40 YEARS
of collaboration, innovation and education.

IMRP2016 | VANCOUVER BC, CANADA

SAND2016-10397C

Security by Design:

Project Overview and Security Assessment Process

Presented By:
- Michal Kuca
- C.J. Hartwigsen
- David Allen

November 2016

Sandia National Laboratories is a multi-mission 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.

Security by Design

Why incorporate security?

- Radiological material is a potential target for theft & sabotage:
  - *Criminal Groups*
  - *Terrorist Groups*

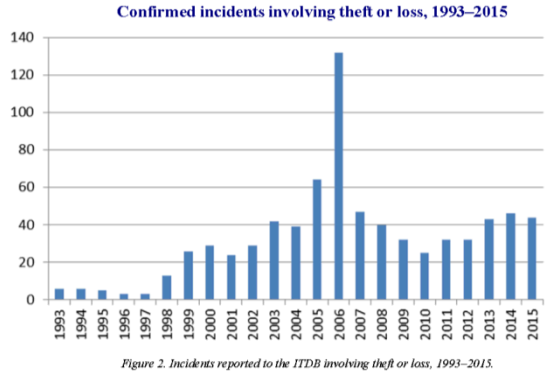


Figure 2. Incidents reported to the ITDB involving theft or loss, 1993–2015.

Source: IAEA Incident and Trafficking Database

News events involving radiological material

"Jose Padilla and two others are arrested and charged with planning a "dirty bomb", an explosive laced with radioactive material, attack on the U.S. "Experts believe the brothers spied on the researcher, who has not been identified for his own safety, and planned to blackmail him to acquire dangerous material."

Source: www.cbsnews.com

Source: www.nbcnews.com

Brussels Attacks: Bombers Filmed Nuclear Researcher, Expert Says, Nancy Ing and Alexander Smith

Security By Design

Program Objective

- Collaborative effort with the manufacturer to identify and develop low-cost detection and delay enhancements that can be incorporated into future facility designs to help mitigate the risk of source theft

- Incorporating security into facility design:
  - Increases # of possible facility enhancements
  - Allows for countermeasures that balance the facility security/usability paradigm
  - Inexpensive compared to retrofitting

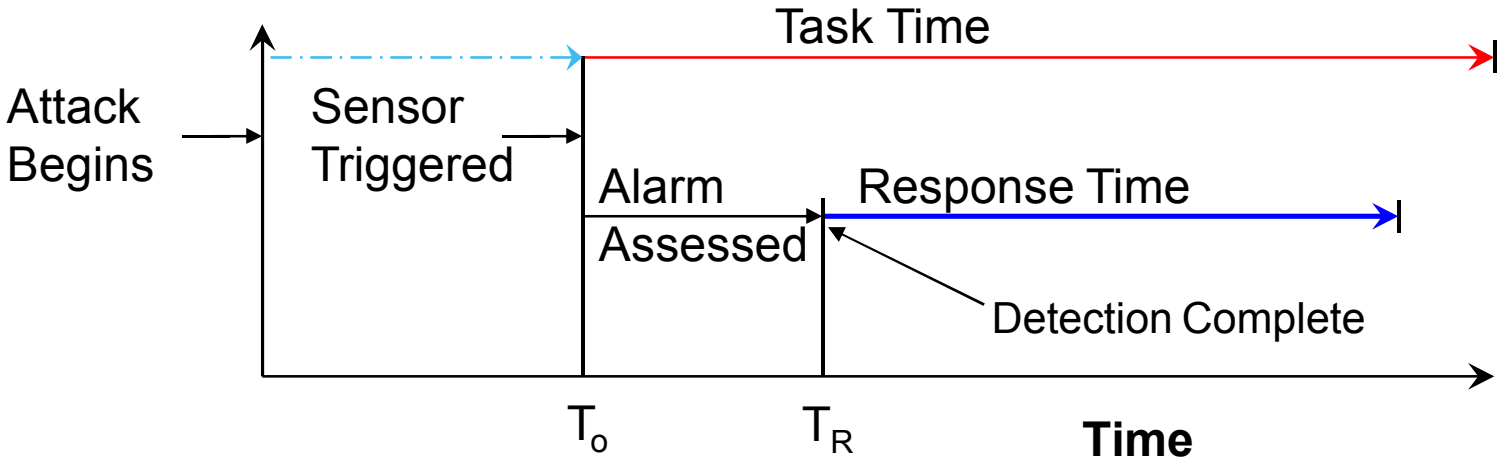
Security by Design

Elements to Security

Three key elements:

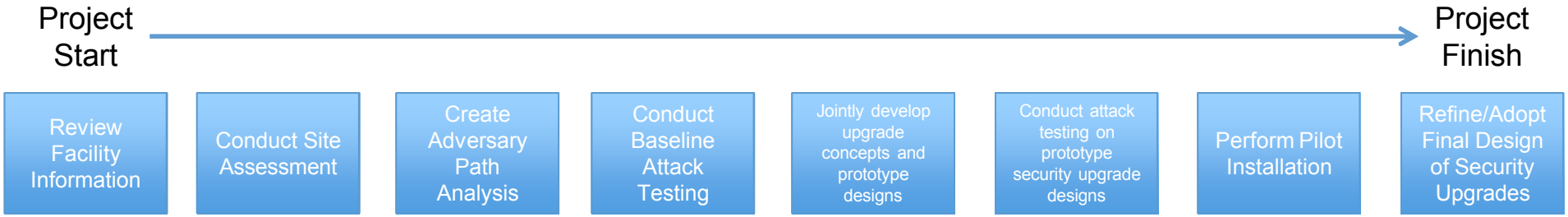
1. Intrusion Detection and Assessment
2. Access Delay
3. Response

Radiation safety measures rarely provide delay!



Security By Design

Project Outline/Steps



- Physical Protection Principles
  - DETECTION BEFORE DELAY
  - Balanced design
  - Design to address the threat
  - Assessment
  - Low NAR/FAR (Nuisance Alarm Rate/False Alarm Rate)
  - Minimize Impact to Operations/Safety

- Common Enhancement Methods
  - Layered Methods
    - Layers: Facility Entry, Maze, Pool, Source Rack
    - Add delay at each layer, concentrated at the sources
  - Detection Elements, early in the attack path
  - Two Person Controls when possible
  - Remove components that aid an adversary
  - Integrate tamper detection sensors into delay barriers

Security By Design

Discussions, Questions and Answers

THANK YOU!

CURRENT SECURITY BY DESIGN PARTNERS:

- SQHL
- SYMEC