SAND2015-7720C

Exceptional service in the national interest

Sandia National Laboratories

Detection Data Libraries

Mark Snell
International Nuclear Security Engineering
Sandia National Laboratories
15 September 2015

U.S. DEPARTMENT OF ENERGY | NNSA

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2015-XXXXP

Unclassified Unlimited Release

Sandia National Laboratories

General Issues With Databases

- Sensitivity of data: typically in the international community:
  - Actual defeat times and values are provided very high security and are not shared
  - Database that show averaged values over several tests, with no specific description of tests is treated as less sensitive and is shared with analysts
  - Sharable databases with more general values
- Types of detection probabilities needed with different testing concerns
  - Types: Human surveillance, sensors, entry control devices
  - Concerns with testing against insider threats

Value of database decreases as sensitivity .

How to Develop Probabilities of Detection for Physical Protection Technology

Sandia National Laboratories

- 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

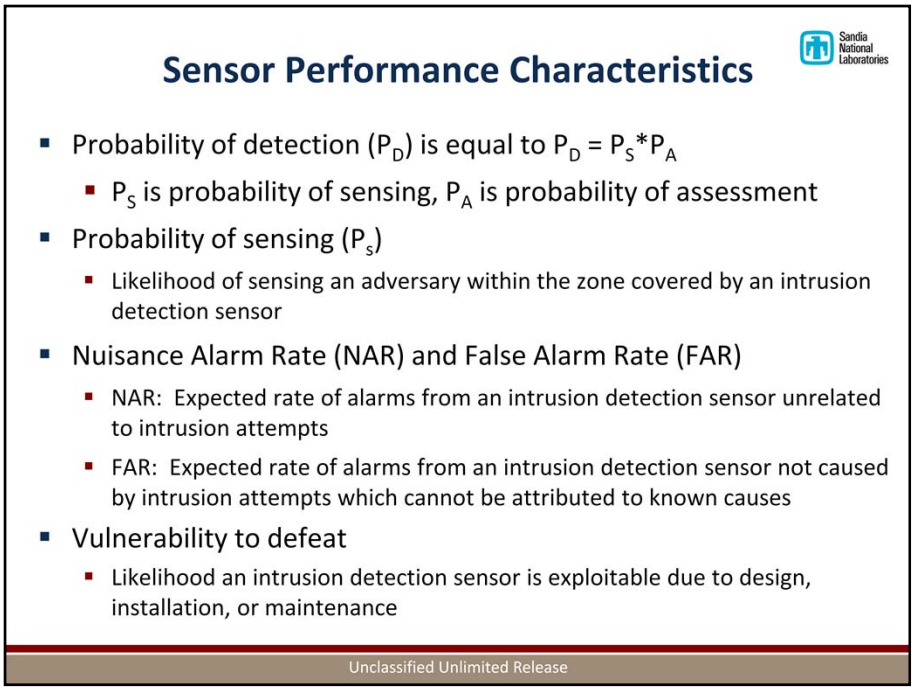
- Develop a dedicated testing center

- All support developing experts to
  - Support inspections
  - Identify vulnerabilities
  - Identify fixes to mitigate vulnerabilities
  - Support training

Approach to Creating Physical Protection Technology Data

- For technology, common performance metrics are
  - Probabilities of Sensing, Assessment, or Detection
  - Times for equipment to perform some function
- For probabilities, the expert would typically assign:
  - Qualitative Measure: Very High, High, Medium, Low, Very Low
  - Quantitative Measure: set value to qualitative score, such as High = .75
  - Validate with testing, if possible
- These values represent performance under ideal operational conditions against the DBT
  - The expert then degrades these values to take into account actual conditions in the field
- For times, keep a database like that kept for access delay

No dedicated test facility is needed to do this, technically



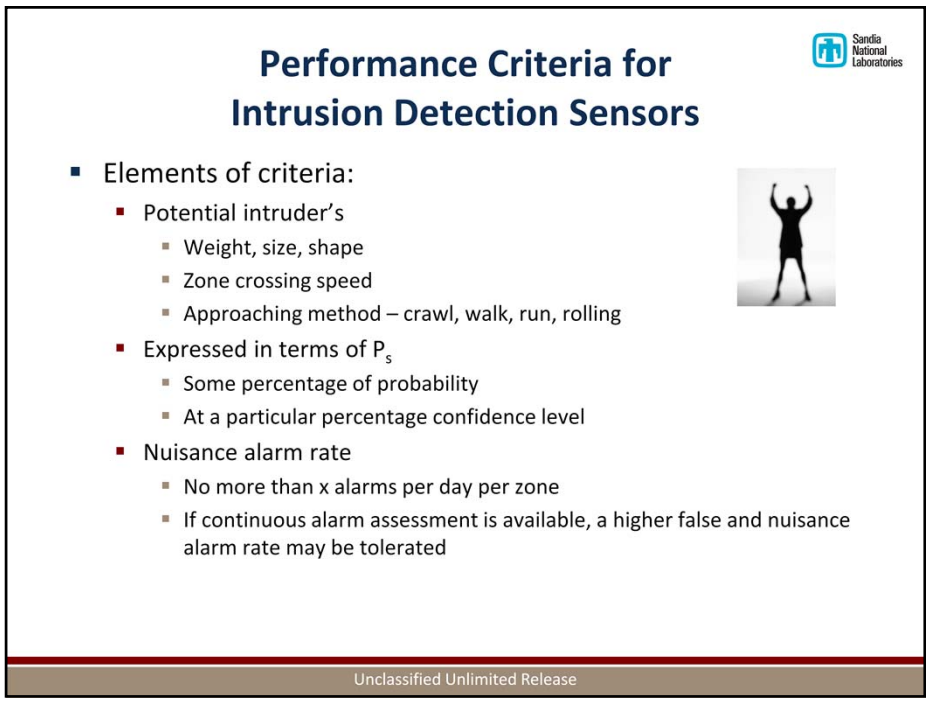
P_D is a statistical function that represents the lower confidence level of a binomial equation. If a sensor is tested 30 times and passes each time, the Pd is 0.9 at a 95% confidence level. This primarily means that there is not enough testing to prove that the Pd is any better than this.

These are three performance measures of the sensor itself. The first is the probability of detection P_D which is the probability of detecting the adversary in a zone covered by an intrusion detection sensor. A detection is only a switch closure in a sensing circuit. You remember that to have a true alarm we need this detection to be assessed.

Nuisance Alarm Rate (NAR) can degrade probability of detection because of the “cry wolf” syndrome. There are two kinds of alarms, valid alarms (an adversary entering the detection zone) and all other alarms (whatever the cause, these other alarms all are nuisances)

One subset of nuisance alarms are False Alarms. The False Alarm Rate (FAR) is important to know about a sensor. A false alarm is any alarm that is from an unknown source. This alarm is clearly “false.” If the alarm was caused by a bird or a rabbit, and this can be seen on the assessment camera, then the alarm was not a valid alarm (it was not an intruder), the alarm was not a false alarm (because the sensor was alarming correctly on an object), but it was a nuisance.

Finally the vulnerability to defeat is important to know about a sensor. The defeat techniques are not generally published, but as a PPS designer you need to know these to design against them.



The statistic, Probability of detection (P_D) for a sensor, is very situation dependent. Often salesmen will tell you that the P_D of their sensor is 0.97 in a effort to sell sensors. In truth the P_D of a sensor depends on all the things listed in this slide.

One thing to notice particularly is that it is dependent on the capabilities of the adversary. This should lead the student to realize that if we had not defined the threat early in this process, the probability of detection could not have been determined at all.

The probability of detection should be determined by installing the equipment in a test bed in the same environment as the facility and testing it with personnel having the same capabilities and equipment that you would expect the adversary to have. Enough tests should be performed to allow the analyst to state a P_D with a C_L (confidence level). In some agencies such tests are performed and the results reported as $P_D = 90\%$ with a $C_L = 95\%$. Statisticians are used to design tests and evaluate results to have a statistically supported conclusion on the capabilities of a sensor.

The students could contribute other "conditions" that would affect the detection capability of a sensor. They might add:

1. Ground preparation
2. Wiring location
3. Quality of equipment

A P_D number is useless unless the testing criteria is well described.

P_S for a Sensor is Conditional

Sandia National Laboratories

- Target size and speed
- Sensor hardware
- Installation conditions
- Sensitivity setting
- Weather conditions
- Maintained condition
- Method of intrusion
  - Walking
  - Jumping
  - Tunneling
  - etc.