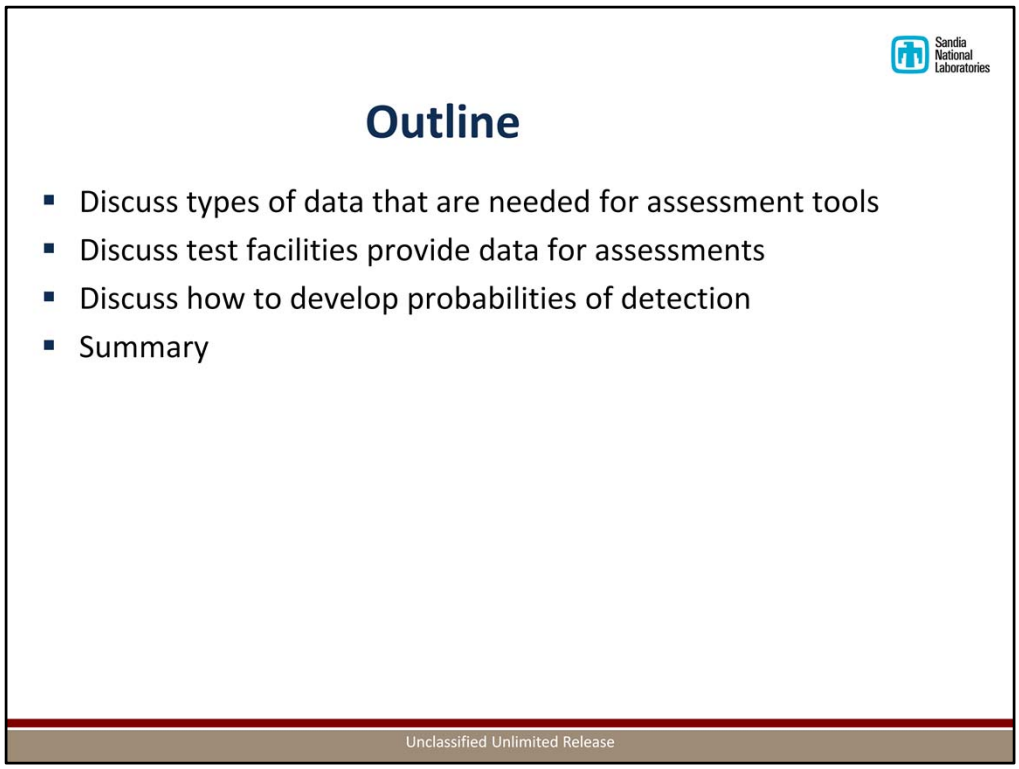
All material in this presentation comes from SAND2014-1920P (in the Legacy System)



Regarding this caution, Taleb, to his credit, remarks that we magnify certain black swans because we can visualize them, to the detriment of rationale thinking and other black swans that are harder to visualize. As he says, "After a Black Swan, such as 9/11, people expect it to recur when in fact the odds of that happening have arguably been lowered. " This relates to Kahneman and Tversky's work. Moreover, perhaps we are unintentionally making things worse… Perhaps we are magnifying the risk of an attack on a nuclear target

Sandia National Laboratories

Reality about Performance-Based Assessments

- Fact: Performance-based assessments require
  - Good performance data
  - Experts who can interpret that data to support the assessment
- Without this information, the overall quality of the assessment may be compromised

Sandia National Laboratories

Types of Data Needed for Performance-Based Assessments

- Probabilities of sensing and detection for intrusion detection, entry control, and contraband detection equipment
- Times for, and probabilities of, assessment
- Information about operating principles for equipment, nuisance alarm sources, etc.
- Access delay times
- Response force and Guard force capabilities
  - Time to respond to an attack, after notification
  - Times and proficiency for individuals performing certain tasks
  - Ability of response weapons and adversary weapons (in Threat Assessment or Design Basis Threat) to hit and kill opposing forces
  - Ability of response units to carry out plans described in security/contingency plans to effectively prevent theft and/or sabotage

There are Two Sources of Performance Data

- Facility level tests, including component testing and subsystem testing
  - Functional/operability tests,
  - Standardized maintenance performance tests for components
  - Simulated adversarial attack tests by skilled testers,
  - Subsystem tests of physical protection subsystems
  - Guard/response force exercises and tests
- State/Competent Authority Testing Laboratories to test
  - Physical protection technologies
  - Barriers
  - Response force equipment

The second source is the focus of this briefing

Sandia National Laboratories

Who Uses This Testing Performance Data?

- An expert that interprets what is in the State/Competent Authority database and then provides advice on how the data should be used
  - Having a trained expert is more important than having the data since all data needs to be interpreted before use
- Other users, typically through the expert or documentation created by the expert
  - The competent authority when reviewing security plans or results of evaluations
  - Organizations performing evaluations
  - Inspectors, where these review evaluation results
  - Physical protection system designers

Sandia National Laboratories

Categories of Test Equipment and Attack Tools

- Based on documented Design Basis Threat (DBT)
- Specify hand tools, power tools, and thermal cutting tools
- Specify heavy equipment
- Specify explosives
  - Types
  - Quantities
- Specify vehicles
  - Ground, air, water, etc.

Sandia National Laboratories

Testing Physical Protection Technology

- Testing physical protection technology is more complex than testing barriers due to the number of factors involved
- To address this complexity test organizations
  - Develop/adopt performance criteria for equipment
  - Determine what conditions influence performance
  - Perform test typically under ideal conditions
  - Monitor long-term patterns of weather, maintenance issues, etc.
  - Train experts to observe and mitigate any potential vulnerabilities in the technology

Sandia National Laboratories

How to Develop Probabilities of Detection for Physical Protection Technology

- Approaches for testing technology
- A general approach for assigning probabilities of sensing and assessment using an expert
  - Test facilities are desirable but not required: the important thing is the depth of knowledge of your expert
- Examining the complexity of testing technology using intrusion sensors as an example
- Considerations in setting up a State/Competent Authority technology testing capability

Approaches to Developing a Technology Testing Capability

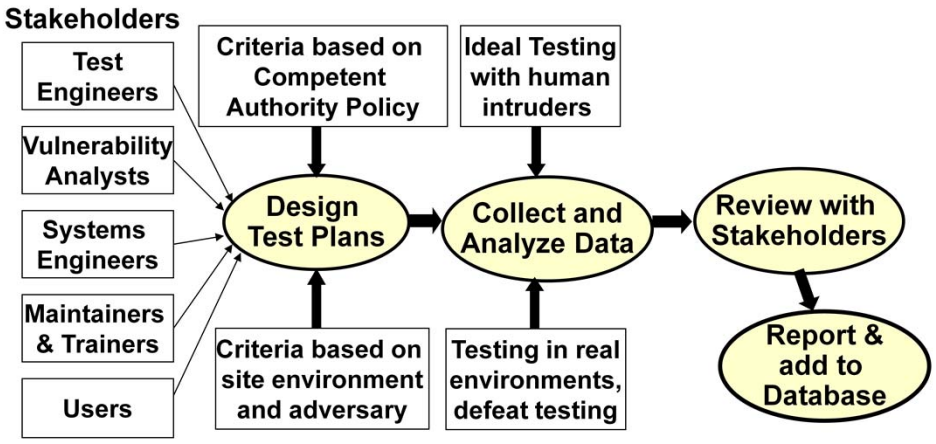
Sandia National Laboratories

- Train experts to maintain the long-term knowledge
- Develop a simple test facility to mock up a facility sector or entry control point, etc., to test hardware without disturbing operations at a facility

- Develop a dedicated testing center
- All support developing experts to
  - Support inspections
  - Identify vulnerabilities
  - Identify fixes to mitigate vulnerabilities
  - Support training

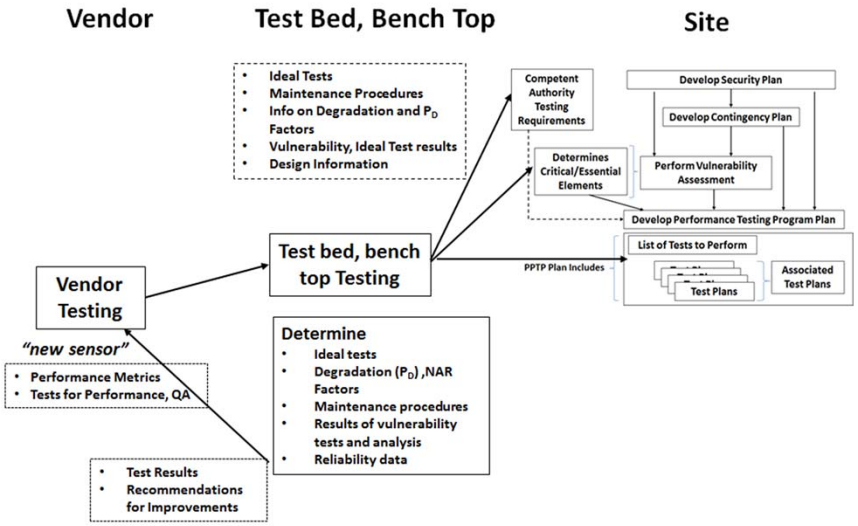
Sandia National Laboratories

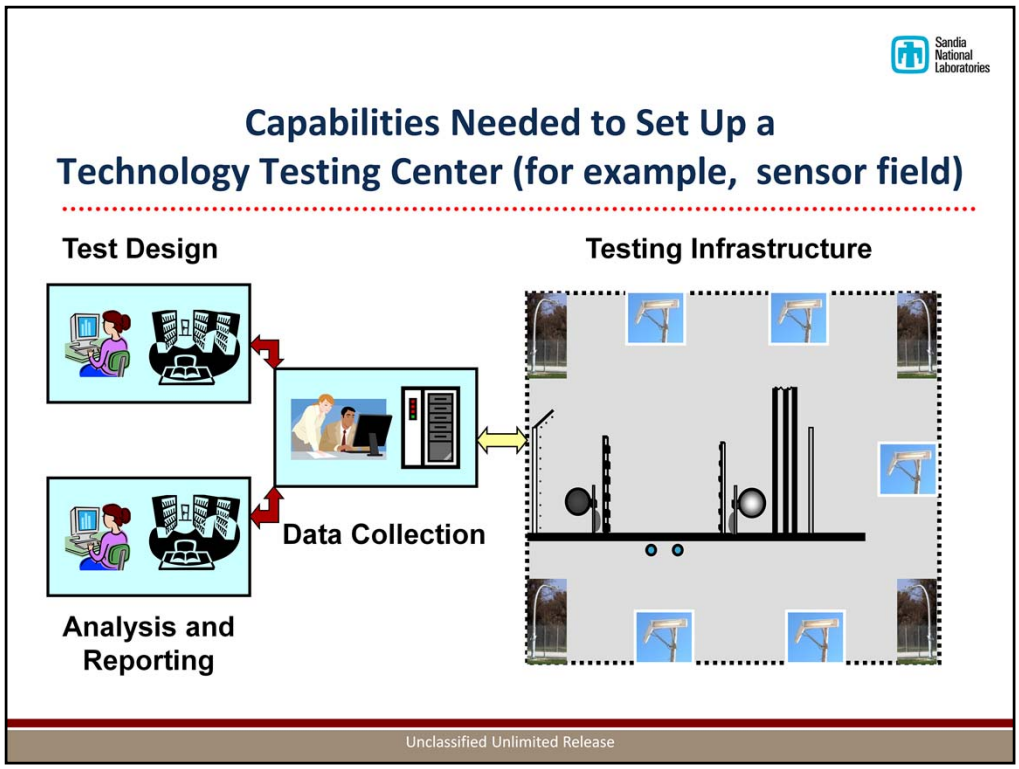
Testing and Evaluation Process for a Technology Testing Center



Sandia National Laboratories

Sensor Testing Phases





Note that the testing infrastructure and data collection system have to be carefully designed and operated to be simple and reliable so that test data from sensors are not thrown into question.

Sandia National Laboratories

Summary

- Fact: Performance-based assessments require
  - Good performance data
  - Experts who can interpret that data to support the assessment
- Without this information, the overall quality of the assessment may be compromised
- While helpful, dedicated test facilities are NOT required to start collecting this information
  - Engage existing experts first, collect literature and reference material, and train experts if need be