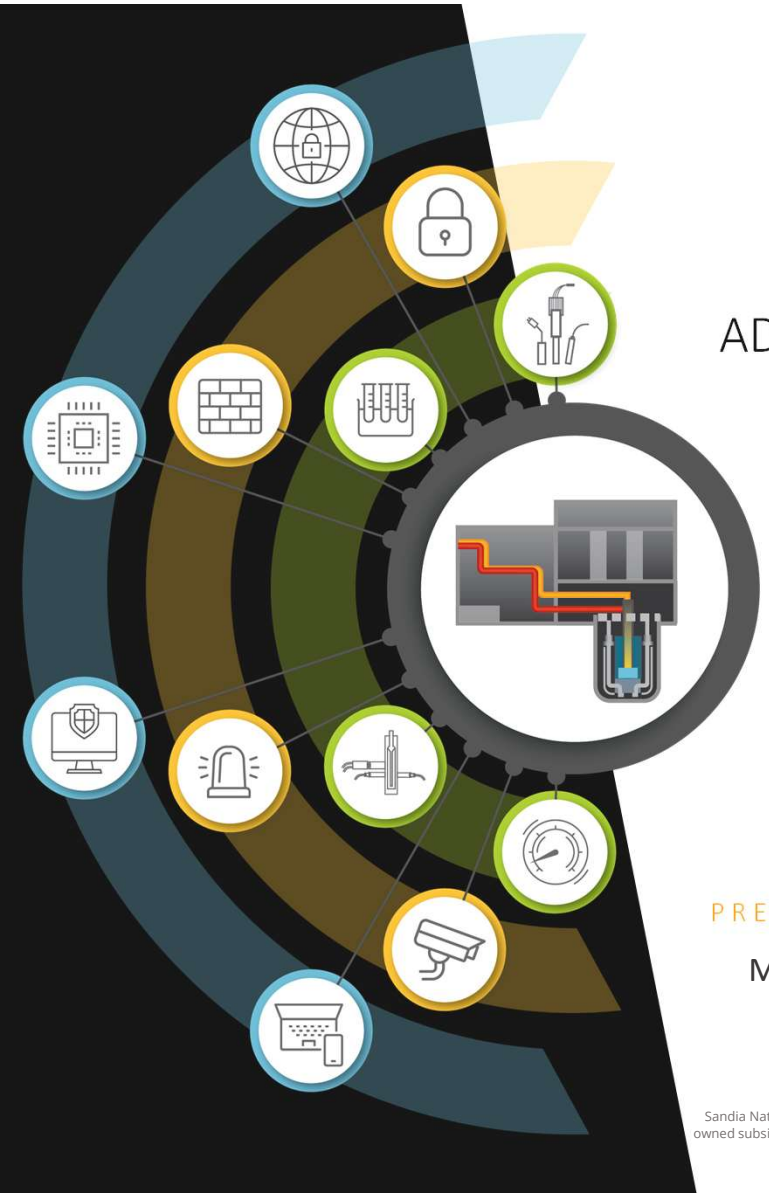


SAND2026-20223PE

ADVANCED REACTOR SAFEGUARDS & SECURITY

Wireless Security Impact Analysis for Important to Safety Systems

Michael T. Rowland, Minami Tanaka, Sheryl Drake, Robert Brulles, Robert Lois II

PRESENTED BY

Michael T. Rowland

April 29th, 2026

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories | U.S. DEPARTMENT OF ENERGY

Problem Statement

- Can Wireless Technologies be relied upon for Important To Safety Systems?
- Two Example Use Cases
  1. Ultrasonic Gas Monitors (Wolf Creek NPP) – consider as an aid for operational decision making without the alternative method (void factor calculation).
  2. Special Tooling – Fuel Handling Robots (X-Energy) – wireless providing command and control functions for radiological safety – not a Nuclear Safety Function – but having other safety impacts.

SAND2026-20223PE

Research Objectives

- M3: Methodology and Security Impact Analysis template for performing Security Impact Analysis for wireless monitoring for Safety Related Systems, Structures, and Components.
- M3: Evaluation of Cybersecurity for Wireless Fuel Handling Systems in High Temperature Gas Reactors (HTGR)

Wolf Creek Effort

I. **Why is wireless needed?**
   - **Ultrasonic Gas Monitoring (UGM)**
   - **Past Efforts**

II. **Research goal:**
   - **Determine if wireless UGM devices could be used as a Critical Digital Assets (CDA)**

III. **The process**
   - **Risk-based conceptual defensive model**
   - **Aligns with Nuclear Regulatory Commission's (NRC) guidance**
   - **Uses EPRI Technical Assessment Methodology (TAM), Rev. 2**

IV. **Results**

Wireless Void Monitoring at Wolf Creek (1/2)

Problem Statement

- 170 piping locations through the Aux and Containment Buildings are required to be monitored for gaseous voids on a quarterly basis
- 27 long term scaffolds erected in the Aux to support monitoring
- 26 locations in Containment accessed via 24 ft ladder
- ~200 climbs per year

Sandia National Laboratories

SAND2026-20223PE

Wireless Void Monitoring at Wolf Creek (2/2)

Solution

- Current scope focused on 50 locations to eliminate long term scaffolds and containment entries
- Completed evaluation and classified as Non-CDA
- Site leadership has a desire to find potential solution to be able to utilize wireless technology for safety-related applications
- Partnership with Sandia National Lab

Past Wireless Research Efforts

Leverages System Lifecycle Process

Literature Search of 27 Standards, Consensus Guides, Regulatory Documents, and Best Practices to define cybersecurity specific requirements *SAND2025-01576C*

NEI 08-09 [Rev. 6]

Process Planning

Requirements Specification

Selection of Pre-Developed Items

System Specification

Detailed Design & Implementation

System Integration

System Installation

Performed by Wolf Creek

Development of a Conceptual Defensive Model *SAND2025-01580C*

- Defensive Strategies
- LBLs
- Test Strategy (V&V)

Wolf Creek Design EC

NRC TLR SIA

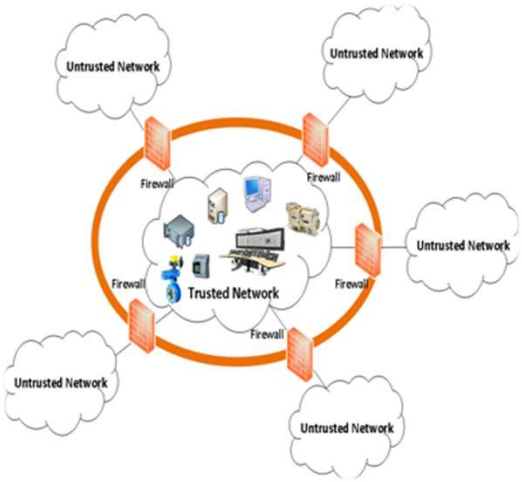
NEI 08-09 [Rev. 7]

System Validation

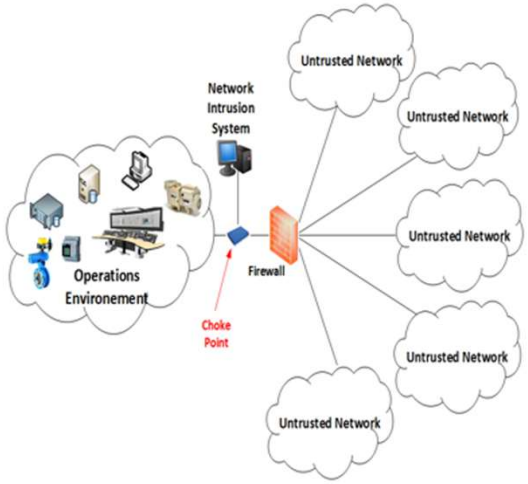
FY25/26 Testing

- CARBON
- **Wolf Creek NPP**

Cybersecurity-by-Design Wireless Technologies Framework Concepts – Defensive Strategies (DS)



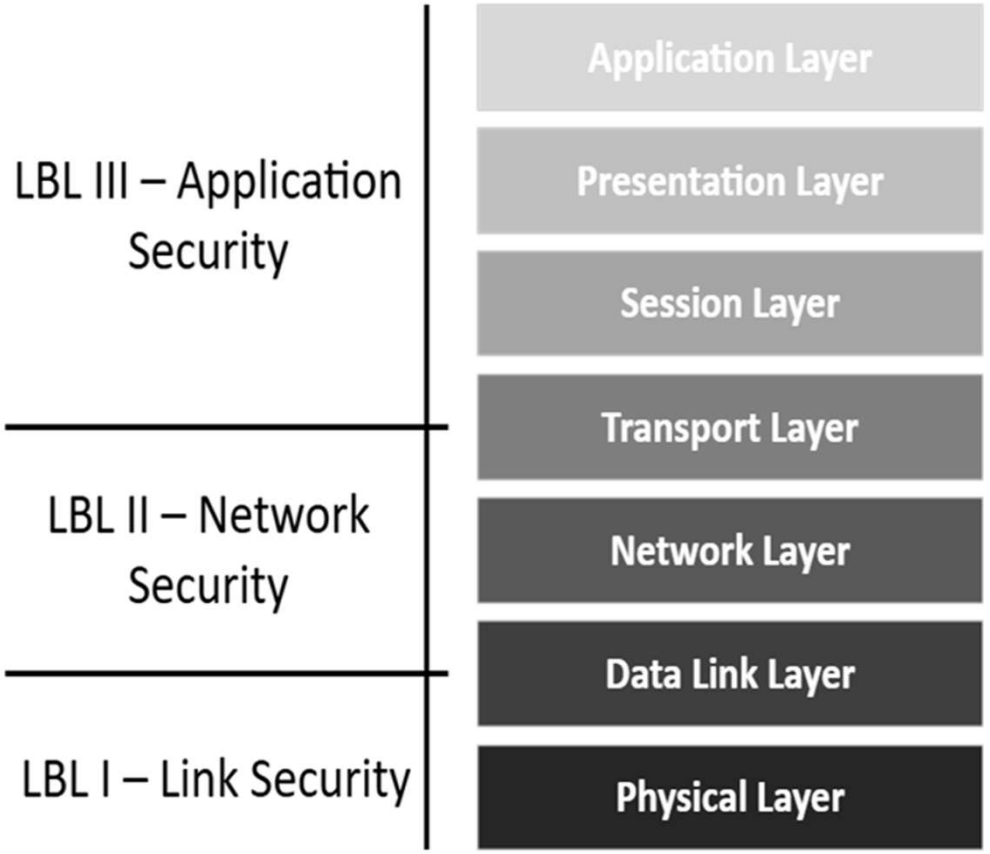
Fortification (F)



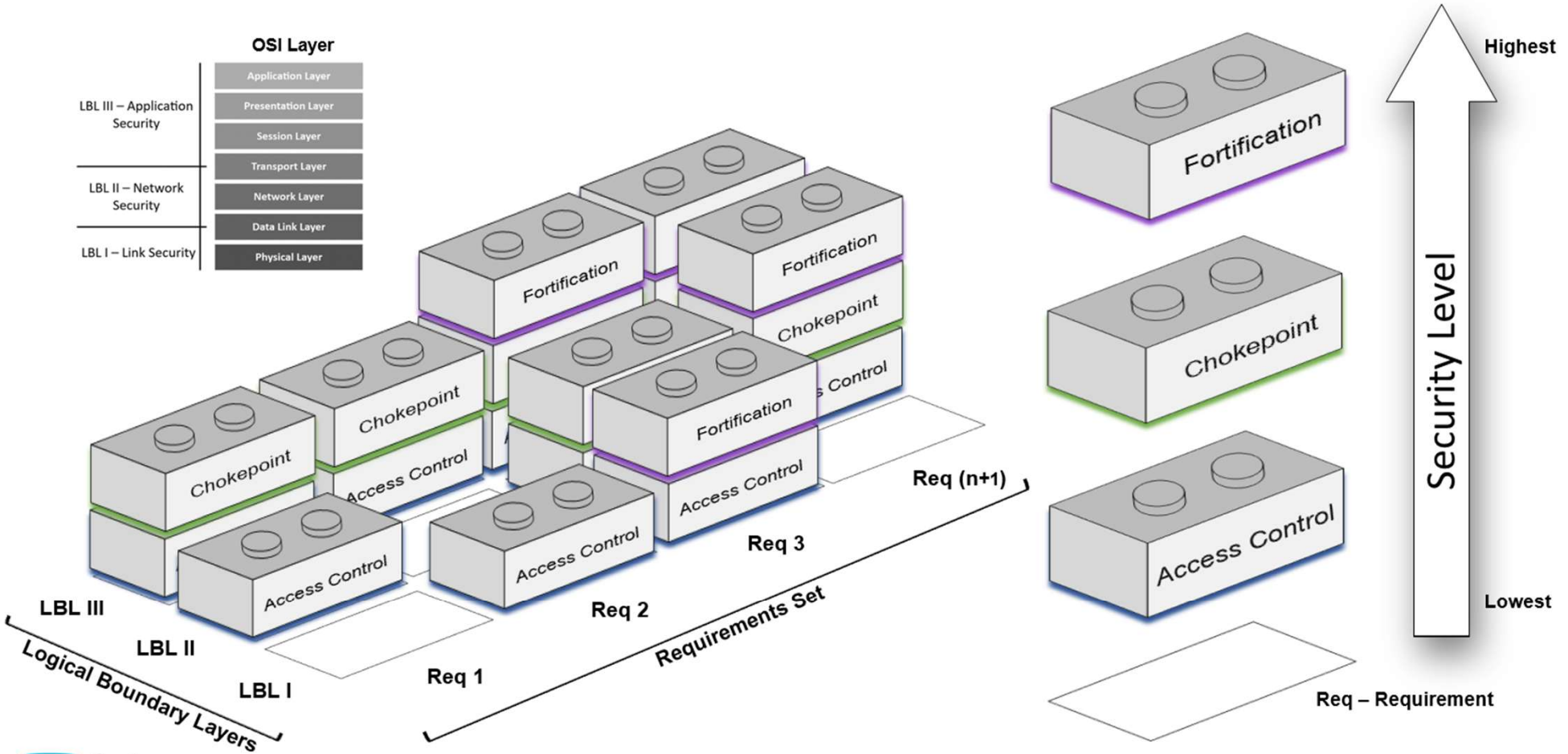
Chokepoint (CP)

Access Control (AC)

Cybersecurity-by-Design Wireless Technologies Framework Concepts – Logical Boundary Layers (LBLs)



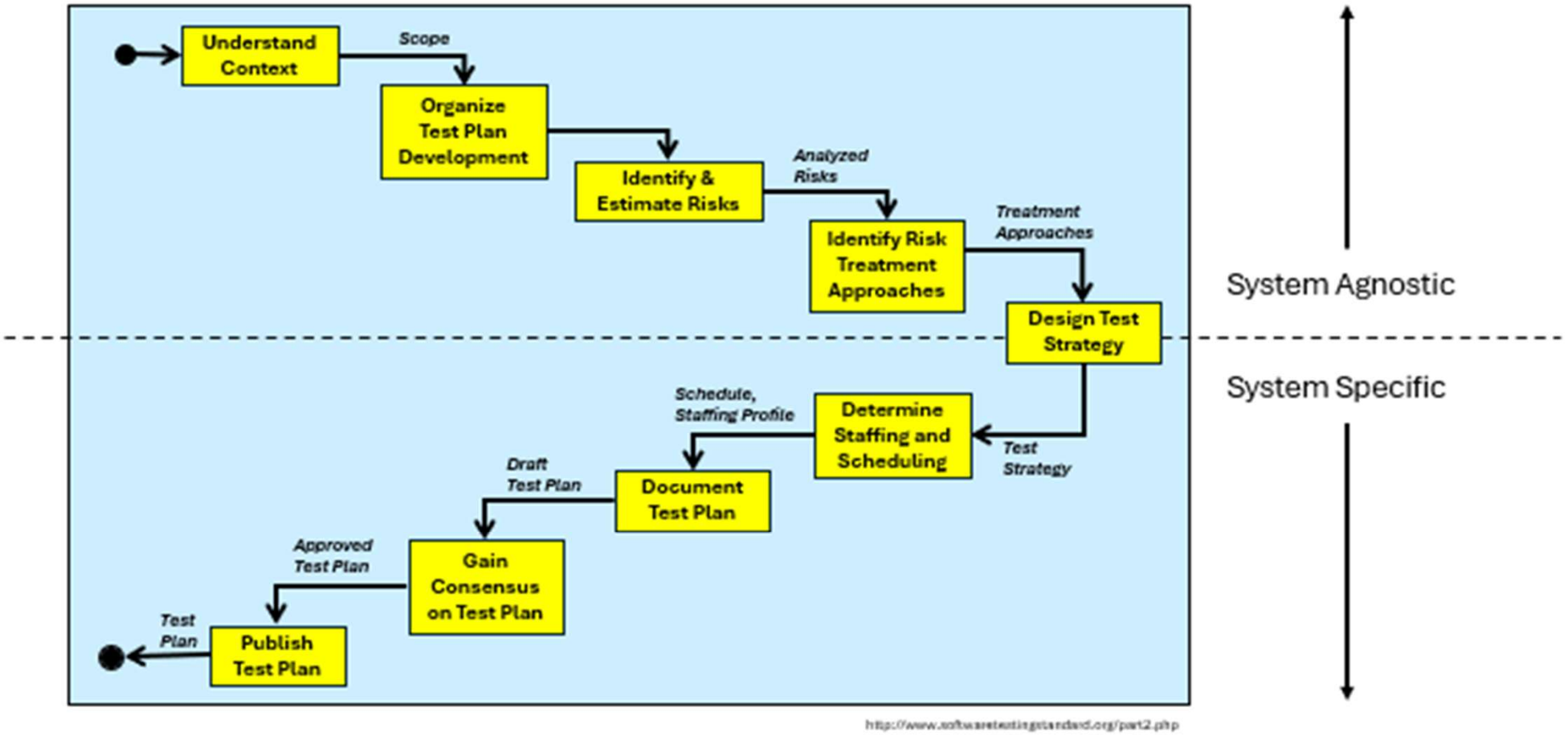
Defense in Depth Strategy



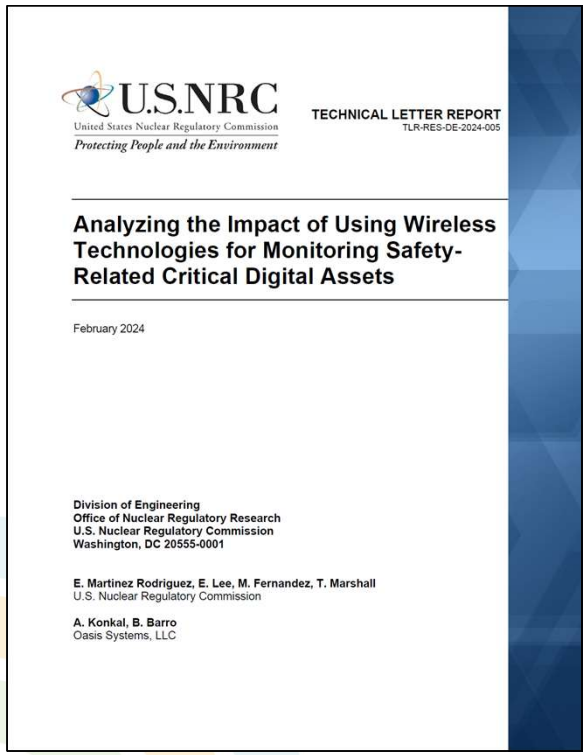
Assumption – All 3 defensive strategies must be implemented to ensure defense-in-depth.

SAND2026-20223PE

ISO/IEC/IEEE 29119-2 Test Planning Process Alignment



Start with NRC TLR Section 5 (p. 21)



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

TECHNICAL LETTER REPORT
TLR-RES-DE-2024-005

Analyzing the Impact of Using Wireless Technologies for Monitoring Safety-Related Critical Digital Assets

February 2024

Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

E. Martinez Rodriguez, E. Lee, M. Fernandez, T. Marshall
U.S. Nuclear Regulatory Commission

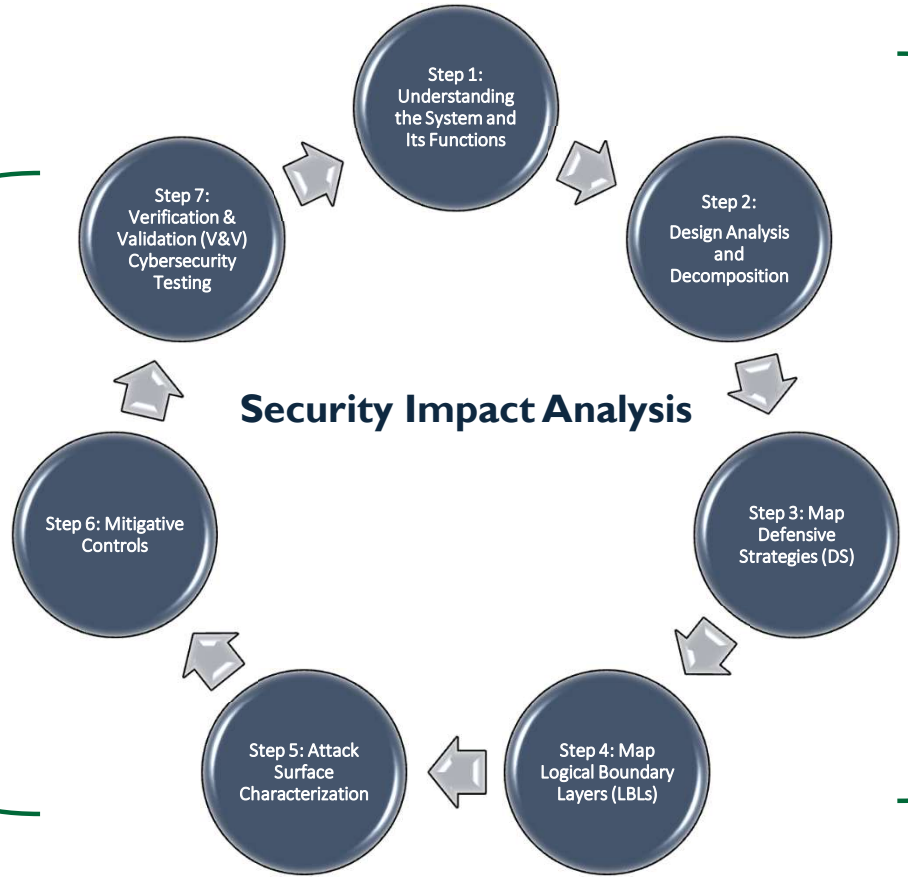
A. Konkal, B. Barro
Oasis Systems, LLC

Understand which elements require documentation review or V&V testing.

5. CRITERIA OR ELEMENTS OF A SECURITY IMPACT ANALYSIS

NRC TLR SIA Elements		
1		The baseline documentation for the proposed wireless network implementation.
	a	The expected as installed baseline configurations, including manufacturer documentation for each type of device, such as the use of any wireless-to-wired gateways, routers, and firewalls or other boundary devices. This information is useful to determine the attack
	b	The acquisition of devices that have wireless (enable or disabled) and the policies and procedures the plant uses to maintain those devices, as well as the qualifications of personnel installing such devices. This information is necessary to assess any possible misconfigurations in the installation and maintenance of wireless devices.
2		The characterization of the attack surface for each wireless device and associated wired pathway, including:
	a	Total number of nodes in the network to determine whether all potential vectors and pathways of attack have been identified.
	b	Characterization of the wireless asset and network to determine whether the licensee has considered all the potential attack vectors and pathways, not just the ones operating under normal conditions. The characterization of the wireless transmitting and receiving capabilities that help identify normal and expected activity of the wireless devices. Transmitters operating at higher or reduced power or transmitting at more frequent intervals are signs of abnormal activity. Changes in receiver signal strength or an increase in noise conditions are indications of rogue devices or unauthorized scanning activity. Some of the information that could help characterize the
	b.i	Knowledge of the operational RF spectrum(s) used by the wireless technologies, including the spectrums the device is capable of operating to understand what the expected RF operating frequencies are. Any RF signals detected outside the normal operating spectrum may be an indication of unauthorized scanning or attempts to establish back channels into the wireless network. The RF spectrum should be monitored so that security controls or processes can be taken to mitigate a cyber threat.
	b.ii	Characteristics from the wireless transmitter and receiver used by a system. Knowledge about the characteristics and capabilities of the transmitters and receivers can aid an adversary to develop targeted cyber threats to a system, such as signal jamming. Information such as the transmitter power range (i.e., the average and peak amount of RF energy per unit power emitted by the transmit antenna) or the receiver sensitivity (i.e., the minimum signal strength, Signal to Noise Ratio, or Signal-to-Noise-And-Interference Ratio required by a receiver to decode an incoming transmission). The transmit power may indicate and affects the area covered by a wireless transmitter, so proper configuration management of components is important for securing a wireless network. A signal may also be jammed by electronic means by targeting a jamming beam at the receiver using a particular known operating frequency that the receiver
	b.iii	Wireless protocol(s) (used and unused), which are required to be documented for all CDAs as part of the CSPs. Unused or insecure protocols can become attack vectors that must be addressed and mitigated.
	b.iv	External antenna placements. It is useful to understand where the potential risks are for broadcasting wireless data further than is necessary for a particular function. Wireless communications can sometimes go beyond the necessary range needed to transmit/receive the data and could provide an opportunity for unauthorized reception of information or unauthorized access to the network. The placement and directionality of radiating antennas also goes to supporting the requirements to preventing any EMI or
	c	All input/output (I/O) capabilities both digital and analog. This information is part of the baseline configuration and it is needed to identify any potential attack pathways to associated systems.
	d	Firmware versions and methods for updating. Documenting firmware revisions is a baseline control requirement. Documenting the methods for updating firmware could factor into portable media management, vulnerability management, software quality assurance, and supply chain requirements.
	e	Device management capability to determine whether the licensee has considered all the attack vectors that could be used to alter the configuration or function of the wireless device. This should include:
	e.i	Methods or operational programs used to manage the individual device configuration settings.
	e.ii.a	Over-the-air programming (OTAP)-A capability that allows a device or devices to be reconfigured or reprogrammed once it is
	e.ii.b	Over-the-air rekeying (OTAR)-A capability in which data signal encryption keys are updated in secure information systems by conveying the keys through encrypted wireless communication channels.
	f	The data flows between the wireless nodes and any wired pathways, including analog connections from digital assets that may influence either connection.
	g	The wireless topology (e.g., star, point-to-point, mesh, ad hoc, etc.) to understand the wireless data flow and whether all potential attack vectors associated with each type of network topology have been considered. For example, the techniques required to monitor a mesh network for intrusion is different than that of a star or point-to-point network.
	h	Information to estimate the potential signal levels and coverage at the highest capable emitter setting for each device (e.g., Heat maps) to determine the overall coverage of the wireless network. This is important to monitor for rogue connections and to know the extent of the signal range that has to be considered to counter an adversary's ability to monitor network traffic remotely.
	i	Equipment required to scan for rogue wireless devices. This is necessary to maintain the capability to effectively monitor the wireless network in all potential modes of the device operation. For example, some devices may have the capability to operate on different RF bands simultaneously. The monitoring equipment should be capable of detecting all modes of operation whether they are configured

Wireless Security Impact Analysis Process

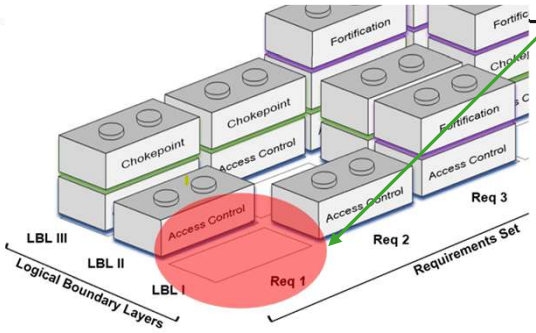


Testing and Evaluation
- Mock Up (SNL)
- On Site (WC)

Wolf Creek Design Engineering Change
- Requirements
- Analysis (as a non-CDA)

Wolf Creek System
- Realization

Example: Design Evaluation and Testing Process



Attack Surface Characterization:

- Identify areas where the attack surface is exposed or DiD is shallow and involves the prioritization of testing of these areas (e.g., LBL I, Requirement RF Propagation Zone)

Control for LBL I Req RF Propagation Zone is containment and Aux building structures.
Structures are anechoic chambers when closed.
Potential for malicious access when open (i.e., during refueling outage)

Determine Mitigative Controls:

- Need access control and detection of attempts to access system at LBL II
- Need fortification of connection requests to the network

Mitigative controls include detection or prevention of connection attempts and fortification of connection requests.

Develop active and passive test plans to collect evidence-based artifacts that confirm:

- Access to LBL I is not possible when equipment and personnel hatches are closed
- Access to LBL I is possible when the hatches are open
- Correct protection of mitigative controls at LBL II and LBL III (detection of access attempts, fortification, etc.)

Types of Attacks Evaluated

I. Direct Attacks
   - Media Access Control (MAC) Spoofing
     - Unauthorized Wireless Access Point (NRC TLR Section 5.2.a)
     - Rogue Device Test (NRC TLR Section 5.2.i)
   - Disruption of the Wireless Transmission Pathway
     - RF Jamming (NRC TLR Section 5.2.b.i, 5.2.b.ii)
   - Denial of Service (DoS)
     - DoS Resilience (NRC TLR Section 5.2.f)
   - Man-in-The-Middle (MiTM)
     - Join Replay (NRC TLR Section 5.2.b.iii)
     - Replay Attack (NRC TLR Section 5.2.b.ii)

II. Indirect Attacks (neither prioritized nor performed)
   - Data Exfiltration
   - Evil Twin

Results & Challenges

- UTGM design and realization can be used as an aid for operational decision making
- Key bases
  - Timeliness of data from UTGM can have high latency – every 90 day surveillance requirement
  - Operational Decisions are only made once the size and shape of the void is confirmed by measurements made by personnel using different equipment
  - Insider Threat Mitigation and RF Propagation Zone (anechoic chamber) credited
  - Additional Recommended Controls implemented and sustained
- NEI 13-10 Rev 7prohibits wireless CDAs from being classified as indirect CDAs
  - Restriction may result in additional costs and resources to assess, implement and sustain full set of controls, regardless of its consequence.

Questions

SAND2026-20223PE