Test Platform Survey and Wireless Test Requirements Outline for Reactor Safety Functions (M3CT-24SN1103063)

Prepared for
US Department of Energy

Michael T. Rowland[1], Sheryl I. Drake[1], Benjamin Karch[1], Romuald S. Valme[1]

[1]Sandia National Laboratories

August 2024
SAND2024-11396R

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

This report aims to progress efforts to develop a framework for a data-driven evidence-based approach to support Advanced Reactor designers and vendors. Specifically, their efforts to leverage wireless technologies for Nuclear Safety, Security, and adjacent functions with an objective to reduce costs, establish a technical basis for investigating use cases such as remote operations and management. These efforts are supported by the changes identified in the Nuclear Regulatory Commission's draft regulatory guide, *DG-5075 Establishing Cybersecurity Programs for Commercial Nuclear Power Plants Licensed under 10 CFR Part 53* [1].

This report builds upon the initial set of thirty-four potential requirements identified in the *Wireless Application Selection Methodology – DOE-NE deliverable M2CT-23SN1104023, SAND2023-10185* [2] report. These initial thirty-four requirements were then analyzed using a taxonomy detailed within a subsequent report, *Assurance Evidence for Wireless Technologies performing Safety Related and Important to Safety Functions, SAND2024-06797R* [3]. This taxonomy leveraged (i) the Tiered Cyber Analysis (TCA) approach detailed in DG-5075 [1], (ii) requirement scope (overall architecture; single system), and (iii) established defensive strategies. The application of this taxonomy resulted in the grouping of twenty-five Tier 2 passive Defensive Cybersecurity Architecture into six groups. Each group of requirements consisted of a set of mutually supporting requirements focused of a particular scope and defensive strategy.

This report details a survey of test platforms and their ranking for use to evaluate a set of requirements for use of wireless technologies to perform safety functions of Advanced Reactors (AR). This report provides a test outline for each of the six groups to ensure that all identified requirements necessary to establish the defensive strategy for the group scope have been implemented. In a classical example, a fortification, such as a fortification wall would demand requirements for (i) type of material, (ii) height, (iii) depth, (iv) bastions for guards, etc. This group of requirements would need to be fully implemented before evaluating the value of the fortification wall to security. In a similar manner, each group of requirements will need to be implemented within a design to holistically evaluate the benefit of those requirements to a defensive strategy and scope for securing wireless technologies.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The implementation of wireless technology in commercial nuclear power plants has been limited to equipment data collection for monitoring activities that are not part of operational decision making. The limited implementation of wireless technology has been partially the result of uncertainties with plant operation and safety system impacts which could occur and also due to cybersecurity regulations which do not permit the use of wireless in significant safety systems.

Recent developments such as the NRCs desire for risk-informed, performance-based security designs, and draft regulations have increased the potential for wireless technologies to be perform Nuclear Safety functions at Nuclear Power Plants (NPP). This report aims to progress efforts to develop a framework by which design, implementation, operations, and maintenance efforts are identified and supported by a technical basis to eliminate all restrictions on wireless technology use within an Advanced Reactor.

Achieving this objective may also enable future efforts to advance remote operations and management due to the high reliance of wireless cybersecurity on logical boundaries and the cryptosystems that establish and defend these boundaries. This objective will demand (i) development and evaluation of novel defensive architectures, (ii) assessing the associated strategies, and (iii) testing of controls (e.g., cryptosystem, diversity, independence) to protect wireless communications from cyber-attack to ensure that the safety functions are appropriately protected.

This report builds upon two previous reports (i) *Wireless Application Selection Methodology – DOE-NE deliverable M2CT-23SN1104023, SAND2023-10185* [2] report ("Requirements Report") and (ii) *Assurance Evidence for Wireless Technologies performing Safety Related and Important to Safety Functions, SAND2024-06797R* [3] ("FY24 Report"). Logical Boundary Layers (LBL) are an important proposed concept for simplifying future testing and evaluation. The activities and results of each report are identified in the figure below:

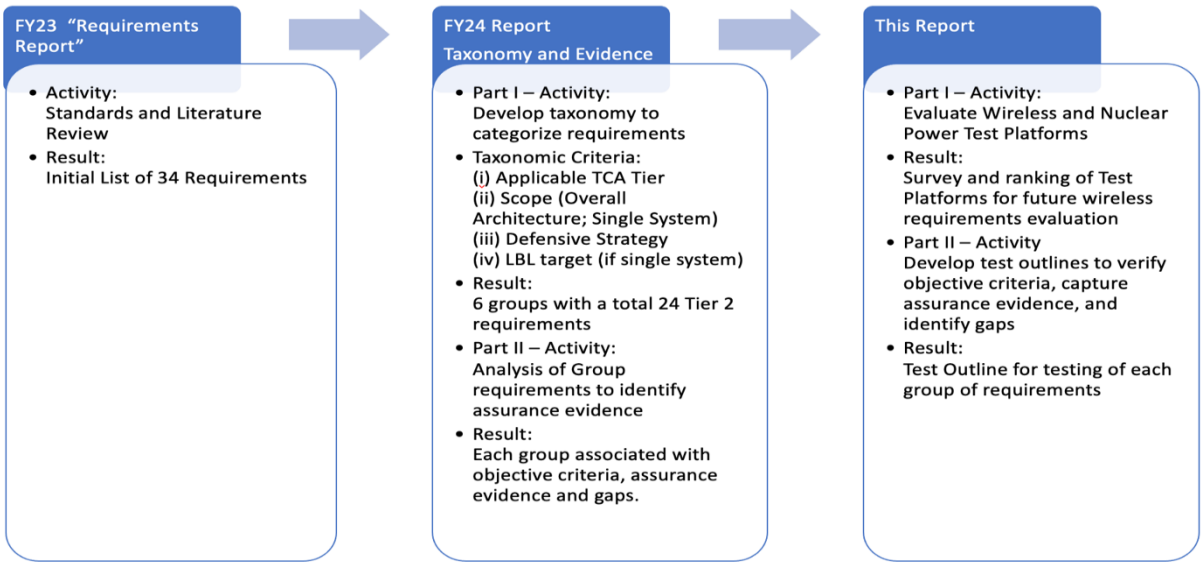

Figure 1: Wireless Technology for Safety Functions Reports

The Requirements Report [2] found that no single international or national standard exists that provides a complete and correct set of requirements for wireless used in Safety Related (SR), Non-

Safety Related with Special Treatment (NSRST), and Important to Safety (ITS) functions. Cybersecurity regulations of many International Atomic Energy Agency (IAEA) member states prohibit the use of wireless for most (if not all) Nuclear Safety functions. Consequently, wireless has not been adopted for these systems, and consequently there is no operational experience for the use of wireless technologies performing safety functions with the existing United States Commercial Reactor Fleet.

The initial set of requirements within the Requirements Report [3] were identified and adapted from the following standards and guidance publications:

i. IAEA Nuclear Security Series [4, 5]
ii. International Electrotechnical Commission (IEC) Nuclear and OT Cybersecurity Standards (e.g., IEC 62645; IEC 62443) [6, 7, 8, 9]
iii. Nuclear Energy Institute (NEI) Publications and formal communications with NRC [10, 11]
iv. Canadian Cybersecurity Standard for Nuclear Facilities, CSA N290.7:21 [12]
v. United States Nuclear Industry Wireless Cybersecurity Reports [13]
vi. International Organization for Standardization (ISO) / IEC Cryptographic modules standards (i.e., ISO/IEC 19790) [14]
vii. National Institute of Standards and Technology (NIST) Publications [15, 16, 17, 18]
viii. European Telecommunications Standards Institute (ETSI) Publications [19, 20]
ix. Internet Engineering Task Force (IETF) Request for Comments (RFC) [21, 22]
x. Cryptography Publications [23, 24]
xi. Wireless Security Architecture Publication [25]
xii. NRC Regulatory Guide [26][1]
xiii. ISO/IEC 27000 series [27, 28][2]
xiv. Institute of Electrical and Electronics Engineers (IEEE) Standards [29, 30][3]

The FY24 Report [3] developed a taxonomy for grouping mutually supporting requirements together to simplify test and evaluation of candidate wireless technologies to perform critical functions in Advanced Reactors (AR). The FY24 report provided an assessment of the initial requirements identified in the Requirements Report [2] by (i) applying the tiered cybersecurity analysis (TCA) outlined in the United States Nuclear Regulatory Commission's draft Regulatory Guide DG-5075 [1], to identify and document the rationale for assignment to Tier 2 (passive; prevention of access) or Tier 3 (active defense; denial of task) defensive measures; (ii) application of the taxonomy to these requirements resulting in six distinct groups.

[1] NRC Regulatory Guide 5.71 was reviewed, however NEI 08-09 [10] adequately justified the inclusion of all requirements identified in Reg Guide 5.71.
[2] Some ISO/IEC 27000 series standards were reviewed, however IEC 62645 [7] adequately justified the inclusion of all requirements identified in ISO/IEC 27000 series.
[3] Some IEEE standards were reviewed, however other publications (e.g., NIST, IETF, ETSI) adequately justified the inclusion of all requirements identified in ISO/IEC 27000 series.

The key criteria of the developed taxonomy are:

i. Applicable TCA Tier

ii. Scope – overall architecture or single system

iii. Associated Defensive Strategy (i.e., fortification, access control, chokepoint, deception)

iv. If single system scope, LBL target. For example, LBL I associated with physical media and encoding/decoding functions are expected to be highly targeted for deny and distort impacts, whereas LBL III is expected to be highly targeted for deceive impacts.

Each group or requirements have common testing and evaluation demands, based upon a specific attack target, and established defensive strategies. The taxonomy simplifies evaluation of the groups of requirements as well as ensuring that mutually supporting requirements (i.e., those within a single group) are tested and validated (or invalidated) holistically to ensure wireless technologies cybersecurity.

Previous work identified a major challenge for wireless technology adoption is the increased complexity of these technologies and the assumption that logical boundaries are monolithic, offering no opportunity to group requirements and simplify testing of key parts of the logical boundaries. The FY24 Report [3] introduced three Logical Boundary Layers (LBLs) based upon functions performed by each LBL (see Table 1 below).

For ideal wireless communications network, these LBLs can be independently and directly targeted by the adversary, LBLs are a significant novel concept for grouping requirements and simplifying development of test cases. LBL I are strongly associated with physical signal (media) interference, distortion, and/or deny (jamming) attacks. LBL II is strongly associated with deceive attacks trying to bypass or spoof authentication credentials. LBL III is associated with disclose and deceive attacks aimed at interacting with the sensitive data and information relied upon by the Nuclear Safety function. However, the FY24 Report [3] found that all of the thirty-four requirements from the Requirements Report [2] as well as current implementations of cryptosystems, implement LBL II/III in an integrated manner.

Table 1: LBL Functions

LBL	LBL Functions
III	• Information exchange after successful secure channel establishment • Encryption and Decryption of data (e.g., Commands, sensor and actuator values) directly used for performance of the Nuclear Safety Function
II	• Cryptographically controls access/authentication to the wireless network • Handshaking to establish secure channel • Logical Network Management
I	• RF Signal Propagation • Transceiver encoding/decoding • RF Channel Management

This report draws heavily from the Requirements Report [2] and the FY24 Report [3], with the starting point being the six groups of requirements, the objective criteria associated with each group and the associated assurance evidence. This report also provides a ranked survey of test bed platforms that could support future testing and evaluation activities. The testing and analysis aim to support further development of the framework and refinement of the initial list of requirements.

The overall goal of these efforts is to provide a risk-informed performance-based framework to design, implement, validate, operate, and maintain wireless technologies for Nuclear Safety functions of Advanced Reactors. As Nuclear Safety functions have the most stringent regulation and requirements, the framework is expected to have utility for Nuclear Security, adjacent to safety, and balance of plant functions.

ACRONYMS AND TERMS

Acronym/Term	Definition
4G	Fourth Generation Mobile Communications (e.g., Long Term Evolution – LTE)
5G	Fifth Generation Mobile Communications
AEAD	Authenticated Encryption and Associated Data
AR	Advanced Reactor
CEAS	Cyber-Enabled Accident Scenarios
CFR	Code for Regulation
CPS	Cyber-Physical System
CSP	Cybersecurity Plan
DCSA	Defensive Cybersecurity Architecture
DG	Draft Guide
DiD	Defense in Depth
DMZ	Demilitarized Zone
DOE NE	Department of Energy Office of Nuclear Energy
E	Emulation
EAP	Extensible Authentication Protocol
ETE	Experiment Test Environment
FT	Field Testing
FY	Fiscal Year (1-Oct to 30-Sept)
HBOM	Hardware Bill of Materials
HitL	Hardware-in-the-Loop
ICS	Industrial Control System
IDS	Intrusion Detection System
IPSec	Internet Protocol Security
IT	Information Technology
ITS	Important to Safety
I&C	Instrumentation and Control
KDF	Key Derivation Function
LBL	Logical Boundary Layer

Acronym/Term	Definition
MAC	Medium Access Control
MCU	Micro-Controller Unit
NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSRST	Non-Safety Related with Special Treatment
OSU	The Ohio State University
PAWR	Platforms for Advanced Wireless Research
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
POWDER	Platform for Open Wireless Data-driven Experimental Research
PSK	Pre-Shared Key
PWR	Pressurized Water Reactor
QoS	Quality of Service
RF	Radio Frequency
RG	Regulatory Guide
SBOM	Software Bill of Materials
SeBD	Secure By Design
SMaHTR	Small Medium advanced High Temperature Reactor
SNL	Sandia National Laboratories
SR	Safety Related
STEC	Sensor Test and Evaluation Center
STPA	System Theoretic Process Analysis
TCA	Tiered Cybersecurity Analysis
TLS	Transport Layer Security
TTP	Tactics, Techniques, and Procedures
UCA	Unsafe Control Action
UIUC	University of Illinois- Urbana-Champaign
VLAN	Virtual Local Area Network
WPA	Wi-Fi Protected Access

1. INTRODUCTION

Wireless technologies have long been proposed to reduce costs and provide scalable communications architecture to support innovation in Nuclear Power Plant (NPP) systems and support new and novel use cases for Advanced Reactors (AR). However, despite ubiquitous wireless technology integration into everyday life, it has yet to be widely deployed in instrumentation & control (I&C) systems of regulated industries, including commercial NPPs [31]. The key challenge with the adoption of wireless technologies for Safety functions within NPPs (both existing and advanced) is associated with complying with elements of Defensive Cybersecurity Architecture (DCSA).

However, as the use of wireless technologies reduces or in some cases eliminates the physical boundaries where a system or device can be accessed, there could be a greater risk of exposure of the function(s) of the device or system to adversaries not authorized to access the physical locations where the devices or systems are located/used. It is then essential to ensure that a proposed wireless infrastructure design meet the safety, security, and reliability requirements for use in AR deployments. Thus, a demonstration to meet a set of established acceptance criteria for each of the requirement groups would benefit both specific use case acceptance and a wider acceptance for a range of applications.

The 2023 "Wireless Application Selection Methodology – DOE-NE deliverable M2CT-23SN1104023; SAND2023-10185" [2] report identified thirty-four wireless security requirements which were subsequently evaluated using a tiered cybersecurity analysis (TCA) methodology in the FY24 report "*Advanced Reactor Safeguards & Security Assurance Evidence for Wireless Technologies Performing Safety-Related and Important-to-Safety Functions.",* [3] hereafter referred to as the "FY24 Report". The TCA is a three-tier cybersecurity assessment methodology based on the requirements of 10 CFR 73.110 [1], proposed by the U.S. NRC. TCA integrates domestic and international standards to select Secure by Design (SeBD) requirements for developing defensive network architectures and effective cybersecurity controls.

TCA Tier 1 evaluates the facility's design basis, passive features, and physical elements to prevent cyber-enabled accident scenarios (CEAS) by leveraging the inherent physics of the plant design. System Engineering approaches, such as System Theoretic Process Analysis (STPA), can also assist in this evaluation. Tier 2 conducts an attack pathway analysis, excluding supply chain pathways, to identify and categorize functions, evaluate attack pathways, and specify passive measures to prevent adversary access. This tier results in the identification of passive or deterministic defensive cybersecurity architecture (DCSA) or Cybersecurity Plan (CSP) elements. Tier 3 focuses on active protections, implementing measures such as detection, delay, response, and recovery to thwart adversary tasks. This tier includes baseline controls for broad information security assurance and risk-informed controls for specific risks, with STPA Unsafe Control Actions (UCAs) informing hazard scenarios [3].

The assessment and classification of each of the 34 wireless security requirements followed four major steps. First, each requirement was evaluated for is applicability to a Tier level, sorting between Tier 1, 2, and 3 requirements. 25 of the initial 34 requirements were categorized as Tier 2. These 25 Tier 2 requirements were then categorized based upon a taxonomy detailed in the FY24 Report [3] resulting in the identification of 6 distinct groups:

- Groups 1 – 2 (Overall Architecture)

- Group 1 – Fortification – requirements focused on increasing the number of independent and diverse fortification layers within the overall architecture. For example, NRC RG 5.71 [1] identifies five layers (Level 4 to Level 0).
- Group 2 – Chokepoint – requirements focused on creating chokepoints within two layers of the architecture. Chokepoints are conduits of communication between these two layers and will have graded security requirements based on the layers that the chokepoint connects.

- Groups 3 – 6: (Single System/Zone)
  - Group 3 – Logical Boundary Layer (LBL) I[4] – Fortification – requirements focused on design and configuration of wireless communications via physical characteristics (e.g., signal power, frequency hopping) and encoding/decoding elements (e.g., error-correcting codes). The objective is to enhance resilience and provide robustness against attacks targeting LBL I.
  - Group 4 – LBL 1 – Access Control – requirements focused on limiting adversary access to the wireless communications across the physical medium (i.e., air). This may include structures and measures meant to attenuate wireless communications or limit propagation of signals past a physical boundary.
  - Group 5 – LBL II/III – Fortification – requirements focused on design, implementation, and configuration of cryptosystems, specifically their authentication, integrity protection, and encryption functions, to enhance resilience against distort and deny attacks, and significantly reducing or eliminating the potential and duration of disclose or deceive attacks. The rationale for combining LBL II (Authentication) and LBL III (Integrity/Confidentiality) is that most cryptosystems, like those that provide Authenticated Encryption and Associated Data (AEAD) implement LBL II/III in a single cryptosystem.
  - Group 6 – LBL II/III – Access Control – requirements focused on limiting access to wireless communications of a specific system to only authenticated entities.

Lastly, each group of requirements were analyzed within the FY24 Report [3] to: (i) enumerate objective criteria; (ii) identify assurance evidence associated with the objective criteria, and (iii) listing gaps or limiting factors for testing.

This report presents a high-level test framework to assess and validate the identified wireless security requirements from the FY24 Report [3]. As part of this effort, several testing site facilities were evaluated for their suitability to evaluate wireless network security requirements specifically for use in AR sites which is presented in Section 2, "Testing Site Surveys". Section 3. "Testing Objectives" provides further description of requirements groups 1-6, with associated testing scenarios applicable to those groups. Section 4 "Conclusion" summarizes all efforts completed to data and summarizes potential future work to further evaluate and testing of selected group requirements. Appendix A, Test Platform Surveys contains supplemental information on the Test Platforms assessed.

[4] LBLs were proposed in the FY24 Report [3] to group requirements and simplify future evaluation and testing of these groups. LBLs are summarized in the Executive Summary and Table 1 of this report.

2. TESTING SITE SURVEYS

Multiple testing platforms were reviewed to assess their capability in evaluating wireless security requirements for advanced reactor communications. Several criteria were considered, including the ability of the test system to utilize either advanced reactor (AR) or nuclear power plant (NPP) control simulators, the fidelity level of the test system (emulator, simulator, Hardware-in-the-Loop (HitL), or a combination (hybrid)), and the ability to test wireless environments, primarily 802.11. Additionally, the feasibility and associated level of effort required by the providing organization to have the testbed ready by Q3 FY25, or Q3 FY26 for red and blue-teaming activities was reviewed.

Of those platforms surveyed, two Platforms for Advanced Wireless Research (PAWR) were evaluated including the Platform for Open Wireless Data-driven Experimental Research (POWDER), which allows for the ability to test physical 4G and 5G-based devices in urban and campus settings, and Colosseum, which enables large-scale wireless network emulation and data analytics. Three university-based test platforms focusing on advanced reactor and/or NPP simulation software were evaluated for their ability to integrate wireless communications into their test systems which included testing sites at Georgia Institute of Technology (Georgia Tech), Ohio State University, and a joint venture between Purdue and the University of Illinois at Urbana-Champaign (UIUC). Two testing platforms with Sandia National Labs (SNL) were also evaluated for their suitability to test wireless communications requirements in AR architectures which included Emulytics™/SCEPTRE which provides significant emulation capabilities for Industrial Control Networks (ICS), Sensor Evaluation and Test Centre (STEC), and Experiment Test Environment (ETE). While still in development, the ETE will integrate HitL functionality with Emultyics™ analytics capabilities. Additionally, possible testing utilizing NuScale Power's control simulator software was investigated, and future work to engage with Comanche NPP for on-site field testing is under consideration.

Table 2-1 presents a summary of test platform surveys which document the primary technology focus of the testing platform, the types of tests supported (emulation - E, physical device Hardware-in-the-Loop testbed -HitL, on-site field testing - FT, or a combination of types), the maturity level of the platform, Availability, and applicable comments. Maturity level considered the organizations experience with conducting cybersecurity experiments, processes, and effort to modify the testbed and orchestrate tests, and fidelity of the testbeds.

This summary offers a variety of potential testing platforms, serving as a reference for future evaluations and the selection of appropriate test systems based on a formalized test plan. From the conducted surveys, the SNL Emulytics™ emulation system utilizing elements of the PAWR Colosseum test system presents the best option for Requirement Groups 1 and 2 due to the level of maturity, availability, and capability alignment. Similarly, from the survey data, SNL STEC, in conjunction Emulytics™ with possible passive Comanche Peak NPP 802.11 testing provides the best testing platform options for Requirement Groups 3, 4, 5 and 6. Additionally, Appendix A provides further detail regarding each test capabilities and focus for reference.

Table 2: Test Platform Survey Group Requirements

Test Facility	Requirements Group Focus	Technology Focus	Type (E, HitL,FT)	Maturity	Availability	Comments
SNL: Emulytics™ / SCEPTRE	1,2	ICS Reactor Simulation	E, HitL	High	Current	Sandia National Labs (SNL) Emulytics™ provides emulation, simulation, modeling and analysis of various infrastructure and network elements can be used in conjunction with SNL SCEPTRE (ICS emulation). Can provide 802.11 emulation services. Platform is available and mature based upon its designed focus with low fidelity AR (SMaHTR) and PWR (Asherah) simulation. Suitable for generic overall architecture testing and single system LBL II/III that does not require field testing. Combination with Open-source PAWR – COLOSSEUM elements, if possible, would result in Emulytics™ being the preferred testbed for Emulation testing.
SNL STEC	3,4,5,6	ICS PPS Reactor Simulation	HitL, E, FT	High	Current	Sensor Test and Evaluation Centre (STEC) provides secure locations for aggressive wireless testing with connections to various infrastructure (e.g., CARBON wireless, Physical Protection System) and network elements can be used in conjunction with SNL SCEPTRE (ICS emulation). Platform is available and mature based upon its designed focus with low fidelity AR (SMaHTR) and PWR (Asherah) simulation. Suitable for single system groups. Combination with Open-source PAWR – COLOSSEUM elements, if possible, would extend testing to overall architecture groups.

Test Facility	Requirements Group Focus	Technology Focus	Type (E, HitL,FT)	Maturity	Availability	Comments
The Ohio State	3,4,5,6	Reactor Simulation Digital Twin	E, HitL	Medium	Current	Provides a iPWR reactor testbed for both reactor physics and control evaluation. Ability to integrate 802.11 physical device testing with physical mock-ups available. Possible ability to integrate with PAWR – Colosseum facility for enhanced data analysis capabilities. Platform is available and mature based upon its designed focus, but work could be required to support specific test plans. Suitable for all groups of testing; significant effort necessary to modify networks and implement HitL due to maturity of processes.
PAWR: POWDER	3,4,5,6	4G,5G	HitL,E	High	Current	Mockup, Field facility. Limited support for 802.11, with most support for 4/G 5G devices testing coverage (Software Defined Radios with some ability to test latency and performance with physical radio devices. No native AR or NPP simulation / emulation capability. Platform is available and mature based upon its designed focus. Suitable for generic single system testing, LBL I, and cryptosystems associated with 4G/5G mobile communications.
PAWR: Colosseum	3,4,5,6	4G, 5G, 802.11	E	High	Current	Virtual, Emulation Environment. Emulation available for 4G, 5G and 802.11 systems. Can support SNL supplied ICS data for testing. Possible ability to integrate emulation capability with some University partner AR / NPP digital twin emulator data. No native AR or NPP simulation / emulation capability. Platform is

Test Facility	Requirements Group Focus	Technology Focus	Type (E, HitL,FT)	Maturity	Availability	Comments
						available and mature based upon its designed focus. Suitable for generic overall architecture testing and single system LBL II/III that does not require field testing.
Comanche NPP	3,4,5,6	802.11	FT	Medium	FY25	Allows for field testing of wireless technology at working NPP field site. On-site testing would require significant coordination with, and documented approvals from stakeholders regarding testing scope and involved systems. Provides the greatest level of testing fidelity being a field trial site. Suitable for single system testing LBL I and LBL II/III disclose tests, potential for passive access control measurements. Active penetration testing may require mockups at SNL facilities. Acquire design and mock-up system for more active testing at STEC.
Purdue -UIUC	3,4,5,6	Reactor Simulation Digital Twin	HitL,FT	Medium	Current	Field Facility with HitL. Provides a reactor testbed for both reactor physics and control evaluation. Ability to integrate 802.11 physical device testing with physical mock-ups available. Possible ability to integrate with PAWR – Colosseum facility for enhanced data analysis capabilities. Platform is available and mature based upon its designed focus, but work could be required to support specific test plans. Suitable for single system testing LBL I and LBL II/III disclose tests, potential for passive access control measurements. Active penetration testing may require mockups at SNL facilities.

Test Facility	Requirements Group Focus	Technology Focus	Type (E, HitL,FT)	Maturity	Availability	Comments
Georgia Technical Institute (Georgia Tech)	3,4,5,6	Reactor Simulation Digital Twin	E, HitL	Low	FY25/6	Provides a reactor testbed for both reactor physics and control evaluation. Ability to integrate 802.11 physical device testing with physical mock-ups available. Possible ability to integrate with PAWR – Colosseum facility for enhanced data analysis capabilities. Platform is available and mature based upon its designed focus, but work could be required to support specific test plans. Ongoing DOE NE UP would lead to network digital twin of an AR. Currently, not suitable for wireless technology testing until post FY26.
SNL: ETE/ Emulytics™	3,4,5,6	ICS Digital Twin, Reactor Simulation	HitL,E	Low	FY25/6	SNL ETE extends the capabilities of Emulytics™ to include HitL ICS devices for greater test fidelity and realism. Future work would be required to integrate 802.11 technology into the ETE lab environment. ETE is a developing lab with more capabilities to be added in FY25/F6. Currently, not suitable for wireless technology testing until post FY26.
NuScale Power	3,4,5,6	Reactor Simulation Digital Twin	E	Low	FY25/6	NuScale Power provides emulation and simulation software for their reactors (operator training, physics validation and controls testing purposes). 802.11 testing and simulation capabilities are not native to the simulation platform and would require work to integrate this function. Platform is available and mature based

Test Facility	Requirements Group Focus	Technology Focus	Type (E, HitL,FT)	Maturity	Availability	Comments
						upon its designed focus, but work could be required to support specific test plans. Currently, not suitable for wireless technology testing until post FY26. However, wireless system design could be acquired from NuScale and Mocked up in STEC for Single System/Zone testing.

3. TEST OUTLINES

The validation of wireless technology cybersecurity requirements for advanced nuclear power plant (NPP) design are critical to ensuring the safety, reliability, and resilience of the facility. Testing scenarios with platform considerations and suggested collected artifacts for Requirement Groups 1 through 6 are presented in Sections 3.1 through 3.6.

The possible expected results of the tests are as follows:

1. All tests and analyses "meet expectations" and are successful.
   a. All objective criteria are achieved.
   b. No tests failed.
   c. Analysis of the assurance evidence validates the objective criteria thereby providing evidence that the Group of requirements are complete and correct for its target and defensive focus.
2. All tests "meet expectations". However, analyses of the evidence have some discrepancies.
   a. Some objective criteria are achieved.
   b. No tests failed.
   c. Analysis of the assurance evidence validates some objective criteria under certain conditions.
   d. Evidence gathered does not provide proof that objective criteria will be met under all conditions (e.g., Gaps may exist).
   e. Group of requirements has evidentiary support but may require modification to cover gaps, specification of additional requirements, or dependency on other groups of requirements or those in Tier 3.
3. Some tests fail to meet expectations and test analysis gives evidence of fails.
   a. Tests fail to produce the evidence expected (i.e., fails).
   b. Collected evidence demonstrably invalidates the requirement. Error in requirements sorting and grouping or invalidation of requirement(s).
4. All tests and analyses fail.
   a. All tests fail to produce the evidence expected (i.e., fails) indicating requirements group is invalid.
   b. Collected evidence demonstrably invalidates the requirement. Error in requirements sorting and grouping or invalidation of requirement(s).
5. Inconclusive results (none of the above).

3.1. Group 1 Requirements – Overall Architecture – Fortification

Group 1 requirements apply to overall architecture (i.e., system of systems) and impose key constraints on design to ensure sufficient diversity and independence. The key assumption is that independent and diverse wireless technologies will increase demands on the adversary to acquire greater disclose or disrupt resources, technical knowledge, and new Tactics, Techniques, and Procedures (TTP).

3.1.1 Test Summary

The test will consider a baseline of a single wireless technology with identical security controls but with differing configurations. For example, 3 Wi-Fi networks having different WPA passphrases or

other protections will be evaluated prior to enabling the fortification requirements and then again after. A red team will be provided with access to all three networks with a goal of minimizing number of resources, technical knowledge, and new or diverse TTP.

The modified topology will then change the wireless technologies for the small and medium sized networks to evaluate the benefit of independent and diverse wireless technologies for fortification of defensive layers. The safety importance of each wireless network is assumed to be inversely related to the number of components of each network.

3.1.1. Adversary Characterization

The adversary will have access to the large network technology and will be able to deploy multiple disclose and disruption resources within the boundaries of the wireless technology.

Adversary can interact with wireless technologies but begins with zero system knowledge of the targets.

3.1.2. Group 1 Requirements [2]

1. Establish and define zones to protect sensitive digital assets, and their wireless communications, if any, based upon a trust model or defensive strategy. In this instance, zones require physical and logical boundaries, with the addition of a logical boundary adds an additional requirement beyond the best practice of only employing physical boundaries
2. Wireless technologies employed within a zone assigned at one security level should be different from those employed at other zones assigned in other security levels. This includes:
    - Signal propagation properties, including signal encoding (physical layer): Characteristics of signal propagation need to be evaluated to ensure that no single adversary action can result in an acceptable consequence resulting from a 4D impact.
    - Cipher Suites: Compromise of one cipher suite shall not impact other zones assigned other security levels. Cipher suites need to be informed by data flows and communications as well as the DCSA and key management processes.
    - Components, including those used for network and communications protections: common vulnerabilities shall be eliminated between zones assigned other security levels.
3. Wireless technologies and their attributes, such as those identified in requirements (2) above, employed within SR functions shall be diverse from one another (adapted from the Requirements Report [2]; DCSA requirement applied to different systems performing Cateogry A functions).
4. A SR function shall employ redundant, diverse, and independent wireless technologies to support critical communications (adapted from the Requirements Report [2]; requirement is addressing a single system).
5. Technical and physical control measures protecting and monitoring the wireless communications shall be located within the zone or at the physical or logical boundaries of their assigned zone.

   The following events should be monitored:
   – new device connecting to the network;
   – output power of wireless devices;

– transmission delay variations (especially for mesh networks);
– unusual battery discharge rate [6][5].

3.1.3. Baseline configuration

Objective Criteria / Cybersecurity Demands Group 1

1. Multiple logical and physical boundaries fortify the overall cybersecurity of an NPP. A single boundary failing or being bypassed by the adversary will not result in unacceptable consequences.
2. Adversary scenario complexity will be increased to overcome multiple logical and physical boundaries while assuming the system or device performing an SR function is susceptible to a publicly known exploit.
3. Diversity provides fortification against a single access, attack, vulnerability, or tool being used to degrade more than one or all layers of Defense in Depth (DiD). Diversity increases the challenges on the adversary to acquire more knowledge, access, and resources to disrupt or disclose information of multiple layers of DiD.

3.1.4. Group 1 Assurance Evidence [3]

i. Adversary task time, adversaries need to acquire diverse means and capability for the adversary to compromise systems performing SR functions.
ii. Increase in failed attempts to compromise, bypass, or degrade boundaries.
iii. Increase in number of resources the to deploy and use for adversaries to achieve Disclose or Disrupt impacts.
iv. Step increases based upon the number of multiple logical and physical boundaries.
v. Adversary task time to gain sufficient knowledge on the diverse systems or technologies; thus requiring deployment of different, multiple disclose resources
vi. Increase in failed attempts to compromise, bypass, or degrade diverse boundaries when compared to homogenous boundaries.
vii. Increase in number of resources necessary for the adversary to deploy and use when compared to homogenous boundaries.
viii. Step increases based upon the number of diverse logical and physical boundaries.
    a. Signal Propagation – requires additional RF frequency antennas and devices.
    b. Cipher Suites – protection against deceive and disclose attacks will be enhanced.
    c. Components – common vulnerabilities can be eliminated across diverse zones.
ix. For Safety Related Functions
    a. Unique Hardware Bill of Materials between the two technologies (no common component).
    b. Unique Software Bill of Materials between the two technologies (no common component).
    c. Unique Cipher Suites.

[5] IEC 62988:2018 [6] defines the following terms:
1Network: A series of devices connected by some type of communication medium
Wireless device: A device that is able to establish a wireless communication with another wireless devices, that may or may not be part of a wireless network.

d. Unique Protocols.

x. LBL I associated evidence:
   a. Electromagnetic compatibility between the two technologies.
   b. Single disruption resource (even multi-antennae) could not achieve Deny or Distort impact on both technologies.

xi. LBL II/III associated evidence:
   a. Cryptosystem attacks do not affect both technologies.
   b. Key acquisition of one technology does not expose cryptographically protected information of the second technology.

xii. Alerts of new device connecting to network can be always detected by wireless access point and authentication.

xiii. Alerts of output power and expansion of logical boundaries beyond physical boundaries can inform when LBL I exceed its design objectives (see 5.3.2.2).

xiv. Alerts of battery discharge to achieve uncreased distortion or deny impacts.

xv. Transmission delay variations especially for mesh networks.

Table 3: Group 1 Requirements Test Outline

Step #	Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
1	Setup of 3 technology-similar environments, having identical control sets with differing configurations	Blue	Three separate wireless networks with common controls and utilizing a single technology.	3 wireless networks: • 1 large – 40+ assets; • 1 medium – 20-25 assets; • 1 small - < 10 assets)	N/A
2	Attack large wireless network (ITS)	Red	• Baseline adversary time • TTPs/exploits used • Failed attempts • Successful attempts • Network captures	Adversary gains access	N/A
3	Attack medium network (NSRST)	Red	• Baseline adversary time • TTPs/exploits used • Failed attempts • Successful attempts • Network captures • Delta time between attacks of large vs. medium networks	Adversary starts with greater system knowledge due to common elements with large network. Adversary gains access in less time with less failed attempts and more targeted TTP.	N/A

Step #	Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
4	Attack small network (SR)	Red	• Baseline adversary time • TTPs/exploits used • Failed attempts • Successful attempts • Network captures • Delta time between attacks of medium vs. small networks	Adversary starts with greater system knowledge due to common elements with large and medium networks. Adversary gains access in less time with less failed attempts and more targeted TTP.	N/A
5	Set up large wireless network utilizing the same technology basis as the baselines, however with changes to configurable security parameters (e.g., WPA passphrase)	Blue	• Change in passphrase, more challenging • MAC filtering • Other configurable changes	New configuration of large wireless network.	N/A
6	Set up a medium network utilizing completely diverse wireless technology from baseline equivalent.	Blue	• Changes in performance (latency) • Changes in behaviors (handshaking, control, collision avoidance) • Different frequency band • Different protocols	New wireless technology set up for medium network.	N/A

Step #	Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
8	Set up two small networks (A&B) – completely diverse from each other.	Blue	• Differences in performance (latency) • Differences in behaviors (handshaking, control, collision avoidance) • Different frequency band • Different protocols • Electromagnetic compatibility between diverse wireless technologies	No single common boundary or control among 3 networks (medium, 2 small networks) 2nd small network established. Two diverse new wireless technologies set up.	i
9	Evaluate wireless technology design and implementation to determine if requirement 5.5.6.1 is met for A and B small networks.	Blue	• HBOM • SBOM • Cipher Suites • Communication Protocols	Wireless technologies will likely contain common elements. Capture common elements and maximize configuration to reduce reliance on these common elements.	(viii) • (ix.a)-(ix.d)
10	Attack large wireless network (ITS)	Red	• Modified adversary time • TTPs/exploits used • Failed attempts • Successful attempts • Network captures	Adversary has similar performance to small network attack in Step 4. Adversary gains access with negligible deviation from baseline large network	N/A

Step #	Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
			• Delta time between attacks of modified large vs. small networks • Delta time between attacks of modified large and initial large networks.		
11	Attack medium network (NSRST)	Red	• Modified adversary time • TTPs/exploits used • Failed attempts • Successful attempts • Network captures • Delta time between attacks of modified medium vs. modified large network • Delta time between attacks of modified medium and initial medium networks.	Adversary time to successfully attack network is deviated from original medium sized network Adversary gained minimal or no useful knowledge from modified large network regarding subsequent networks during attack Adversary is unable to pivot from large network to medium network.	(i)-(iv)
12	Attack small network A (SR)	Red	• Modified adversary time • TTPs/exploits used • Failed attempts • Successful attempts	Adversary time to successfully attack small network A is deviated from original small network Adversary gained minimal or no useful knowledge from modified large or medium networks regarding subsequent networks during attack	(i)-(vii)

Step #	Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
			• Network captures • Delta time between attacks of modified medium vs. modified large network • Delta time between attacks of small network A and initial small network.	Adversary is unable to pivot from medium network to small network. Adversary time to successfully attack network is deviated from original small sized network, and small network A due to diversity Successful attack on network A does not affect network B, and shared assets continue to operate	
13	Attack small network B (SR)	Red	• Modified adversary time • TTPs/exploits used • Failed attempts • Successful attempts • Network captures • Delta time between attacks of small network A vs. small network B • Delta time between attacks of small network B vs. initial small network.	Adversary time to successfully attack small network B is deviated from original small network and small network A. Adversary gained minimal or no useful knowledge from modified large, medium, small A networks regarding subsequent networks during attack Adversary is unable to pivot from medium network to small network. Adversary time to successfully attack network is deviated from original small sized network, and small network A due to diversity Successful attack on network B does not affect network A, and shared assets continue to operate	(v)-(viii) (x.b) (xi.a,b)

Step #	Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
14	Modify large network with event monitoring, physical tamper indication devices and structures	Blue	• Event alerts • Available output from additional controls such as tamper alarms	Event monitoring provided on large network consistent with requirement 5.3.2.3	
15	Adversary attack modified large network	Red	• Adversary-generated alerts or evidence of alert bypass • Tamper indications • Signal attenuation resulting from physical structures • Baseline of adversary task time • TTPs used	Deviation from previous two attacks on the large networks for time to successfully attack Increased network artifacts generated from attack Greater number of TTPs required	(xii)-(xiv) (xv) – if mesh network utilized. [3]

3.2. Group 2 Requirements: Architecture Focused, Chokepoint Strategy

A chokepoint architecture is a centralized, controlled point for monitoring, filtering, and managing network traffic. By ensuring that all inter-segment communication passes through this chokepoint, organizations can enhance their ability to detect and respond to threats, enforce security policies, and contain potential breaches. This approach is particularly valuable in environments where security is critical. In an advanced reactor facility, a chokepoint architecture might be implemented to control traffic between the reactor control network and the corporate IT network. All communication between these networks would pass through a central firewall and IDS, which would monitor for suspicious activity and enforce strict access controls. The success of the chokepoint is reliant on the chokepoint asset's cybersecurity features. As such, test results may or may not show an inability for lateral movement between networks when the chokepoint is installed but will likely show that the time required for the adversary will increase. This setup would help prevent unauthorized access to the reactor control systems and detect any attempts to compromise the network.

3.2.1. Test Summary

The requirements in this group impose chokepoints between interzonal or inter-system communications and between wired and wireless technologies. Additionally, requirements on the type of control implemented at the chokepoint.

The test will consider a baseline of a single wireless technology with identical security controls but with differing network architecture configurations with and without the implementation of a chokepoint. A red team will be provided with access to the large and medium network architectures with a goal of a goal of minimizing the number of resources, technical knowledge, and new or diverse TTP.

3.2.2. Adversary Characterization

The adversary will have access to the large and medium network technology locations and will be able to deploy multiple disclose and disruption resources within the boundaries of the wireless technology.

Adversary can interact with wireless technologies but begins with zero system knowledge of the targets.

3.2.3. Group 2 Requirements [2]

1. Wireless network is connections to a wired network shall have a technical security control such as an intrusion detection system (IDS), Firewall, or demilitarized zone (DMZ) installed between them.
2. Conduits between zones should be implemented via wired technologies with the aim to increase the potential for detection.
3. SR shall only intercommunicate with NSRST functions via wired, deterministic, fail-secure, unidirectional communication pathway.

3.2.4. Baseline Configuration

The test will set up a baseline as follows:

1. Baseline Setup of two ITS networks – no wired chokepoints – just logical separation (VLAN)
2. Baseline Setup of two ITS networks – wired chokepoint - no technical control measure
3. Baseline Setup Similar setup to Group 1 – three networks – wired chokepoints – no technical control measures
4. Delta Setup of two ITS networks (entirely wireless) with a single wired chokepoint between them. 5.4.3.1 demands a technical control.
5. Delta Setup of two ITS networks (1) entire wireless; (2) hybrid wireless/wired – (2) will have an additional chokepoint within (2) at the wireless/wired connection. A technical control will be implemented at the chokepoint.
6. Delta Setup – 3 networks – Group 1 Baseline – data diode

3.2.5. Group 2 Assurance Evidence [3]

i. All traffic routed out of the zone is sent through the conduit or chokepoint.
ii. Wireless traffic internally routed only and not sent outside the zone.
iii. Distort or Deny attacks from outside of the zone targeting wireless technologies inside the zone (i.e., across the conduit) do not impact on chokepoint and control measures.

Table 4: Group 2 Requirements Test Outline

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
1	Setup of 2 technology-similar environments, having identical control sets with differing configurations	Blue	Two wireless networks on identical physical infrastructure Logical (VLAN) separation only	2 wireless networks: • 1 large – 40+ assets; • 1 medium – 20-25 assets	N/A
2	Attack VLAN networks	Red	• Baseline adversary time • TTPs/exploits used • Failed attempts • Successful attempts • Network captures • Percent of traffic routed between networks via a common access point	Adversary gains access to both networks.	N/A
3	Modify wireless networks to include single wired chokepoint, router restrictions to communicate between different class networks.	Blue	Higher protection accorded to medium network. Wired chokepoint Distinct class networks. Single router between two networks.	2 physically separated networks connected via wired chokepoint	N/A
4	Attack network from large to medium. Red team is limited in attacking medium network wireless communications directly.	Red	• Modified adversary time • TTPs/exploits used	Adversary gains access; requires additional step to compromise/exploit router.	(i), (ii)

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
			• Failed attempts • Successful attempts • Network captures • Percent of traffic routed between networks via a common access point • Delta time between attacks of initial VLAN separated networks vs. modified wired chokepoint network		
5	Attack networks from medium to large. Red team is limited in attacking large network wireless communications directly.	Red	• Modified adversary time • TTPs/exploits used • Failed attempts • Successful attempts • Network captures • Percent of traffic routed between networks via a common access point • Delta time between attacks of initial VLAN separated networks vs. modified wired chokepoint network	Adversary gains access; reduction in time to conduct attack and less failed attempts.	(i), (ii)

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
			• Delta time between attack step 5 vs. step 4.		
6.	Modify wireless networks to include single wired chokepoint, stateful firewall, between different class networks.	Blue	• Firewall Access Control List • Stateful communications/data flow restrictions		N/A
7	Repeat attack steps 4 and 5.	Red	• Same as Steps 4 and 5 • Performance of firewall	Adversary gains access, but time and failed attempts increase for Step 4 attacks (unprotected side to protected side)	N/A
8.	Modify wireless networks to include single wired chokepoint, data diode between different class networks.	Blue	• Modification of data flows to support one-way traffic	No data flow from large network to medium network.	(iii)
9.	Repeat attack steps 4 and 5.		• Same as Steps 4 and 5 • Performance of data diode	No adversary access from large network to medium network. No bidirectional command and control channel established from medium network to large network	N/A

3.3. Group 3 Requirements: LBL I - Fortification Defensive Strategy

LBL I Fortification Defensive Strategy requirements are associated with control measures that provide the capability to control and coordinate other devices to occupy the same frequency spectrum, use redundant radio channels to reduce and avoid RF interference and employ priority-based radio resource allocation to other devices or functions [3].

3.3.1. Test Summary

The test will consider a baseline of a single wireless technology with identical security controls but with differing configurations. This test will conduct Distort and Deny attacks with an aim at impacting the RF signals, medium (air), and encoding/decoding functions of the wireless technologies.

Modified network aim to increase the protections against these Distort and Deny attacks but may be associated with other undesirable effects. Comparative analysis against the baseline will determine the whether the expected benefits are achieved. For example, Distort and Deny attacks are performed in Wi-Fi network architecture, including baseline and one with security remediations in place.

The test includes granting the adversary control of an authorized device primarily for deceive attacks, albeit the impacts may be increased latency or failure of communications generally associated with Distort or Deny attacks.

3.3.2. Adversary Characterization

The adversary will have access to the medium network technology and will be able to deploy multiple disclose and disruption resources within the boundaries of the wireless technology. The adversary will also be given control of a single authorized client on the medium network.

Adversary can interact with wireless technologies but begins with zero system knowledge of the targets.

3.3.3. Group 3 Requirements [2]

1. Wireless technology and/or associated control measures shall provide the capability to:
    - Control and coordinate other devices to occupy the same frequency spectrum.
    - Use redundant radio channels to reduce and avoid RF interference.
    - Use priority-based radio resource allocation to other devices or functions.
    - Adopt multiple access technologies with directional transmission to create multiple and directed spatial streams to reduce RF interference.
    - Configurable Idle Period Management function [6].

3.3.4. Baseline Configuration

The test will set up a baseline as follows:

1. Baseline Setup of a medium to large network - single wireless technology.
2. Baseline Setup - Implement and configure controls as per the NIST [32] checklist for wireless technologies including Spread Spectrum, QoS, collision avoidance and Signal to Noise Ratio
3. Delta Setup to modify baseline network to implement increased protections for spread spectrum, QoS and frequency hopping.

3.3.5. Assurance Evidence [3]

i. Increase signal power for jamming and distortion attacks positively correlated to redundant radio channels, multiple access technologies and coordination.
ii. Coordination and control signals have protections against spoofing or hijacking device providing these signals.
iii. QoS or priority-based resource allocation cannot be directly inferred.
iv. Idle Period Management can limit latency to accept limits.

Table 5: Group 3 Requirements Test Outline

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
1	Set up medium network using single wireless technology.	Blue	• Network captures • Client information • Access Point information	Single wireless technology network with 20 clients and 1 access point	N/A
2	Implement and configure controls as per NIST checklist for wireless technologies • Spread Spectrum • QoS • Signal to Noise Ratio [32]	Blue	• Baseline (over 1 hour) • Latency • Data Rate/Bandwidth • Frequency Allocation • Error Rate • Collisions	Compliant wireless network based on NIST checklist.	N/A
3	Distort Attack targeting physical layer and/or data link layer	Red	• Adversary time to initial success; sustained success • Failed attempts • Successful attempts • TTP, exploits, attack messages (over 1 hour) • Latency • Data Rate/Bandwidth • Frequency Allocation	Successful corruption of bits of targeted messages at LBL I	Baseline (i), (iii),(iv)

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
			• Error Rate • Collisions		
4	Deny Attack targeting physical layer and/or data link layer		• Adversary time to initial success; sustained success • Failed attempts • Successful attempts • TTP, exploits, attack messages (over 1 hour) • Latency • Data Rate/Bandwidth • Frequency Allocation • Error Rate • Collisions	Lower time to success as knowledge of distort attack simplifies effort Complete jamming of all communications	Baseline (i),(iii),(iv)
5	Implement requirements from Group 3 to modify network.	Blue	Modified measurements • Baseline (over 1 hour) • Latency • Data Rate/Bandwidth • Frequency Allocation • Error Rate • Collisions	Modified wireless network with differing characteristics and behaviors	

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
6	Repeat Distort Attack on Modified Network	Red	Modified & Attack measurements • Adversary time to initial success; sustained success • Failed attempts • Successful attempts • TTP, exploits, attack messages (over 1 hour) • Latency • Data Rate/Bandwidth • Frequency Allocation • Error Rate • Collisions	Adversary task time increases Adversary success rate decreases Error correction requirement reduces or eliminates impact Redundant channels provide enhanced protection	(i),(iii),(iv)
7	Repeat Deny Attack on Modified Network	Red	Modified & Attack measurements • Adversary time to initial success; sustained success • Failed attempts • Successful attempts • TTP, exploits, attack messages (over 1 hour)	Adversary task time increases Adversary success rate decreases Protection against sustained jamming attacks	

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
			• Latency • Data Rate/Bandwidth • Frequency Allocation • Error Rate • Collisions		
8	Conduct Deceive Attack on Modified Network with: • No persistence (new malicious client) • Hijacked device	Red	Same as step 6 above • Attempts at spoofing or hijack of device • Retransmissions • Coordination and control messages	Adversary is successful with spoofed device Protection against spoofing or hijack devices	(ii)

3.4. Group 4 Requirements: LBL I - Access Control Defensive Strategy

LBL I wireless technology access control defensive strategy requirements are designed to ensure wireless communications are confined within the logical boundary of their assigned zone, utilizing technologies that minimize signal propagation beyond the necessary area. Requirements for additional controls for SR and NSRST functions include requirements for further signal restriction and/or establishing methods to limit signal transmission [3].

3.4.1. Test Summary

The test will consider a single system and network leveraging a single wireless technology. The specific focus is LBL I Access Control which aims at reducing the access to wireless communications by tuning of physical characteristics (e.g., signal propagation) and external physical boundaries. The test will evaluate whether the coupling of wireless communications within LBL I can meet the FY24 Report [3] - Group 4. Additionally, specific external measures and structures will be evaluated to determine their benefit in meeting these requirements. Tests will aim to validate or invalidate the objective criteria in FY24 Report [3] Group 4 and capture the associated evidence necessary for this evaluation.

3.4.2. Adversary Characterization

The adversary will have access to the medium network technology logical boundaries and will be able to deploy multiple disclose and disruption resources within the logical boundaries but outside the physical boundaries of the wireless technology. The adversary will also be given control of a single authorized client on the medium network.

Adversary can interact with wireless technologies but begins with zero system knowledge of the targets.

Disclose resources, such as high gain antennas will be limited to those commercially available of the shelf; mobile (transportable on foot) and concealable in a back-pack or bag.

3.4.3. Group 4 Requirements [2]

1. Wireless communications shall be confined within the logical boundaries of their assigned zone. Physical assets providing the wireless communications shall be located within the physical boundaries of their assigned zone.
2. SR functions shall employ wireless technologies that result in minimize signal propagation beyond that necessary for the wireless communications. The signal power of the wireless technology should be highly configurable and confinable to a physical volume without external measures.
3. SR communications shall not be routable outside local network.
4. NSRST functions shall employ wireless technologies that are closely coupled to the physical boundary of the zone and shall not propagate beyond the site boundary. This may require external measures such as a Faraday cage, structures like cement barriers to limit propagation, or directional antennas.
5. ITS functions may employ wireless technologies that should minimize propagation beyond the site boundary. Category C functions that have a direct interaction or interdependency with SR or NSRST functions shall only employ wireless technologies within the site boundary.

3.4.4. Baseline Configuration

Group is a single system.

The test will set up a baseline as follows:

1. Baseline Setup of a medium network to enable default signal propagation – 802.11
2. Delta Setup of a medium network to enable the lowest signal propagation / RF permissible physical boundary.
3. Delta Setup of a medium network to enable lowest signal propagation / RF absorbing/interference physical boundary.

3.4.5. Group 4 Assurance Evidence [3]

i. Signal propagation attenuation or distance from source.
ii. Wireless technology ability to tune signal strength.
iii. Adversary capability with high-gain antennas (i.e., attenuation limit; what size of antennae is credible?)
iv. Effect of use of Faraday cages or other measures - destructive measures to limit signal propagation or accelerate signal attenuation.
v. Noise/interference generation

Table 6: Group 4 Requirements Test Outline

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
1	Set up medium network – single wireless technology.	Blue	• Network captures • Client information • Access Point information	Single wireless technology network with 20 clients and 1 access point	N/A
2	Implement and configure controls as per NIST checklist for wireless technologies	Blue	• Baseline (over distance) • Signal Attenuation from source • Faraday Cage effects and other measures	No physical boundaries Typical Interior/Office Building Hardened/reinforced cement structures (Vital Area) Faraday Cage	(i),(iv)
3	Conduct Disclose Attack with: • Low Gain • Medium Gain • High Gain Antennae	Red	• Adversary success time • Frequency, channels, wireless technology • Reception distance • Signal power	Disclosure of frequency and identification of wireless technology is dependent on antennae gain. Low gain – infrequent interception Medium gain – frequent interception High gain – complete interception	(iii)

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
4	Conduct Distort Attacks based upon Disclose attack results for wireless network placed within the following structures: • No physical boundaries • Typical Interior/Office Building • Hardened/reinforced cement structures (Vital Area) • Faraday Cage If no results from Disclose attacks, Distort attack will be randomized	Red	• Baseline for each type of physical boundary (at equal distance) • Adversary noise injection • Corrupted/distort communications • Noise interference generation characteristics • Equipment, Power, Gain antennae	Continual successful corruption of single or few bits at LBL I for networks with no physical boundaries and typical interior / office building. Intermittent success at corrupting single or few bits for hardened/reinforced cement structures (Vital Area) No success at corrupting bits for Faraday Cage	Comparison between Baseline values and attack values (iii)
5	Repeat step 4 for Deny attacks.	Red	• Baseline for each type of physical boundary (at equal distance) • Adversary noise injection • Corrupted/distort communications.	Continual successful denial LBL I for networks with no physical boundaries and typical interior / office building	Comparison between Baseline values and attack values

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
			• Noise interference generation characteristics • Equipment, Power, Gain antennae	Intermittent success at denial for hardened/reinforced cement structures (Vital Area) No success at denial for (iv) Faraday Cage. Denial of physical medium (Air) from adjacent area to physical boundary	Limits of adversary to inject noise and distort communications Noise interference generation characteristics Equipment, Power, Gain antennae
6	Change Wireless technology and tune Signal Propagation configuration to meet Group 4 requirements for structures hardened / reinforced cement structures and Faraday Cage	Blue	• Tuning settings (Signal to noise ration) to meet coupling requirements • Signal propagation limits • Signal attenuation effects of Faraday cage. • Degree of logical boundary coupling to physical boundary based on low, medium and high gain antennae.	Modified network	
7	Repeat Step 3 for modified network (Disclose Attack) for hardened / reinforced cement structure and Faraday Cage.	Red	Baseline (over distance) same as Step 3	Reduction in information gained from attack for cement structures No information gained for faraday cage.	Comparison between attack values and those from 1st Disclose attack.

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
8	Repeat Step 4 for modified network (Distort Attack) for hardened / reinforced cement structure and Faraday Cage.	Red	Modified & Attack measurements same as Step 4	Randomized attacks are less successful. Protecting against information disclosure reduces effect of distort attacks.	Comparison between attack values and those from 1st Distort attack.
9	Repeat Step 5 for modified network (Deny Attack) for hardened / reinforced cement structure and Faraday Cage.	Red	Modified & Attack measurements same as Step 4	Successful jamming attacks cannot be sustained. Protecting against information disclosure reduces effect of attacks.	Comparison between attack values and those from 1st Deny attack.

3.5. Group 5 Requirements: LBL II / LBL III – Fortification Defensive Strategy

LBL II/III wireless Fortification Defensive Strategy requirements stipulate that cryptographic modules used in the protection of information must be appropriately secure for their use case. Cryptographic keys, or secrets used to derive ephemeral keys, critical to securing communications must be stored in protected areas and use tamper-resistant devices. All hardware, software, and data components within the cryptographic boundary must be protected. Additionally, wireless technologies must employ secure functions to protect integrity where Authenticated Encryption and Associated Data (AEAD) cipher suites cannot be utilized. Wireless technologies must also minimize error propagation resulting from distort or deny attacks that result in the corruption of ciphertext. Wireless technologies for SR and NSRST functions must encrypt both header (i.e., control, routing information) and data for all layers protected by LBL III, as well as employ cipher suites that provide error-correcting codes. [6]

3.5.1. Test Summary

The test will consider a single system and network leveraging a single wireless technology. The specific focus is LBL II/III Fortification which aims at fortifying the wireless technologies and protecting the function (e.g, Application) without adverse impact. The test will conduct baseline tests on a system implemented per its design and other specifications, such as NIST checklists and (ii) confirm operational characteristics of Safety Function with an implemented crypto system at the LBL II/III boundary [32]. Attacks will be conducted against this baseline system and their impacts recorded. The system will then be modified based upon the FY24 Report [3] Group 5 requirements and the baseline tests and attacks repeated. Tests will aim to validate or invalidate the objective criteria in FY24 Report [3] Group 5 and capture the associated evidence necessary for this evaluation. The tests will also evaluate whether implementing the requirements leads to increased effects from certain attacks.

3.5.2. Adversary Characterization

The adversary will have access to the medium network technology logical boundaries and will be able to deploy multiple disclose and disruption resources within the logical boundaries but outside the physical boundaries of the wireless technology. The adversary will also be given control of a single authorized client on the medium network.

Adversary can interact with wireless technologies with or without knowledge of a master key or session key(s).

3.5.3. Group 5 Requirements [2]

1. Cryptographic modules used in the protection of information shall be appropriately secure for their use case.
2. Cryptographic keys (or secrets used to derive ephemeral keys) critical to securing communications shall be stored in protected areas and use tamper-resistant devices. All

[6] Within this document the order of Group 5 LB II/III Fortification Defensive Strategy and Group 6 LB II / LBIII – Access Control Defensive Strategy are switched from the FY24 Requirements Document [4] for organizational purposes.

hardware, software, and data components within the cryptographic boundary shall be protected (adapted from the Requirements Report [2]).

3. Wireless technologies for SR and NSRST functions shall encrypt both header (i.e., control, routing information) and data for all layers protected by LBL III (adapted from the Requirements Report [2]).
4. Wireless technologies shall employ secure functions to protect integrity, where Authenticated Encryption and Associated Data (AEAD) cipher suites cannot be utilized.
5. Wireless technologies shall minimize error propagation resulting from distort or deny attacks resulting in corruption of cipher text.
6. SR and NSRST functions should employ cipher suites that provide error correcting codes.
7. Symmetric Encryption shall leverage sessional or ephemeral private keys that provide for perfect forward secrecy.
8. KDF should ensure perfect forward secrecy (PFS).

3.5.4. Baseline Configuration

Group is a single system with a target of Cryptosystem Fortification

The test will set up a baseline as follows:

1. Baseline Setup of a medium-size 802.11g network with one WAP and multiple clients
2. Baseline Setup - Implement and configure controls as per the NIST checklist for wireless technologies (WPA3, 802.1X/EAP, PKI, etc.) [32]
3. Delta Setup to implement group requirements for Fortification of the Cryptosystem, including Radius, TLS, Ephemeral Keys, Key Derivation Function (KDF), Authenticated Encryption with Associated Data (AEAD, Full Packet Encryption

3.5.5. Group 5 Assurance Evidence [3]

i. Communications protected by LBL III will not expose data associated with the network devices, architecture, and client devices.
ii. Reduction in error propagation requires continual use of disruption resources by adversary to achieve deny impacts by injection of single or multiple bit faults into the wireless cipher text packets.
iii. Change in a disclosed session key providing PFS with reauthentication eliminates adversary access to LBL III.
iv. AEAD integrity protections ensure that corrupted data is not used by the Application layer within LBL III.
v. AEAD cipher suites do not increase latency to an unacceptable level based on system technical specifications.

Table 7: Group 5 Requirements Test Outline

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
1	Set up medium network – single wireless technology.	Blue	• Network captures • Client information • Access Point information	Single wireless technology network with 20 clients and 1 access point	
2	Implement and configure cryptosystem as per NIST checklist for wireless technologies [32]	Blue	• Baseline Timing • Cryptosystem Characteristics • Cryptographic key • Latency	Network using Pre-shared symmetric key No perfect forward secrecy No error correction codes	
3	Disclose Attack Attempt to intercept traffic from other clients Assume knowledge of pre-shared key (PSK)	Red	• Baseline disclose values • Handshaking messages • Data • Routing/header information	Disclosure of all encrypted communications	
4	Change pre-shared key (PSK)	Blue	• Baseline Timing Characteristics (2nd pre-shared key)	Change of PSK	
5	Disclose Attack: Passive attempt to intercept traffic from other clients. No knowledge of pre-shared key (PSK); No exploit use to	Red	• Disclosed data including headers and cipher text • Exhaustive key search timing	Disclosure of header Brute Force of pre-shared key	

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
	compromise clients or access points to leak PSK.				
6	Distort Attack targeting • Cipher Text • Headers	Red	• Error propagation values • Function impacts • TTP • Distort device; power	Corruption of bits of cipher text (LBL II)	
7	Deny Attack based targeting • Cipher Text	Red	• Error propagation values • Function impacts • TTP • Deny device information (e.g., power)	Corruption of entire packets	
8	Deceive Attack no-authentication (may be bypassed) targeting • Plain Text • Headers	Red	• Error propagation values • Function impacts • TTP • Exploits (e.g., power) • Handshaking messages	Successful deception of Application Data (Plain Text, LBL III)	
9	Modify network to implement • AEAD cipher suite (LBL II/III • IPSEC full packet encryption • Cipher modes that reduce error propagation	Blue	• Modified Network Timing characteristics • New sessional key shared/established • Session key duration	Modified network Encrypted header information 6.4.1.2 – OSI Layer 2 encryption	Delta between baseline and modified timing. (v)

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
	• Sessional/Ephemeral Keys • Perfect Forward Secrecy				
10	Repeat Step 5 (Disclose Attack) on Modified Network No knowledge of Master Key	Red	Disclosed data including cipher text Exhaustive key search timing	Only Cipher Text gained from attack Exhaustive key search time to completion takes longer than session key in use. PFS mitigates value of session key for future disclose attacks.	(i)
11	Repeat Step 10 (Disclose Attack) on Modified Network with knowledge of: (i) Sessional Key (ii) Master Key	Red Team	• Disclosed data including cipher text • Exhaustive key search timing • Timing of other attacks to disclose future session key from master or previous session key.	Only Cipher Text gained from attack (Master Key) Only plain text from single session (Session Key) PFS eliminates value of knowledge of Master Key Session Key Changes prior to adversary gaining key 6.4.1.5 - PFS 6.4.1.6 – Sessional Keys	(i) (iii)
12	Repeat Step 6 (Distort Attack) on Modified Network	Red	• Error propagation values • header • data • Increased transmission (repeat messages)	Distortion of single and multiple bits (3-4) in intermittent cipher text header Error propagation and mode of cryptosysem increases	(ii) (v)

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
				potential of deny impact from distort attack.	
13	Repeat Step 7 (Deny Attack) on Modified Network	Red	• Deny timing • repeat transmissions • successful packets • Attack throughput • corrupted packets/minute • Application data communications • corrupted data not utilized	Denial of cipher text (LBL II) Optimized deny attacks leveraging error propagation and integrity protections of AEAD cipher suite.	(iv)
14	Deceive impacts to modify plain text by either: (i) establishing a secure channel without authentication. (ii) Hijacking an already established secure channel	Red	• Successful deception attacks TTP and exploits • Timing • Impact • Change in session key • Persistence of authentication • Timing	Multiple attacks to inject or modify information to be acted upon by Application	(iii) (iv) (v)

3.6. Group 6 Requirements: LBL II / LBL III – Access Control Defensive Strategy

LBL II/III requirements for wireless Access Control Defensive Strategy include establishing successful authentication of wireless client devices with the access point or controller using AEAD cipher suites. Additionally for wireless technologies for SR and NSRST functions asymmetric cryptography and mutual authentication must be employed before symmetric session keys are established [3].[7]

3.6.1. Test Summary

The test will consider a single system and network leveraging a single wireless technology. The specific focus is LBL II/III Access Control which aims to enforce authentication prior to access to function significant communications (e.g., Application) without adverse impact. The test will conduct baseline tests on a system implemented per its design and other specifications, such as NIST checklists and (ii) confirm operational characteristics of Safety Function with an implemented and enforced authentication at the LBL II/III boundary [32]. Attacks will be conducted against this baseline system and their impacts recorded. The system will then be modified based upon the FY24 Report [3] Group 6 requirements and the baseline tests and attacks repeated. Tests will aim to validate or invalidate the objective criteria in FY24 Report [3] Group 6 and capture the associated evidence necessary for this evaluation.

3.6.2. Adversary Characterization

The adversary will have access to the medium network technology logical boundaries and will be able to deploy multiple disclose and disruption resources within the logical boundaries but outside the physical boundaries of the wireless technology. The adversary will also be given control of a single authorized client on the medium network.

Adversary can interact with wireless technologies with or without knowledge of a master key or session key(s)for authentication.

3.6.3. Group 6 Requirements [2]

1. 5.5.2.1 Establishing wireless communications shall require successful authentication of client devices with the access point or controller.
2. 5.5.1.1 Wireless technologies should implement AEAD cipher suites.
3. 5.5.1.4 Wireless technologies for SR and NSRST functions shall employ asymmetric cryptography and mutual authentication before symmetric session keys are established (Amended from the Requirements Report [2]).

[7] Within this document the order of Group 5 LB II/III Fortification Defensive Strategy and Group 6 LB II / LBIII – Access Control Defensive Strategy are switched from the FY24 Requirements Document [4] for organizational purposes.

3.6.4. Baseline Configuration

Group is a single system with a target of Access Control Authentication

The test will setup a baseline as follows:

1. Baseline Setup of a medium-size 802.11 network
2. Baseline Setup - Implement and configure controls as per the NIST checklist [32] for wireless technologies (WPA3, 802.1X/EAP, PKI, etc.)
3. Delta Setup to implement group requirements for Access Control of the Cryptosystem, including Radius, TLS, Ephemeral Keys, Key Derivation Function (KDF), Authenticated Encryption with Associated Data (AEAD, Asymmetric and Mutual Authentication

3.6.5. Group 6 Assurance Evidence

i. No data communications established until client and server have mutually authenticated.
ii. All traffic from authenticated devices must pass through the cryptosystem to access LBL III.
iii. AEAD cipher suites can be configured to always demand mutual authentication.

Table 8: Group 6 Requirements Test Outline

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
1	Set up medium network – single wireless technology. Secure Element to store Master Key	Blue	• Network captures • Client information • Access Point information	Single wireless technology network with 20 clients and 1 access point	
2	Implement and configure cryptosystem as per NIST checklist for wireless technologies Pre-shared symmetric key No perfect forward secrecy No error correction codes [32]	Blue	• Baseline Timing • Cryptosystem Characteristics • Cryptographic key • Latency • SE-MCU bus captures	Secure element may introduce latency from Group 5 tests	
3	Distort Attack targeting Headers Authentication	Red	• Baseline error propagation values • Function impacts • Error propagation values	Corruption of bits of cipher text (LBL II)	
4	Deny Attack based targeting Headers Authentication	Red	• Baseline denial values • Handshaking messages • Data • Routing/header information	Corruption of entire packets (LBL II), Authentication process/handshaking (LBL II)	

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
5	Deceive Attack targeting Headers Authentication	Red	• Baseline deceive values • Handshaking messages • Data • Routing/header information	Successful deception of Application Data (Plain Text, LBL III) Successful authentication of malicious client Avoidance or Bypass of authentication	
6	Modify network to implement Enforce Mutual Entity Authentication via Asymmetric prior to session key establishment AEAD cipher suite (LBL II/III) Sessional/Ephemeral Keys & Perfect Forward Secrecy	Blue	Modified Network Timing characteristics • Authentication • New sessional key shared/established • Session key duration	Modified network	Delta between baseline and modified timing. (i), (iii)
7	Repeat Disclose Attack on Modified Network targeting authentication messages and information No knowledge of Master Key	Red	Disclosed data including cipher text • Exhaustive key search timing • Number of disclosed authentication messages	No disclosed header information 6.4.1.2 – OSI Layer 2 encryption	(ii)
8	Repeat Disclose Attack on Modified Network targeting authentication messages and information knowledge of Master Key knowledge of a single Sessional (symmetric) Key	Red	Disclosed data including cipher text • Exhaustive key search timing • Timing of other attacks to disclose key	Header and cipher text information (Master Key) Only plain text from single session (Session Key)	(i)

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
9	Repeat Distort Attack on Modified Network based on knowledge of Master Key knowledge of a single Sessional Key	Red	• Error propagation values • header • data • Increased transmission (repeat messages)	Distortion of single and multiple bits (3-4) in intermittent authentication messages header	(i), (ii)
10	Repeat Deny Attack on Modified Network	Red Team	• Deny timing • repeat transmissions • successful packets • Attack throughput • corrupted packets/minute • Application data communications • corrupted data not utilized	Denial of cipher text (LBL II) Optimized deny attacks Authentication is denied	(i), (ii)
11	Deceive impacts to authenticate or bypass authentication with session key no session key	Red Team	• Authentication likelihood with or without session key • Authentication impacts during session key change	Multiple attacks to exploit vulnerabilities to authenticate or bypass authentication Authentication cannot be bypassed Authenticated clients cannot be impersonated	(i), (ii), (iii)

Step #	Test Step Description	Red or Blue Team	Key Observations & Measurements	Expected Results	Assurance Evidence
12	Deceive impacts to modify plain text with successful authentication	Red Team	• Successful deception attacks • Timing • Impact • Change in session key • Persistence of authentication • Timing	Multiple attacks to inject or modify information to be acted upon by Application	(i), (ii), (iii)

4. CONCLUSION

This report builds upon the foundations laid by two previous reports: (i) *Wireless Application Selection Methodology – DOE-NE deliverable M2CT-23SN1104023, SAND2023-10185* [2] report ("Requirements Report") and (ii) *Assurance Evidence for Wireless Technologies performing Safety Related and Important to Safety Functions, SAND2024-06797*R [3] ("FY24 Report").These earlier works, referred to as the "Requirements Report" and the "FY24 Report," respectively, provided the basis for the identification and classification of wireless security requirements for use in AR facilities.

This report presented a high-level test framework to assess and evaluate the identified wireless security requirements from the FY24 Report [3]. As part of this effort, several testing site facilities were evaluated for their suitability to evaluate wireless network security requirements specifically for use in AR sites which is presented.

Section 2 of the report contains a ranked survey of Test Platforms. The ranking is based on the test platform's suitability for assessing the wireless security requirements from the FY24 Report [3]. Multiple testing platforms were evaluated to determine their capability in assessing wireless security requirements for advanced reactor (AR) communications. The evaluation considered several criteria, including the ability to utilize AR or nuclear power plant (NPP) control simulators, the fidelity level of the test system (emulator, simulator, Hardware-in-the-Loop (HitL), or hybrid), and the capacity to test wireless environments, primarily 802.11. Additionally, the feasibility and level of effort required by the providing organization to have the testbed ready by Q3 FY25, or Q3 FY26 for red and blue-teaming activities, were also reviewed. This survey aimed to identify the most suitable platforms for validating the safety, security, and reliability of wireless technologies in AR deployments. Additional information on the assessed test platforms was provided in Appendix A, "Test Platform Surveys".

Section 3, "Testing Objectives," further elaborated on testing requirements groups 1 through 6 and their associated testing scenarios. For each requirement group test summaries', adversary characterizations, requirements descriptions, bassline configurations, assurance evidence and test outlines were provided. These test outlines detailed will form the basis for the future development of test cases to holistically evaluate one or more requirements groups. Assurance evidence will be gathered either directly or through a comparative analysis between networks that have implemented a modified group of requirements and similar networks that follow current practices as a baseline.

The aim of this and future efforts would be to propose and test a risk-informed, performance-based framework for designing, implementing, validating, operating, and maintaining wireless technologies for Nuclear Safety or safety-related functions in Advanced Reactors.

REFERENCES

[1] Nuclear Regulatory Commission, "DRAFT REGULATORY GUIDE DG-5075 - Establishing Cybersecurity Programs for Commercial Nuclear Power Plants licensed under 10 CFR Part 53," NRC, Washington, DC, 2023.

[2] M. T. Rowland, A. Haddad, B. Karch and R. Valme, "Wireless Application Selection Methodology (SAND2023-10185)," Sandia National Laboratories, Albuquerque, 2023.

[3] M. T. Rowland, R. S. Valme, B. Karch, A. Hahn, L. Maccarone and J. deCastro, "Assurance Evidence for Wireless Technologies performing Safety Related and Important to Safety Functions (SAND2024-06797R)," Sandia National Laboratory, 2024.

[4] International Atomic Energy Agency, "Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev 1)," IAEA, Vienna, 2021.

[5] International Atomic Energy Agency, "Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T," IAEA, Vienna, 2018.

[6] International Electrotechnical Commission, "Nuclear power plants - Instrumentation and control systems important to safety - Selection and use of wireless devices 62988:2018," IEC, Geneva, 2018.

[7] International Electrotechnical Commission, "Nuclear power plants - Instrumentation, control and electrical power systems - Cybersecurity requirements, IEC 62645:2019," IEC, Geneva, 2019.

[8] International Electrotechnical Commission, "Nuclear power plants - Instrumentation, control, and electrical power systems - Security Controls 63096:2020," IEC, Geneva, 2020.

[9] International Electrotechnical Commission, "Security For Industrial Automation And Control Systems - Part 3-2: Security Risk Assessment For System Design 62443-3-2:2020," IEC, Geneva, 2020.

[10] Nuclear Energy Institute, "Cyber Security Plan for Nuclear Power Reactors, NEI 08-09 Rev 6," NEI, Washington, DC, 2010.

[11] Nuclear Energy Institute, "Subject: Wireless Cyber Security Guidance," [Online]. Available: https://www.nrc.gov/docs/ML2306/ML23060A327.pdf. [Accessed 17 July 2024].

[12] CSA Group, "Cyber security for nuclear power plants and small reactor facilities, N290.7:2021," CSA, Toronto, 2021.

[13] Paragon Energy Solutions LLC, "Wireless Cybersecurity for NPP Report," 2023.

[14] International Organization for Standardization, "Information technology — Security techniques — Security requirements for cryptographic modules, ISO/IEC 19790:2006," ISO/IEC, Geneva, 2006.

[15] National Institute of Standards and Technology, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," NIST, Gaithersburg, 2007.

[16] National Institute of Standards and Technology, "Guide to IPsec VPNs, NIST SP800-77 rev 1," NIST, Gaithersburg, 2020.

[17] National Institute of Standards and Technology, "Guide to a Secure Enterprise Network Landscape, NIST SP 800-215," NIST, Gaithersburg, 2022.

[18] National Institute of Standards and Technology,, "Security Requirements for Cryptographic Modules FIPS 140-3,," NIST, Gaithersburg, 2019.

[19] European Telecommunications Standards Institute, "5G; Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS) (3GPP TS 33.535 version 16.2.0 Release 16)," ETSI, Valbonne, 2021.

[20] European Telecommunications Standards Institute, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception (3GPP TS 36.101 version 14.5.0 Release 14)," ETSI, Valbonne, 2017.

[21] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3, Request For Comment 8446," Internet Engineering Task Force, 2018.

[22] C. Y. T. H. S. a. K. R. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 4120," IETF, 2005.

[23] K. M. Martin, Everday Cryptography: Fundamental Principles & Applications, 2nd Edition, Oxford: Oxford Univeristy Press, 2017.

[24] A. Drissi, The Security of Cryptosystems Based on Error-Correcting Codes, InTechOpen, 2021.

[25] J. (. Minella, Wireless Security Architecture: Designing and Maintaining Secure Wireless for Enterprise, Hoboken: Wiley, 2022.

[26] Nuclear Regulatory Commission, "Cyber Security Programmes for Nuclear Power Reactors, Regulatory Guide 5.71, Revision 1," NRC, Rockville, 2023.

[27] International Organization for Standardization/International Electrotechnical Commission, "SO/IEC 27002:2022 - Information security, cybersecurity and privacy protection: Information security controls," ISO/IEC, Geneva, 2022.

[28] International Organization for Standardization, "Information security, cybersecurity and privacy protection, Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO/IEC 27000:2018," ISO/IEC, Geneva, 2018.

[29] Institute of Electrical and Electronics Engineers, "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006), pp. 1-314, 2011.," IEEE, Piscataway, NJ, 2011.

[30] Institute of Electrical and Electronics Engineers, "Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: IE," IEEE, Piscataway, NJ, 2011.

[31] C. Lamb, J. deCastro, A. Haddad, A. Kim, E. Lee and K. A. Manjuna, "TLR-RES-DE-2022-007 Study of Wireless Technology Implementation in Isolated, High Consequence Networks," Nuclear Regulatory Commision, ONRR, Washington, DC, 2022.

[32] M. P. Souppaya and K. A. Scarfone, "SP 800-153. Guidelines for Securing Wireless Local Area Networks (WLANs)," NIST, Washington DC, 2012.

APPENDIX A. PLATFORM SURVEY SUMMARIES

Multiple testing platforms were initially evaluated for their suitability to support testing of wireless security requirements for advanced reactor communications. A summary of platform capabilities is described in Sections B.1 through B.6. including a description type of platform (emulation, simulation, physical HitL testbed, hybrid), the focus on the platform (communications, reactor simulations, etc.), and existing and future platform capabilities. This section provides a sampling of possible testing platforms, giving a reference for future testing system evaluation and the selection of applicable test systems based upon the development of a formalized test plan.

A.1. PAWR Platforms

The Platforms for Advanced Wireless Research (PAWR) initiative, funded by the National Science Foundation (NSF) and a consortium of industry partners was designed to assist in the development and deployment of next-generation wireless technologies through large-scale, city-scale testbeds.

A.1.1. POWDER

PAWR POWDER provides a wireless testbed located in Salt Lake City, Utah, designed to support advanced research and development. POWDER offers a diverse range of environments including urban areas and university campuses, enabling researchers to test wireless devices in various real-world scenarios, supporting both outdoor and indoor experiments. Focused primarily on 4G and 5G, Powder features software-defined radios (SDRs) that allow for flexible and programmable radio configurations, however with limited availability of 802.11 technologies.

The POWDER testbed provides instrumentation for real-time data collection and monitoring, facilitating detailed analysis of wireless device performance with analytics tools to research network behavior and optimize device performance for 4G and 5G devices. Although POWDER staff offered to integrate 802.11 wireless devices into the testing facility, Powder does not have natively at this time support 802.11 testing.

POWDER dos does not have any advanced reactor or NPP Simulation capability. However, the POWDER platform is mature and currently available for use in testing per its focus and limitations.

A.1.2. Colosseum

PAWR Colosseum is a wireless network emulator designed to support research and development in wireless communication technologies (4G, 5G, and 802.11) allowing for the testing of wireless devices and protocols under realistic and controlled conditions. Colosseum supports the simulation of up to 256 fully programmable wireless nodes providing high-fidelity emulation of wireless channel propagation effects (multipath, fading, and interference).

Although Colosseum does not have native ICS data within its emulation system, Colosseum does have the ability to use customer-provided test data as payload input for wireless communications testing. Similarly, Colosseum does not natively have any advanced reactor or NPP Simulation capability. Additionally, the Colosseum platform is mature and currently available for testing in FY 25/FY 26 per its focus and limitations.

A.2. Sandia National Laboratory (SNL) Platforms

A.2.1. Emulytics™ / SCEPTRE

Sandia National Laboratory's Emulytics™ experiment platform was designed to support cyber emulation, mathematical modeling, and data analysis methodologies to produce quantitative knowledge about critical systems. Used in conjunction with the SCEPTRE software tool, allows for emulated testing and modeling of both digital and physical components of cyber-physical systems (CPS) and ICSs. Additional software components of Emulytics™ provide for emulation and modeling of 802.11 wireless network components, which could be incorporated into ICS-emulated systems for cyber-related testing. Emulytics™ and SCEPTRE are mature testing platforms with advanced emulation and testing capabilities and would be available for testing scenarios within their focus areas in FY25. However, there is not currently any associated advanced reactor or NPP simulation capability available to use directly with these platforms and further research would need to be done to determine how to integrate these types of systems into Emulytics™ and SCEPTRE.

A.2.2. Sensor Test and Evaluation Center (STEC)

"The Sensor Test & Evaluation Center (STEC) is a 72-acre facility dedicated to the design, development, and real-world testing of current, new, and emerging sensor technologies.

- Electro-field
- Microwave
- Ported coax
- Fence disturbance
- Taut wire
- Object detection
- Radar"

STEC can be connected to emulated and HitL environments to evaluate functional impacts resulting from attacks targeting specific wireless technologies and associated devices and systems.

A.2.3. Experimental Test Environment (ETE)

Sandia Nation Laboratory's (SNL) Experimental Test Environment (ETE) is designed to augment the existing SNL Emulytics™ and SCEPTRE emulation systems through the addition of integrated physical HitL devices (sensors, controllers, PLCs, etc.) to enhance realism, supporting increased fidelity of testing and validation of security measures. The ETE laboratory is currently in development and could have the ability to integrate the testing of 802.11 wireless devices into the HitL testbed in FY25 or FY26. ETE does not currently support advanced reactor or NPP Simulation capability natively and research would need to be done to determine the work effort to incorporate this element into this testbed.

A.3. UIUC – Purdue

The University of Illinois at Urbana-Champaign (UIUC) – Purdue University reactor test bed is a collaborative initiative designed to advance research and development in nuclear reactor technologies, offering a platform for testing, validating, and optimizing various aspects of nuclear

reactors, including safety, and performance. The UIUC–Purdue testbed features advanced reactor simulators that simulate reactor behavior under various conditions, allowing researchers to study reactor dynamics and advanced control systems and architectures, enabling the simulation and evaluation of reactor control strategies. Their testbed supports network emulation capabilities, allowing the simulation of communication networks within a nuclear power plant, in a hybrid testing environment that integrates both simulation and physical hardware components.

The UIUC – Purdue testbed also has wireless communication capabilities to simulate and emulate this environment, enabling the study of wireless technologies in nuclear reactor settings. Physical mock-ups of wireless communication systems are available for hands-on testing, and the test bed leverages PAWR (Platforms for Advanced Wireless Research) platforms to provide diverse and realistic wireless network environments. The testbed is designed to support research activities planned for FY25, including the testing of advanced reactor simulators with physics engines, safety systems, and network configurations. It also includes setups for defensive architecture, allowing researchers to evaluate and enhance the security and resilience of reactor control systems and communication networks. However, based upon a finalized formalized test plan, possible modifications to the UIUC - Purdue testbed could be required.

A.4. Georgia Institute of Technology

The Georgia Institute of Technology (Georgia Tech) reactor test bed (digital twin) is a platform designed to integrate physical and digital components to create a comprehensive and realistic environment for testing, simulation, and validation of various aspects of nuclear reactors. The digital twin concept involves creating a highly accurate virtual replica of the physical reactor system and its control environment. The hybrid testing environment integrates both simulation and physical hardware components, allowing for test environments where real hardware can interact with simulated reactor systems. Additionally, the platform enables the testing of wireless communications capabilities and associated cybersecurity measures, ensuring that the reactor's communication networks are resilient against potential cyber threats. There are possible integration opportunities for testing with PAWR wireless testing platforms. The Georgia Tech testbed is currently available and would be able to support 802.11 requirements testing in FY25 and FY26. Based upon a finalized formalized test plan, possible modifications to the Georgia Tech testbed could be required.

A.5. The Ohio State University (OSU)

The Ohio State University (OSU) has a reactor test bed used to support research and development in nuclear reactor technologies that integrates both physical and digital components to evaluate reactor dynamics and control system architectures. Additionally, the OSU reactor testbed has the ability to enable physical mock-ups of wireless communication systems (802.11) to research the use of wireless communication in nuclear reactors with the ability to support red-team cybersecurity testing. The OSU testbed is based on small modular and advanced reactor designs and incorporates a third- generation HitL simulation system (GSN3). GSN3 enables high-speed data acquisition capabilities to capture detailed information about reactor performance and response. GSN3 is based on open-source code and virtual machine architecture. The OSU Tech testbed is currently available and would be able to support 802.11 requirements testing in FY25 and FY26. Based upon a finalized formalized test plan, possible modifications to the OSU testbed could be required.

A.6. NuScale Power

NuScale Power is an American company that specializes in the development of small modular reactors (SMRs) for nuclear power generation. NuScale Power has a reactor testbed platform designed to support the development, testing, and validation of their reactor systems and for operator training purposes. The NuScale testbed includes simulation tools, physical mock-ups, and real-time data analysis of the simulate reactor dynamics and control systems. Currently, the testbed does not natively support wireless emulation or the ability to incorporate testing of wireless systems within their testbeds. Based upon a finalized formalized test plan, possible modifications to the NuScale Power testbed could be implemented to support testing of wireless requirements in FY25 / FY26.

A.7. Comanche NPP

The Comanche Peak testing would allow for measurements and evidence to be collected in real-world NPP conditions, particularly important for Architectural requirements associated with signal propagation and single boundary/LBL I requirements. Comanche Peak testing would involve red teaming of controls listed in NEI 22-07 and also provide insights into interactions and dependencies between process (safety) and corporate (non-safety) networks. On-site testing would require significant coordination and validation of testing scope and involved systems with stakeholders and likely be limited to passive wireless security measurements. Active testing would likely occur on a mocked-up system that complies with Comanche Peak design and implementation specifications. The Comanche Peak NPP test would provide higher fidelity than either simulation or HitL testbeds and is currently available pending testing approval.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Ben Cipiti	8845	bbcipit@sandia.gov
Michael Rowland	8851	mtrowla@sandia.gov
Benjamin Karch	8851	brkarch@sandia.gov
Sheryl Drake	8815	sidrake@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Katya Le Blanc	katya.leblanc@inl.gov	INL
Daniel Warner	daniel.warner@nuclear.energy.gov	DOE-NE

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.