SAND2012-5719P

Exceptional service in the national interest

Sandia National Laboratories

General Overview of SNL Physical Security Training

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. 2011-XXXXP

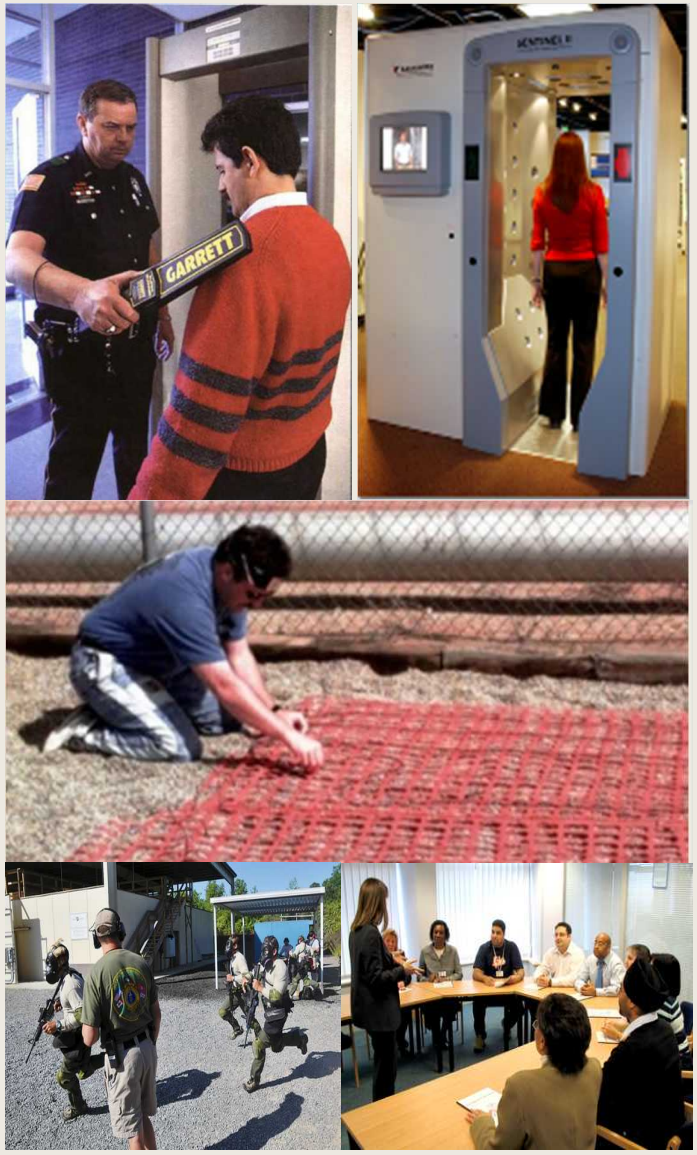
Physical Security Training History

Sandia National Laboratories

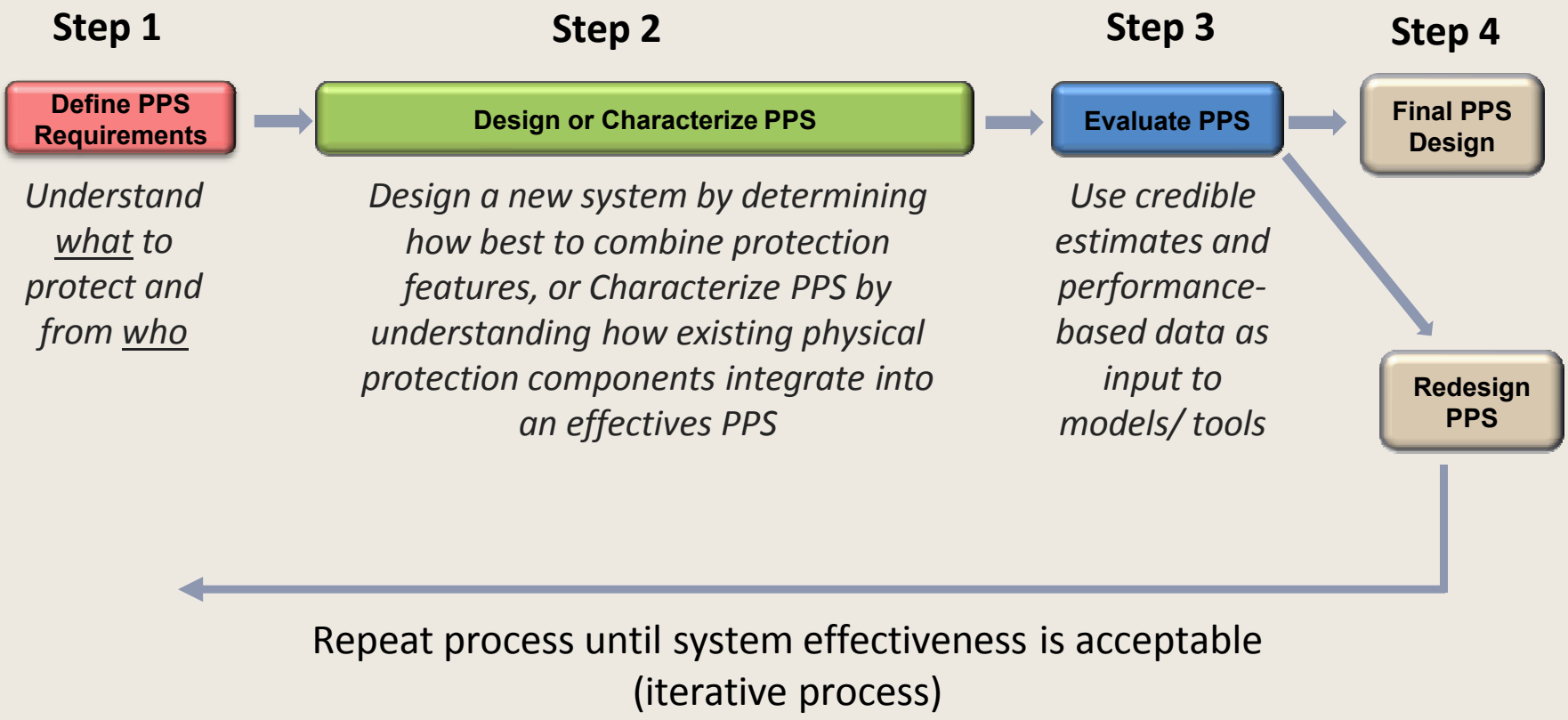
- Basic fundamental PPS courses provided to:
  - Federal customers (DOE, DOD, NRC, etc.)
  - Internal tech staff
  - Internationally (IAEA)
    - Purpose: to teach and promote common PPS definitions, concepts, principles, and terminology
- Primary focus was nuclear sites/assets, but now includes critical infrastructures
  - Training program in place for 35+ years

Physical Security Training Mission

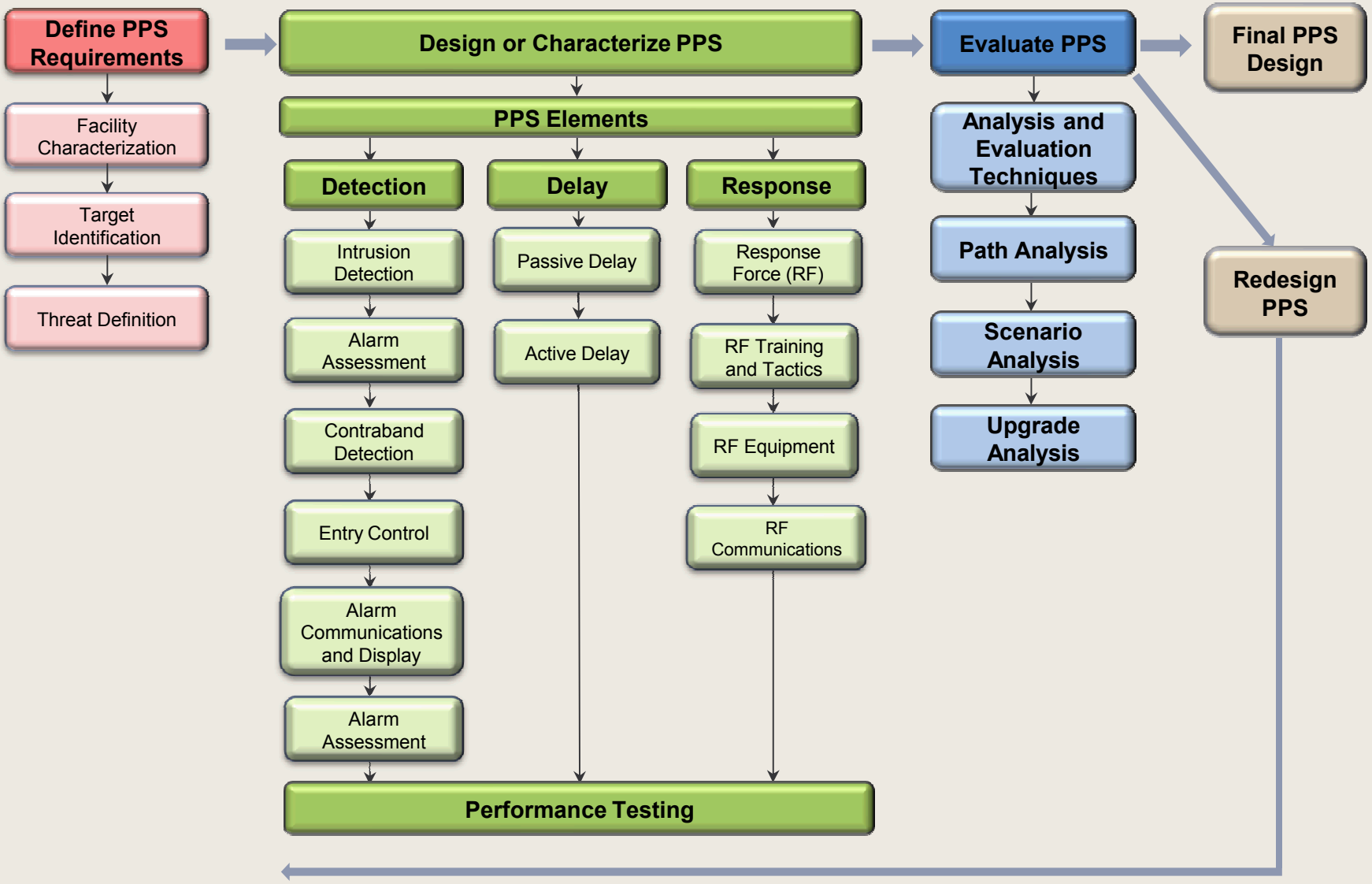
- The mission of Sandia's training team is to develop and maintain the proficiency and competence of domestic and international personnel in security disciplines
- The mission of the training has evolved over decades to meet the changing needs of the security community
  - Initial courses focused on basic concepts and principles of PPS
  - Over time the expertise of our audiences have increased, therefore requiring the development of intermediate and advanced courses
  - Additional security topics are continually being added
- Vision: to create an organized physical security curriculum program similar to a university program



All Training is Based on SNL's Design and Evaluation Process



Physical Protection System (PPS) Training Areas



Specialty Courses

- Transportation Security
- Cyber Security
- Establishing, Implementing, and Operating a Testing Facility
- Risk Analysis Methodologies (RAM) for Critical Infrastructures
  - ~10 RAM courses for specific critical infrastructures

Vital Area Identification (VAI)

This course addresses vital area identification for specific types of facilities and can be tailored to the needs of the particular audience.

Topics covered include the assumptions necessary for VAI, facility characteristics, the use of safety analysis results in VAI, logic model development and solution, and computer software used for VAI.

Define PPS Requirements

Design Basis Threat (DBT)

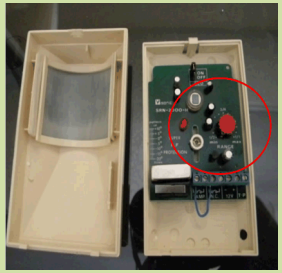
This workshop presents the international process used to develop a comprehensive design basis threat. Participants will learn about the various classifications of threats, sources of information for DBT development as well as:

- Threat assessment process
- Process for developing a DBT
- DBT implementation and life cycle

Design or Characterize PPS

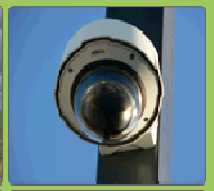
Fundamentals of Physical Protection Technologies & Systems

This interactive workshop provides participants with hands-on field experience with a variety of current security technologies of a physical security system. Upon workshop completion, participants will be able to apply the principles of the performance-based design and evaluation process.


Intrusion Detection, Assessment Systems, and Access Control

This workshop is designed to familiarize the physical protection systems professional with existing technologies, their operations, and their potential strengths and weaknesses. The workshop covers sensors, alarm communication, display, assessment, and access control as well as their sub-systems.

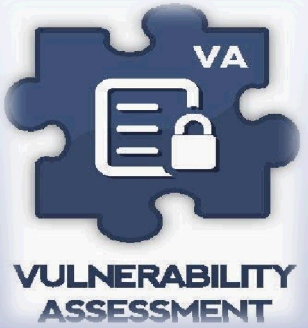
Performance Testing

Security Systems Performance Testing

Participants will be introduced to the concept of performance testing security system elements (detection, delay, and response). Performance test planning and testing activities for system components will also be discussed, up to and including end-to-end systems.

Introduction to Vulnerability Assessments (VA)

Introduction to VA introduces participants to the process used to conduct a performance-based evaluation of a physical protection system. Participants will learn about the purpose of the VA in the security process, the five phases of the VA, and will be introduced to various tools used to conduct a VA.



Vulnerability Assessment Tools & Methodologies

This workshop introduces students to the current methods used to evaluate a site's physical protection system to protect against theft or sabotage of nuclear materials and facilities. Participants will have hands-on access to various analysis tools and use these tools to analyze various scenarios of concern.

Advanced Vulnerability Assessment Process

In this course, participants will conduct a VA of a functional training facility in parallel with training activities. Participants will complete the course with an in-depth knowledge of the analysis process, reporting, and presentation of findings.

Evaluate PPS

Transportation Security

Introduction to Transportation Security

The challenges associated with protecting nuclear material from unauthorized removal and sabotage during transport are unique and require a dedicated approach. This workshop focuses on these challenges by discussing the elements of a transportation security program. Topics will range from VA to PPS and MC&A functions and how they can mitigate risks identified.

Vulnerability Assessment for Transportation Security

The tactical advantages that are present at fixed sites become advantages for the adversary when the target is mobile. These advantages range from tactical planning to preparing the terrain for battle. This course focuses on methodologies that assess vulnerabilities for a transportation security program.

Design & Evaluation for Secure Transportation

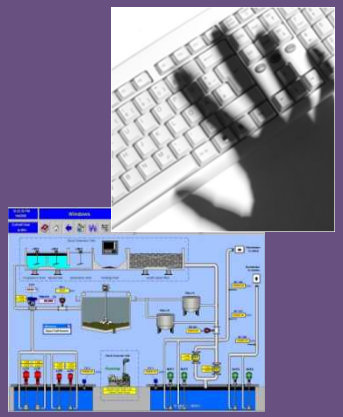
Secure transportation of nuclear material present challenges that require a unique approach. Convoy designers utilize a transportation security plan as a methodology to define, review, and communicate the tools and principles to protect mobile assets. The Security Plan is a system that integrates people, procedures, and equipment. This workshop focuses upon the components and measures that will mitigate risks found in the VA.

Cyber Security

Information Design Assurance Red Team (IDART)

This training workshop is designed to help attendees improve the defensive posture of their information systems by assessing them from an adversarial perspective.

The workshop provides detail exposure to a red-teaming assessment process through lecture and practical application.



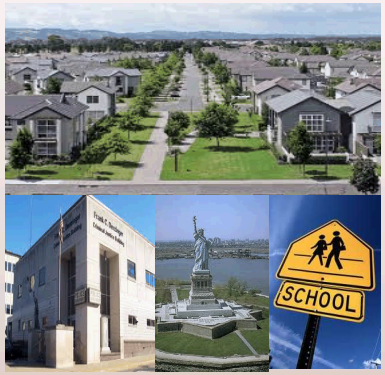
Methodologies for Assessing SCADA Systems

Supervisory Control and Data Acquisition (SCADA) systems have become a critical component in the operation of critical infrastructures, and are often overlooked when assessing information systems. This customizable course covers a breadth of SCADA and other digital control system use in infrastructures and industry, identifies vulnerabilities of these components and systems, and present methodologies and tools to assess these systems in a successful, measurable, reproducible manner.

Establishing, Implementing, and Operating a Testing Facility

This workshop introduces the essential elements for establishing and operating a PPS testing facility infrastructure. The workshop focuses upon testing facility infrastructure basics including sensor/video communications, video assessment, lighting, and electrical power. Additional topics include testing methodology, data analysis, and reporting.

Risk Analysis Methodologies



Risk Assessment Methodology for Communities (RAM-C)

RAM-C is a systematic process that has been developed to assist communities in assessing threat, prioritizing targets, identifying consequences, evaluating completeness and effectiveness of physical security systems and helping to effectively use resources to address vulnerabilities in security and response systems.

Risk Assessment Methodology for Critical Infrastructures (RAM-CI)

RAM-CI has a basic security risk assessment framework common to all critical infrastructures and it can be adapted to any critical infrastructure/key resource (CI/KR) sector. The RAM-CI tool provides the processes for combining consequence, vulnerability and threat information for a comprehensive and systematic risk assessment and management capability that can be applied to all CI/KR sectors.