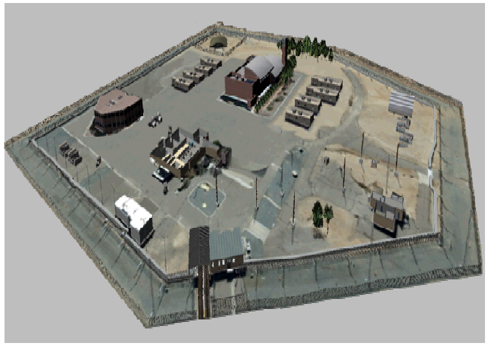
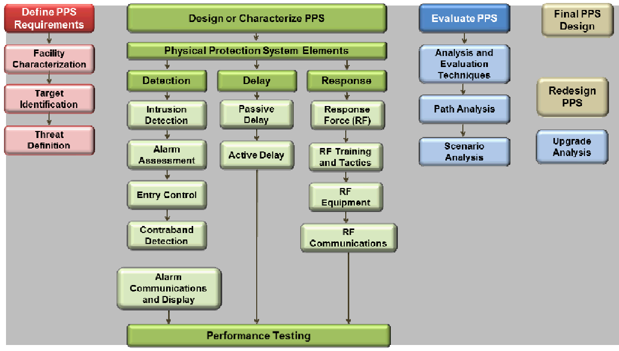
Exceptional service in the national interest

SAND2013-9776P

Sandia National Laboratories
MANAGED FOR DOE BY SANDIA CORPORATION,
A LOCKHEED MARTIN COMPANY





Define PPS Requirements
Facility Characterization
Target Identification
Threat Definition

Design or Characterize PPS
Physical Protection System Elements
Detection
Delay
Response
Intrusion Detection
Passive Delay
Response Force (RF)
Alarm Assessment
Active Delay
RF Training and Tactics
Entry Control
RF Equipment
Contraband Detection
RF Communications
Alarm Communications and Display
Performance Testing

Evaluate PPS
Analysis and Evaluation Techniques
Path Analysis
Scenario Analysis

Final PPS Design
Redesign PPS
Upgrade Analysis

Computer Security Guidance – Literature Review

Shawn E. Taylor, Ph.D.
Security Systems Analysis

Korea Hydro Nuclear Power/Central Research Institute
Daejon, South Korea – November 18-22, 2013

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 2013-XXXX

Presentation Outline

- Overview of Literature Review
- Highlights of U.S. Nuclear Regulatory Commission (U.S. NRC) Cyber Security Requirements
  - Cyber Security Program
  - Demonstrating High Assurance
  - Elements of the Program
  - Licensee Duties
  - Cyber Security Plan Requirements
  - Additional Information
  - U.S. NRC Technical Guidance Reports (NUREG documents)
  - Network Topology and Data Flow

Cyber Security Program

- Licensees must submit a Cyber Security Plan
- Computers, Communications and Networks must be protected when associated with:
  - Safety
  - Security
  - Emergency preparedness
- These systems should be protect from attacks which
  - Adversely impact integrity or confidentiality of data or software
  - Deny access to systems, services, or data
  - Adversely impact the operation of these systems

Demonstrating High Assurance

- Identify assets to be protected
- Establish, implement, and maintain a cyber security program
- Incorporate the cyber security program as a component of the physical protection program

Elements of the Program

- Security controls to protect the identified assets from cyber attacks
- Defense-in-Depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks
  - Department of Homeland Security, “Control Systems Cyber Security: Defense in Depth Strategies,” INL/EXT-06-11478. May 2006.
  - Additional references cited in this report have been provided to KHNP/CRI.
- Mitigation of adverse effects of cyber attacks

Licensee Duties

- Ensure that appropriate personnel are aware of cyber security requirements and receive the necessary training
- Evaluate and manage cyber risks
- Ensure that modifications to assets are evaluated before implementation to ensure that the cyber security performance objectives are maintained

Cyber Security Plan Requirements

- The cyber security plan must describe how the requirements of this section will be implemented and must account for site-specific conditions that affect implementation
- The plan must include measures for incident response and recovery for cyber attacks, including descriptions for how the licensee will:
  - Maintain the capability for timely detection and response to cyber attacks
  - Mitigate the consequences of cyber attacks
  - Correct exploited vulnerabilities
  - Restore affected systems, networks, equipment affected by cyber attacks

Additional Information

- The cyber security program is a component of the physical security program, in accordance with 10 CFR 73.55(m)
- RG 5.71, "Cyber Security Programs for Nuclear Facilities," [NRC, 2010]
  - An NRC regulatory guide that provides direction for the submittal of licensees for operating nuclear reactors.
- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" [NRC, 2006]
  - Direction on the methodologies that the NRC staff deems acceptable

NUREG Technical Documents

- "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," NUREG/CR-6847, U.S. Nuclear Regulatory Commission, Washington DC, October 2004.
    - Documents the development of a cyber security self-assessment method that could be used by licensees to systematically assess the risk to systems deemed to be critical to the operation of NPP.
- "High Integrity Software for Nuclear Power Plants," ISO/IEC 12207, Software Lifecycle Process, NUREG/CR-6263. U.S. Nuclear Regulatory Commission, Washington DC, 1995.
    - Documents the work performed in support of the US NRC to examine the technical basis for candidate guidelines that could be considered in the review and evaluation of high integrity computer software used in the safety systems of NPP

NUREG Technical Documents

- "Assessment of Wireless Technologies and Their Application at Nuclear Facilities," NUREG/CR-6882, U.S. Nuclear Regulatory Commission, July 2006.
  - Documents technology considerations that could contribute to the technical basis for comprehensive guidance on wireless systems.
- "Secure Network Design for Nuclear Power Plants," SAND2010-8222P, Draft NUREG/CR Report, U.S. Nuclear Regulatory Commission, Washington DC, October 2010.
  - Describes the critical design elements of a secure digital Nuclear Power Plant Data Network.
  - Provides technical guidance about features contributing to secure network designs for safety applications at NPP.
  - Lists applicable criteria to be met for protection against cyber threats

NUREG Technical Documents

- “Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment, NUREG/CR-6939, U.S. Nuclear Regulatory Commission, Washington DC, July 2007.
  - Details an interface study of the three most prominent wireless devices in use in 2007 (Bluetooth, Zigbee, and Wireless Fidelity), using computer models and simulations.
  - Looks into whether the three technologies can coexist in an industrial environment.

Defense in Depth Principle

- The ideal of defense in depth when associated with protecting a network asset simply means having a defensive strategy that includes multiple layers of different security methods. If one layer of the defense is breached then another layer can be used to protect the important or critical asset. Each layer should be independent from each other; this is a modern approach to secure network architectures.
- See: Department of Homeland Security, “Control Systems Cyber Security: Defense in Depth Strategies,” INL/EXT-06-11478, Idaho National Laboratory, Idaho Falls ID, May 2006.

Defense in Depth Principle

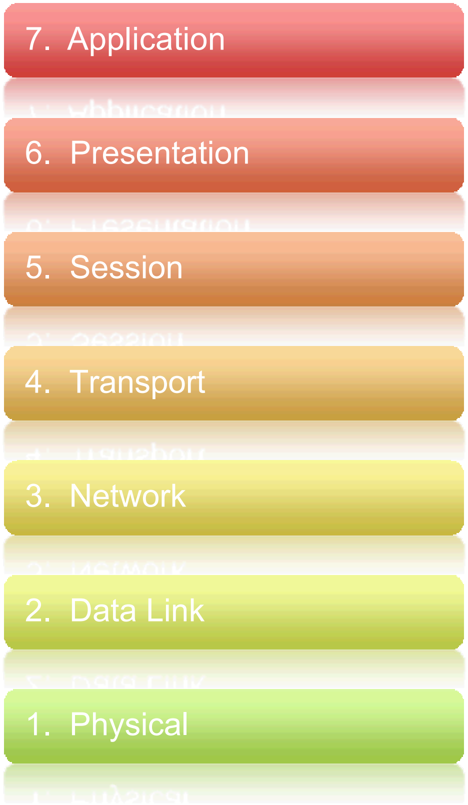
- Critical Cyber Asset Identification
  - Is it a Critical Systems? Does it support a Critical System?
- Consequence Based Evaluation
  - Safety, Security, and Emergency Preparedness
  - Business Operations
- Where is it located on the Network?
  - Type of Network?

Network Topology

Network Topologies using OSI layers for Address and Port Security Filtering

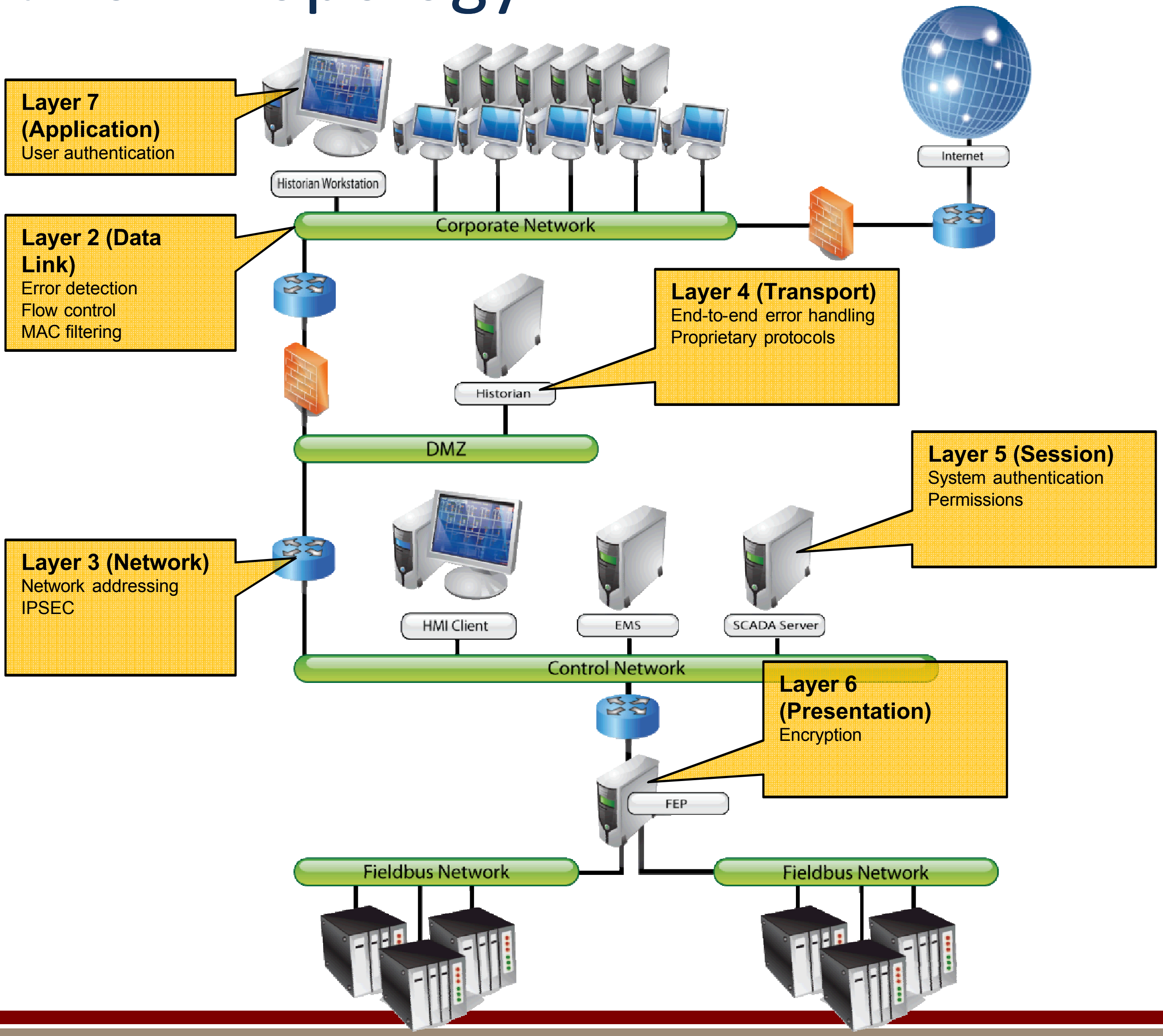
- Flat – Layer 1
- Switched – Layer 2
- Segmented – Layer 3
- Multilayer Switching – DMZ Segregated

OSI 7 layer model



7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

Network Topology



Layer 7 (Application)
User authentication

Layer 2 (Data Link)
Error detection
Flow control
MAC filtering

Layer 4 (Transport)
End-to-end error handling
Proprietary protocols

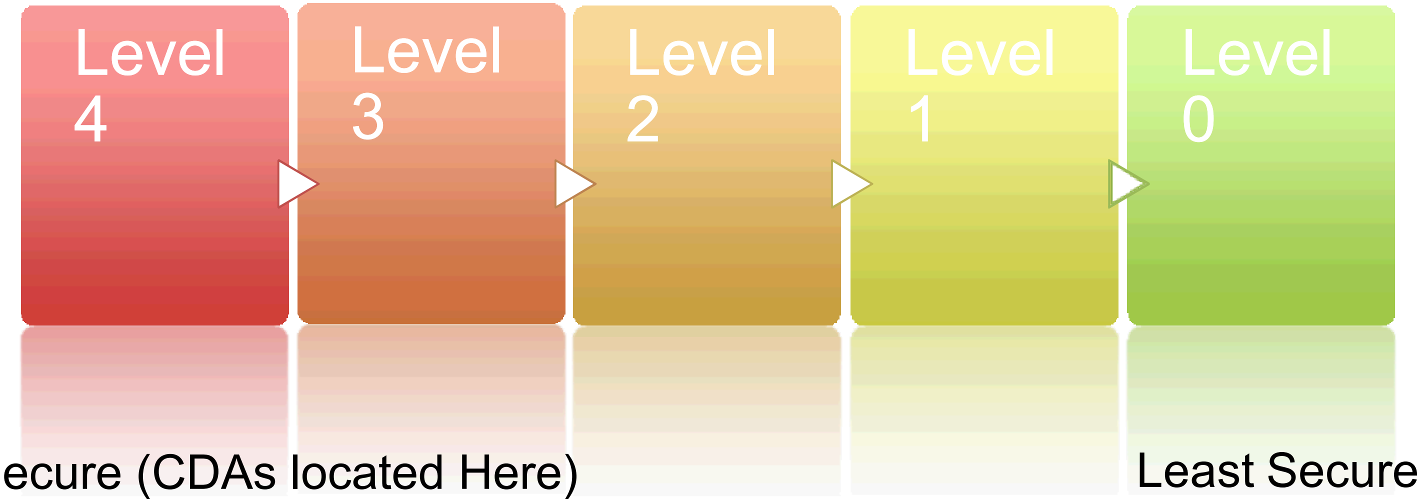
Layer 5 (Session)
System authentication
Permissions

Layer 3 (Network)
Network addressing
IPSEC

Layer 6 (Presentation)
Encryption

Network Topology

- Data Flows within Layers of Defense Model
- U.S. NRC’s layers: RG5.71 and NEI 08 09 revision 6

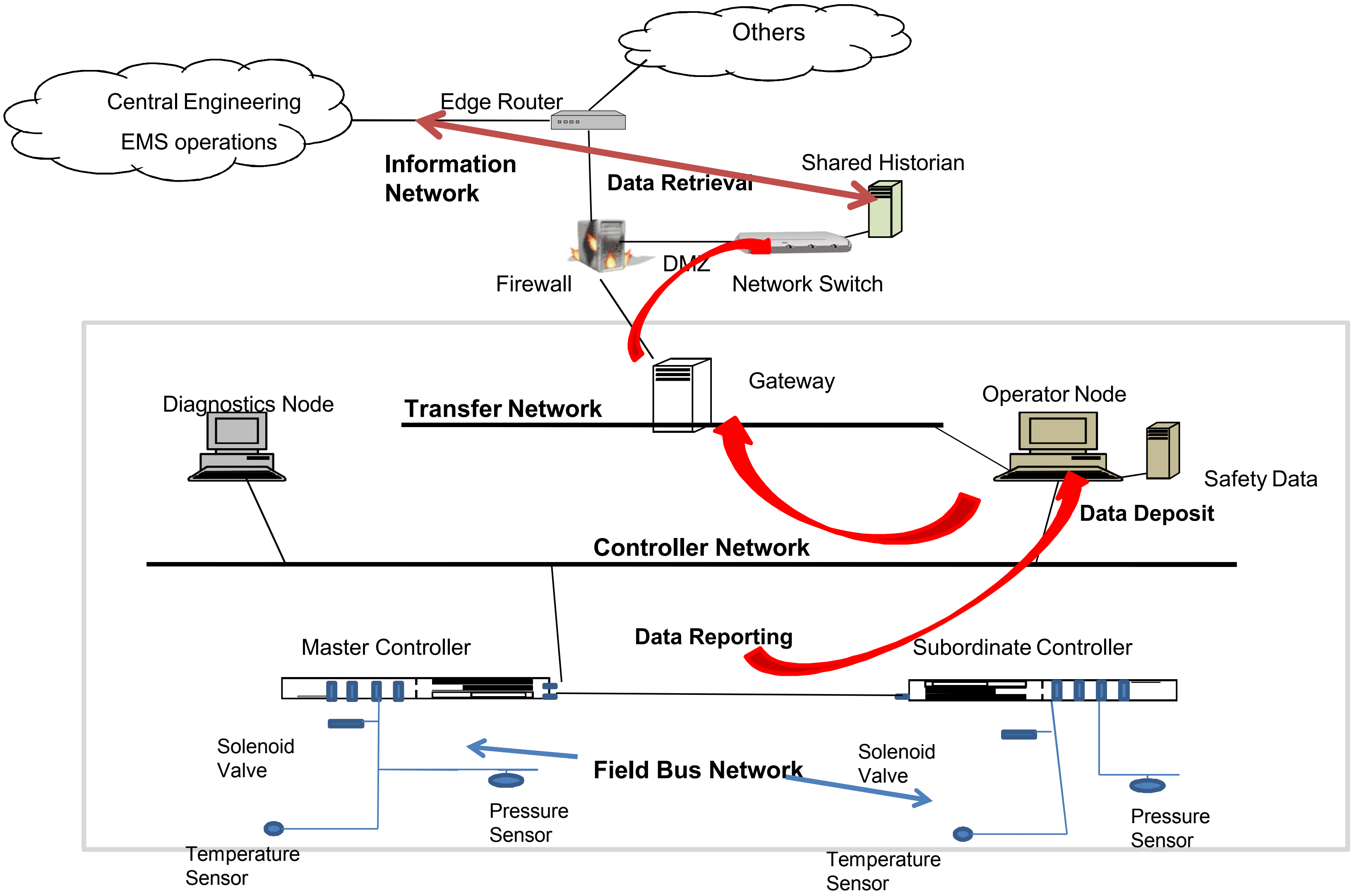


Most Secure (CDAs located Here)

Least Secure

Network Topology

(Example Implementation: Initiation of Data Flow)



Network Data Flow

- Data Flow Boundaries
  - Understanding how data will flow on a NPP system network is to understand how interconnecting devices such as serial bus nodes, hubs, switches, routers, and gateways affect the flow of data on a network.
- Data Flow Identification
  - The ability to interpret the contents of a header field attached to a data packet is a key means of understanding the flow of data across the network and performing network analysis.

Summary

- Task has been completed
- Some follow-up to obtain additional references
- Follow-up discussion with Sandia Subject Matter Expert will be arranged