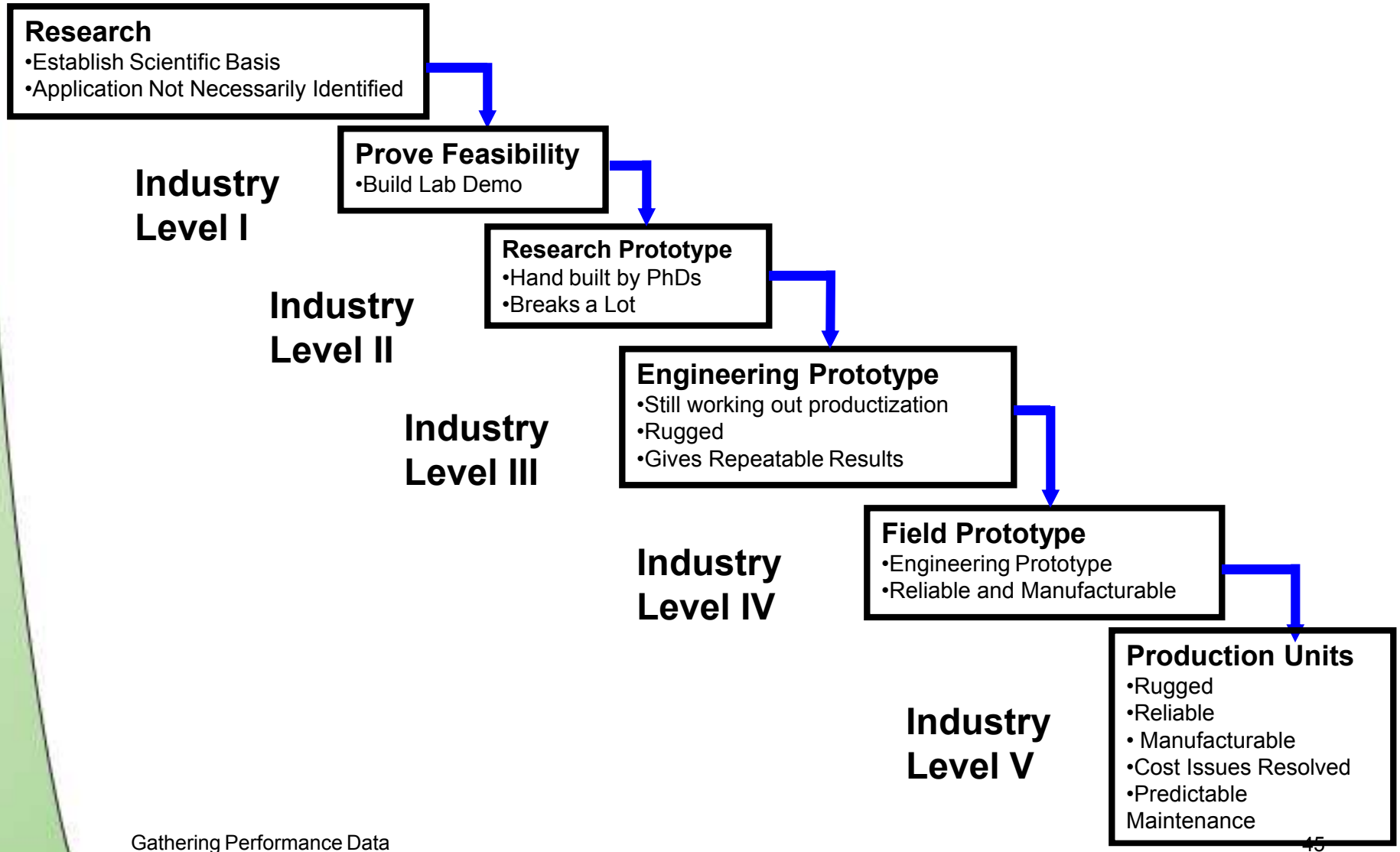
Sandia National Laboratories

Maturity Model for Security Technologies

Maturity Model For Emerging Technologies



Maturity Levels for Emerging Technologies



Maturity Levels for TL-1 Applications

Level VI

Performance Testing (3-12 months)
- Adequate Probability of Sensor Detection Ps, i.e. .9 at 95%
- Low Nuisance Alarm Rate
- Low Vulnerability to Defeat, tested against DBT
- Identify Degradation Factors
- Does not interfere with other equipment or itself, QUPID
- Enter Data Into Atlas Data Base

Level VII

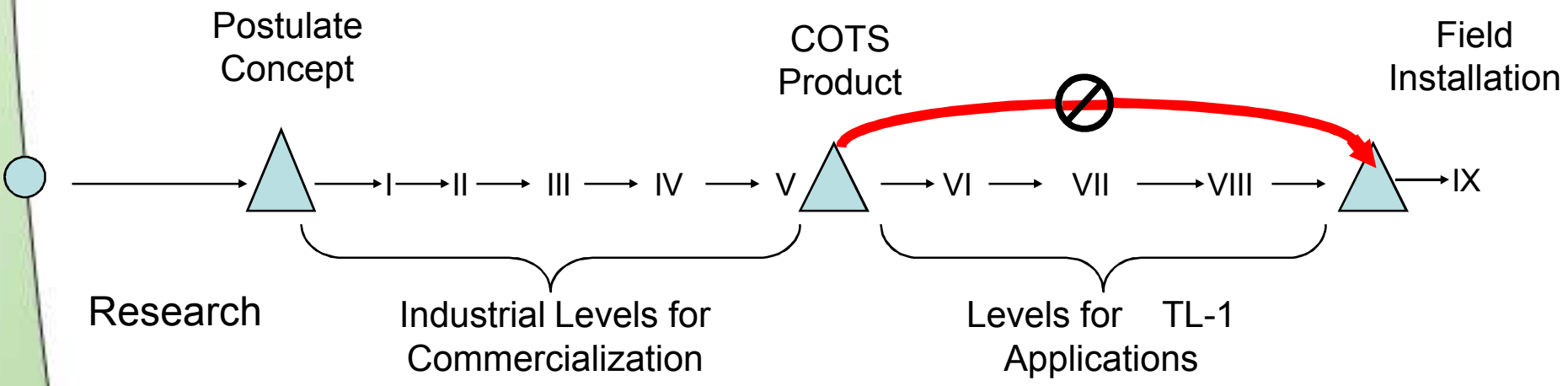
Tests Conducted Under Site Conditions
- Observe Degradation due to:
  - Foliage
  - Weather
  - Existing Operational Procedures/Integration
- Establish Reliability
- MTBF (failure)
- MTBR (repair)

Level VIII

Non-Technical Maturity Factors
- Vendor Stability
- Availability of Product/Parts
- Vendor or site has knowledgeable repair staff (do they have to come from Israel-- 9 weeks)
- Develop Concept of Operations
- DOE Policy Authorizing use of Technology and Concept of Operations

Maturity Model for Security Technologies
Closing Comments

If Maturity Levels are "skipped", the stakeholders incur Significant Risk



Technical Risk
Project Risk
Security Risk