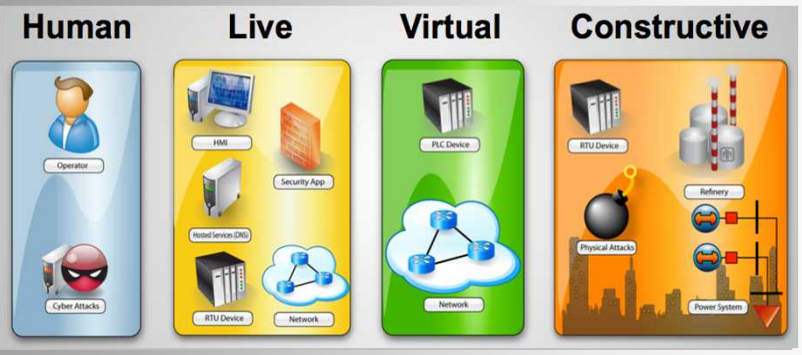
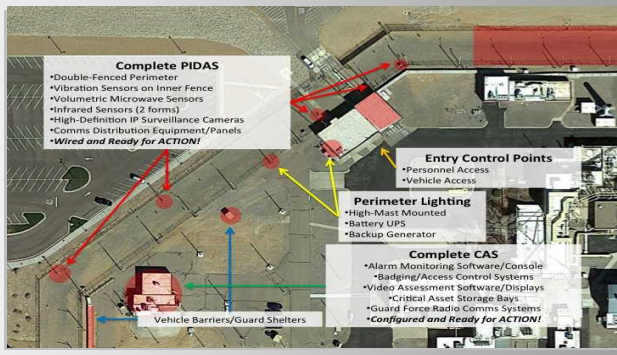
SAND2015-4204C

Exceptional service in the national interest

Sandia National Laboratories





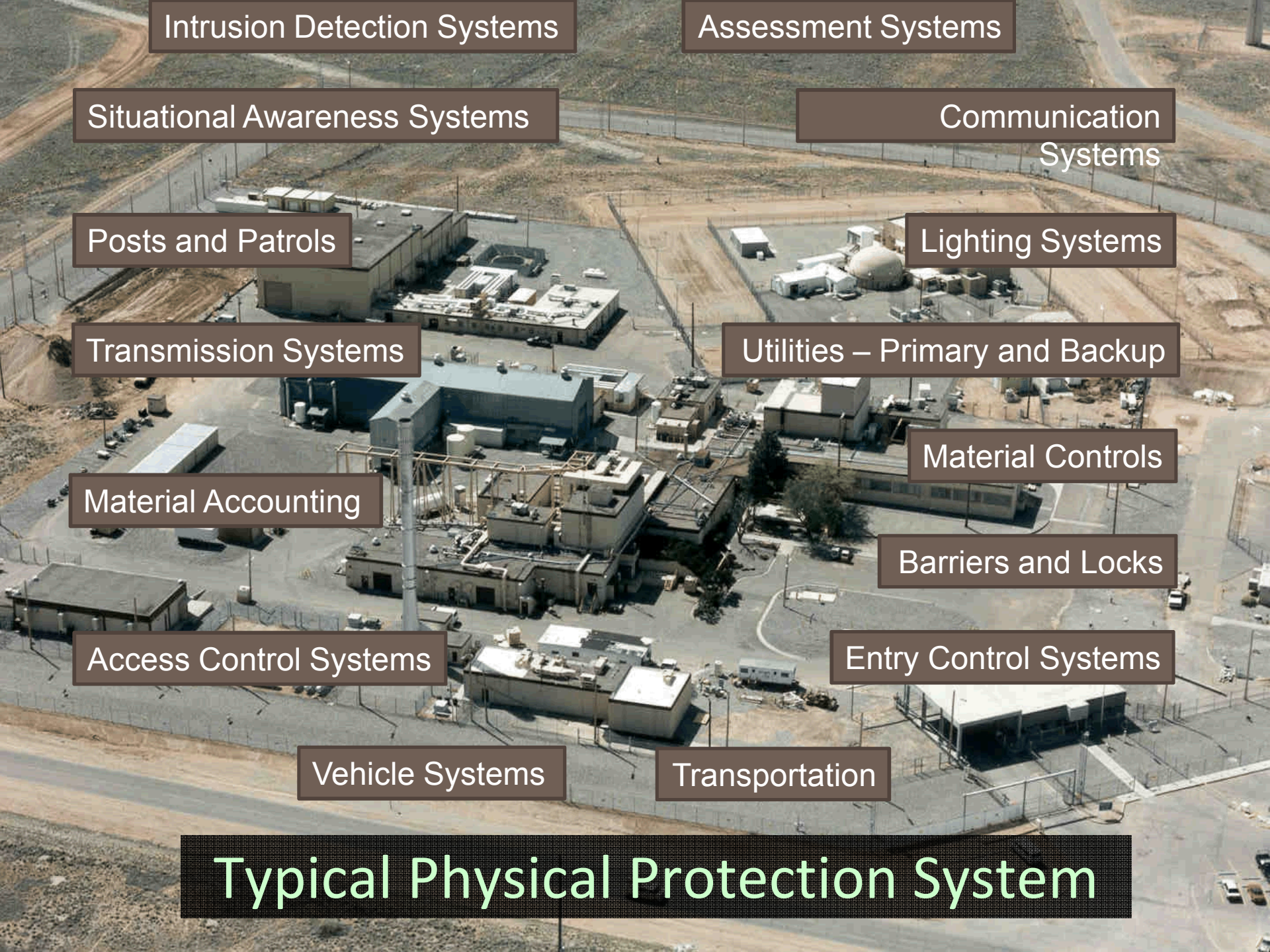
Investigation of Cyber-Enabled Physical Attack Scenarios

John F. Clem

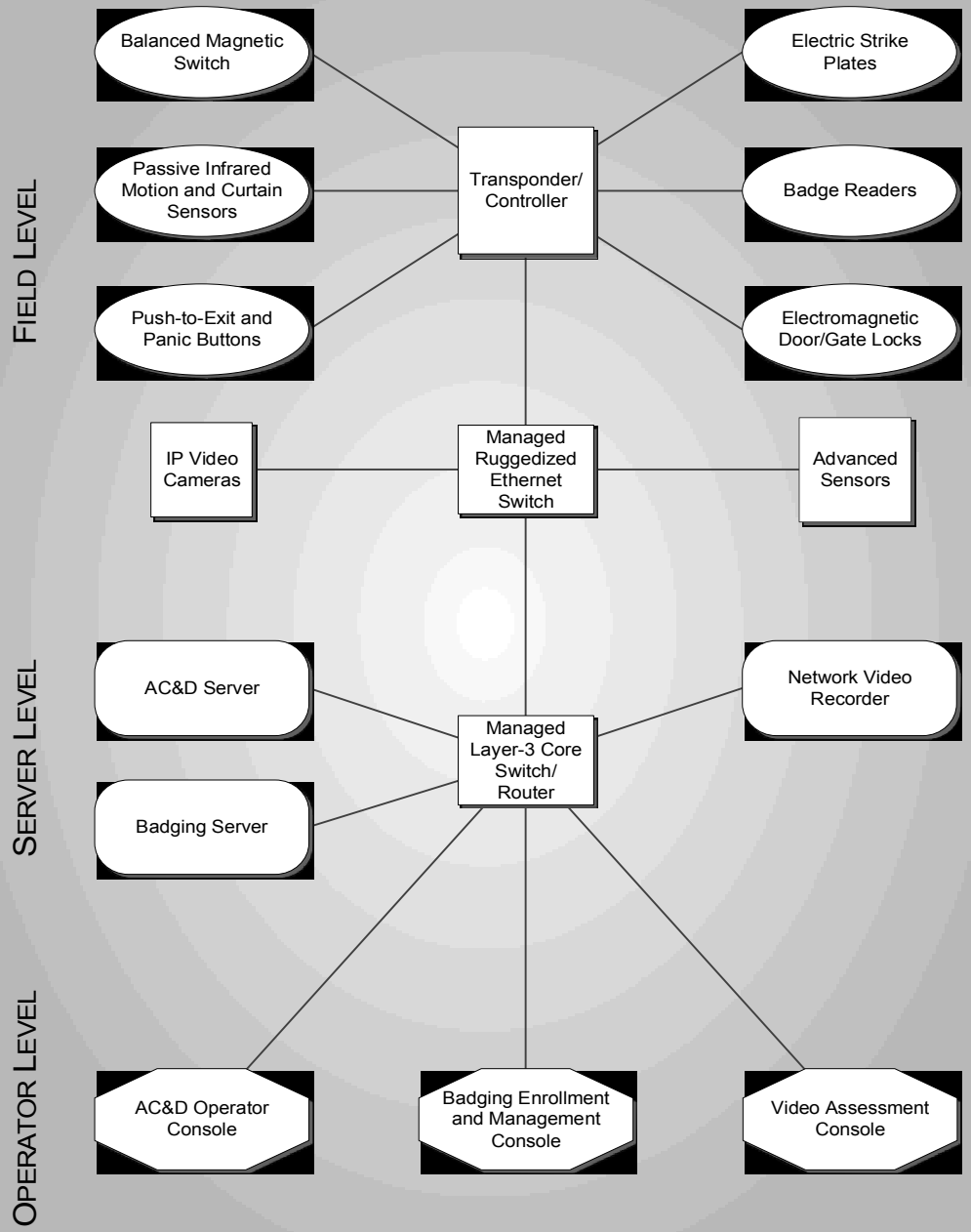
IAEA-CN-228/4D3/060

U.S. DEPARTMENT OF ENERGY | National Nuclear Security Administration

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



Typical Physical Protection System



Physical protection system (PPS) hardware and networks can be abstracted at layers.

This image represents a notional system.

Threats to All Cyber-Based Systems

- Isolation is a myth.
  - Exhibit (A) Stuxnet – sneaker net attack; target done in by a USB drive with malicious code.
  - Exhibit (B) – the Power Pwn, $1,495
  - Exhibit (C) – the Pwn Pad, $895

Low-cost, commercially available, innovative disrupters available to anyone.

Hypothetical Attacks – High Level

- Goal: compromise the PPS to prepare for a physical attack
  - Exploit access control system to gain unauthorized entry
- Goal: buy time – move detection behind the critical detection point
  - Exploit assessment systems to degrade the detection function
- Goal: create a diversion and confusion to avoid interruption
  - Spoof device alarms from sensors in remote locations to draw response force away from the real attack
- Goal: degrade PPS performance
  - Exploit workstations that manage PPS configuration

Stakeholder Questions

- Could increasing computer-based components in PPS result in the ability of emerging, asymmetric threats to exploit cyber vulnerabilities that degrade the performance of a PPS?
- Are there exploitable vulnerabilities in physical protection systems?
- Which subsystems and components are vulnerable?
- Would operators be aware if their system was compromised?
- How does the threat of cyber exploitation change the set of attack scenarios against which the PPS is engineered to protect?

Problems to Overcome

1. Key stakeholders must be convinced the threat is credible.
2. The breadth of the threat must be understood in the PPS system-of-systems, and issues prioritized
3. Cyber security assessors won't be permitted to test production systems
4. There are many makes and models of PPS systems and components

Our R&D Answer and Approach

- Goal: develop low-level modeling & simulation for cyber-enabled physical attack scenarios
  - Enables cyber security testing “hands-off”
  - Avoids the need to build expensive test beds
  - Support rapid mitigation testing
- Phase One: identify and understand credible cyber threats
  - Using Sandia’s international PPS test bed, systematically enumerate the PPS and perform vulnerability discovery
  - Develop and demonstrate a credible end-to-end cyber attack
    - Be sure to demonstrate how an outsider could do this
  - Understand how PPS hardware and software interact at lowest levels
- Phase Two: develop the ModSim framework, and experimentally validate the reliability of the capability, improve and refine

Research Challenges

- Lack of prior cyber vulnerability testing of PPS components
- Proprietary vendor application/communication protocols
- Investigating cyber/physical attacks require expert knowledge in both the cyber and physical domains
- Small number of cyber/physical attack case studies are available publicly
- Identification and discussion of vulnerabilities may be unclassified to highly classified depending on the circumstances

Q&A

What questions do you have for me?

*Image used with the permission of the owner without restriction.