ADVANCED REACTOR SAFEGUARDS & SECURITY

Advanced Reactor Wireless Communications

Safety Related/Important to Safety Functions

PRESENTED BY

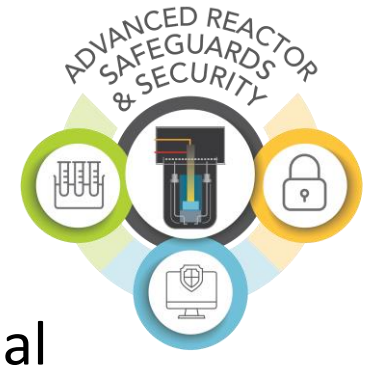
Michael T. Rowland

15-May-2024

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

SAND2024-03609C

Research Objectives (FY23+)



- Identify generic set of requirements from existing international and national standards, regulatory guides, and industry best practices related to architecture, communications, data flows, and controls (e.g., cryptographic mechanisms)
- Adapt these requirements for use of wireless technologies that perform or support any SSEP function at a Nuclear Power Plant (FY23 Report & updates).
- Innovate new approaches that meet the NRC's expectations for an acceptable defensive strategy for architectures that include wireless technologies (FY24 & FY25)
- Provide a systematic and robust approach to design, implementation and assurance of defensive architectures, control measures, and systems that use existing or to be developed future wireless technologies (FY24++)
- Align the above processes between existing fleet and proposed advanced reactor cybersecurity draft regulatory guide (DG-5075) (FY24 & FY25)

NEI 22-07 (FY22)

Figure 2 - Technical Analysis of Wireless Cybersecurity[8]

- System Focused
- Additional 3 Controls needed for equivalent protection
  - Radio Resource Management
  - RF Monitoring
  - RF-restricted Zones

- 4D Impacts
  - Distort
  - Deny
  - Disclose
  - Deceive

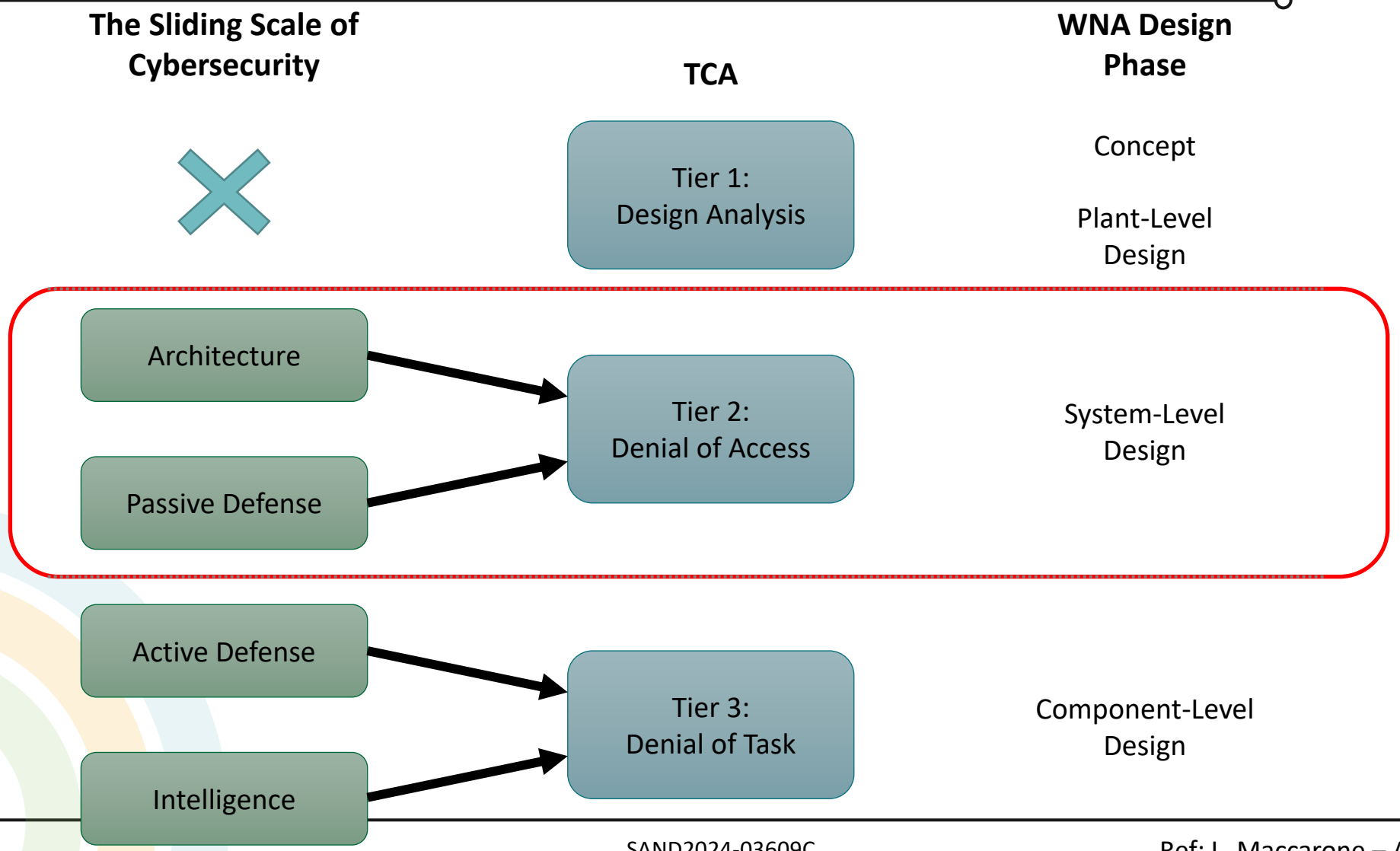
FY23 Requirements Specification Process

1. Review of International and National Standards
2. Identify and adapt requirements for wireless technologies
3. Add justification (e.g., reference to standard) and rationale
4. Add supplemental guidance and cyber-attack space considerations
   - Important for FY24 efforts

- **Important Findings**
  - Canada – allows for Category B & C (e.g., Some Direct CDAs & All Indirect CDAs)
  - IEC (Europe) – allows for Category C (e.g., Some Indirect CDAs)

FY24 Efforts

Tiered Cyber Analysis (TCA) – NRC DG-5075



Ref: L. Maccarone – ANS NPIC HMIT 2023

NRC RG 5.71 Defensive Strategies Elements

Acceptable defensive strategies must comprise of two elements

1. [DENIAL OF ACCESS] a defensive architecture that describes a physical and logical network design that implements successive security levels separated by boundary control devices with segmentation within each security level.
2. [DENIAL OF TASK] a defensive strategy that employs multiple, diverse, and mutually supporting tools, technologies, and processes to effectively perform timely detection of, protection against, and response to a cyberattack.

- Element 1 [DENIAL OF ACCESS] will be the key focus of FY24 activities

Ref: RG 5.71 Revision 1 Section C.3.2

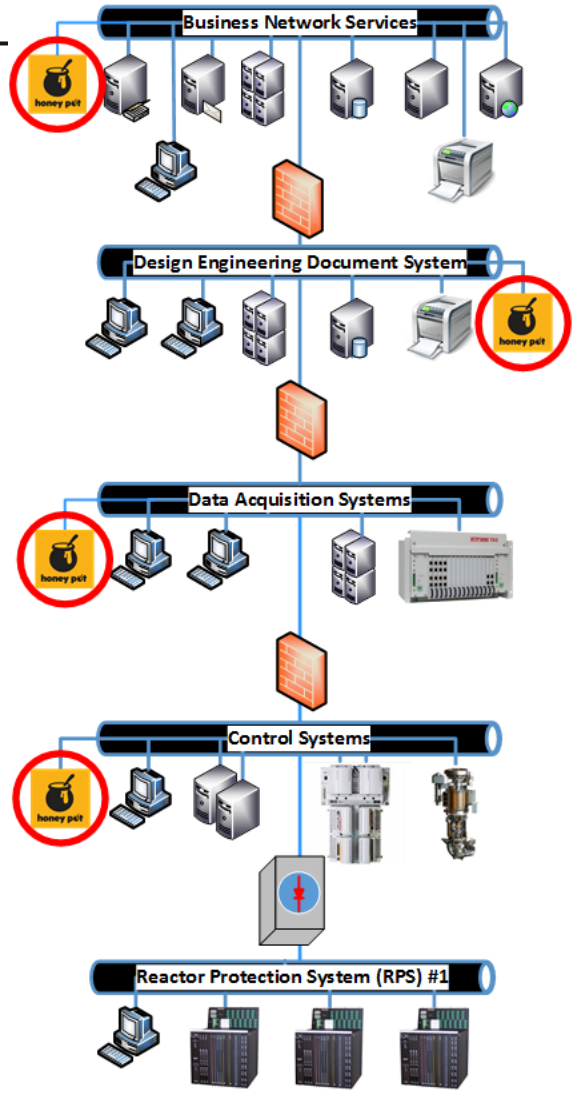
Examples of Defensive Strategies

Consider one or more defensive strategies

1. Fortification
2. Chokepoint
3. Area or Access Control
4. Deception

Desired Outcome:

- Defense in Depth
- Resilient DCSA that prevents adversary access to attack pathways and protects against adversary actions on target.



Level 5
Business Related Systems

Level 4
Technical Data Management Systems

Level 3
Data Acquisition Systems

Level 2
Operational Control Systems

Level 1
Systems Important to Safety and Security

Ref: IAEA ITC M-51 DCSA (Guy Landine/PNNL)

Identifying Evidence (Milestone 1)

FY24 focus

- Key challenge
  - Current NRC defensive strategies assume prohibition of wireless for Direct (SR) and Indirect CDAs (ITS)
  - Data Diode between Level 4 and Level 2 (or 3) provides a deterministic fortification at a single chokepoint.
  - Wireless communications in Level 4 may allow the adversary to bypass the data diode.

- Defensive Strategy Element 1 [Denial of Access] – DG-5075 Tier 2 analysis
  - Architecture and Passive Defense Requirements to develop objective criteria and identify evidence
  - Identify Gaps - where Denial of Access cannot be guaranteed; requiring Denial of Task (Active Defense)
  - Cross-reference Gaps with FY23 Requirements for Denial of Task (Active Defense)

FY24 Expected Outcomes (Milestone 2)

- Evaluate Platforms for Advanced Wireless Research testbeds (www.advancedwireless.org)
  - Evidence capture capabilities
  - Available/implemented disruption/disclosure resources
  - Representative systems/environment availability
  - Cyber-attack – 4D impact capabilities (emulated/simulated/actual)
- Test outline for architecture requirements
  - Select a test platform and provide a framework to capture evidence to validate (or invalidate) objective criteria
  - Inform update to or evaluation of Active Defense Requirements

Questions and Feedback

Michael T. Rowland
Cybersecurity Researcher
Sandia National Laboratories
mtrowla@sandia.gov
+1.505.220.0199

SAND2024-03609C