Sandia National Laboratories

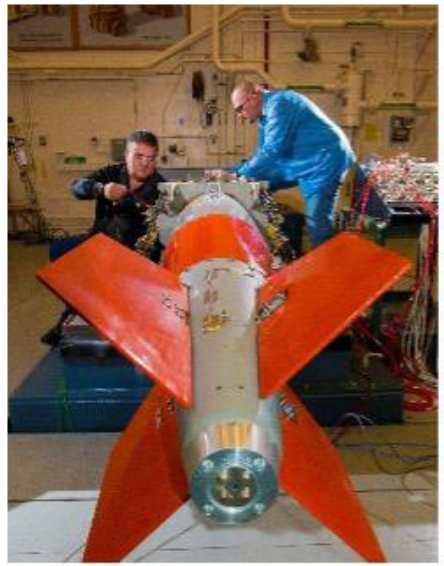
Exceptional service in the national interest

Advanced Reactor Wireless Communications

Mike Rowland

ARSS PROGRAM REVIEW

November 1, 2023



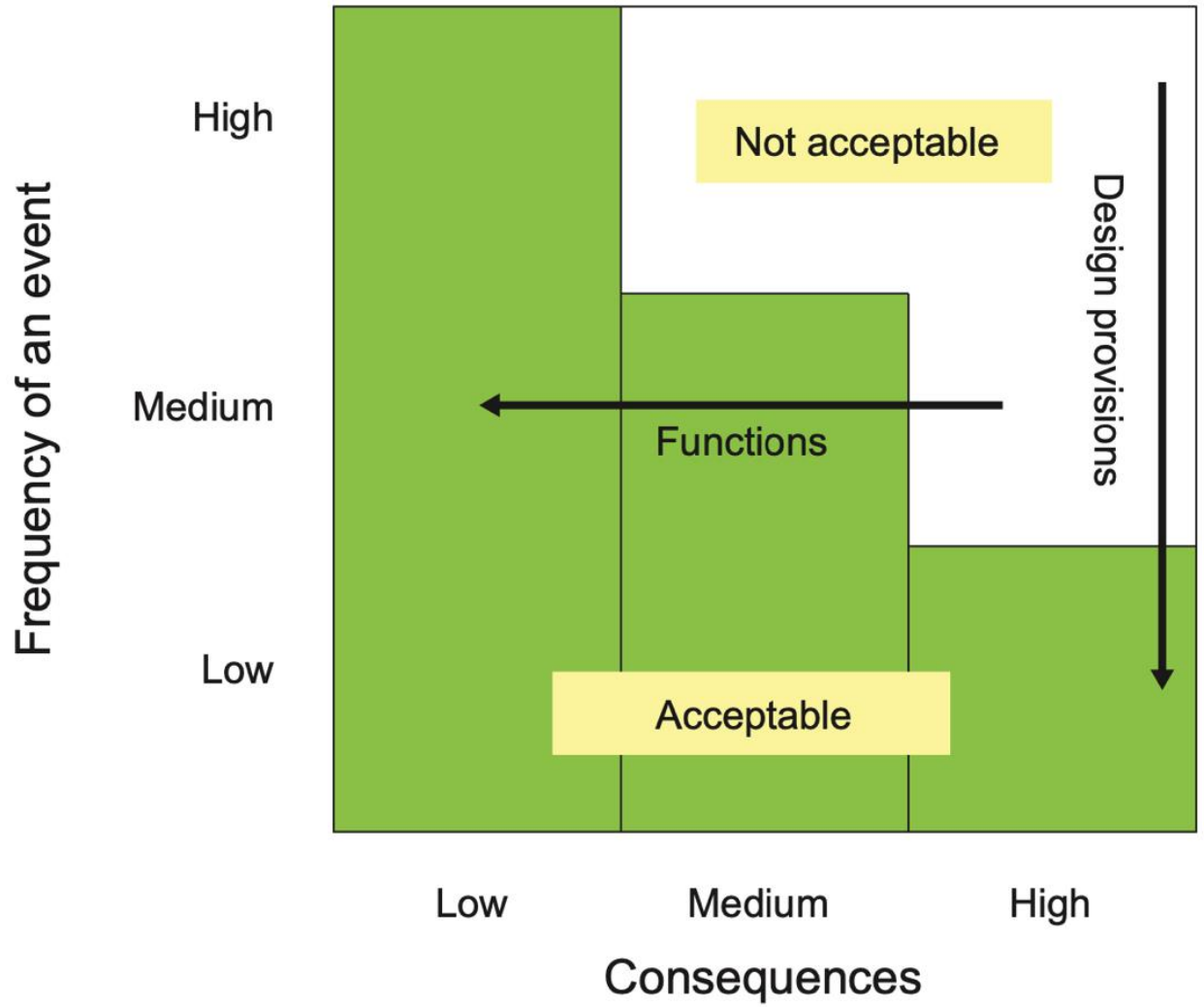
U.S. DEPARTMENT OF ENERGY NNSA

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. **SAND2024-15028PE**

Motivation

- Economic
  - Legacy networking technologies introduce high costs for wiring, shielding, maintenance, etc.
- Performance
  - Scalability
  - Multi-domain remote monitoring and control
- Key enabler for green energy production goals

Frequency vs Consequences Basic Principles



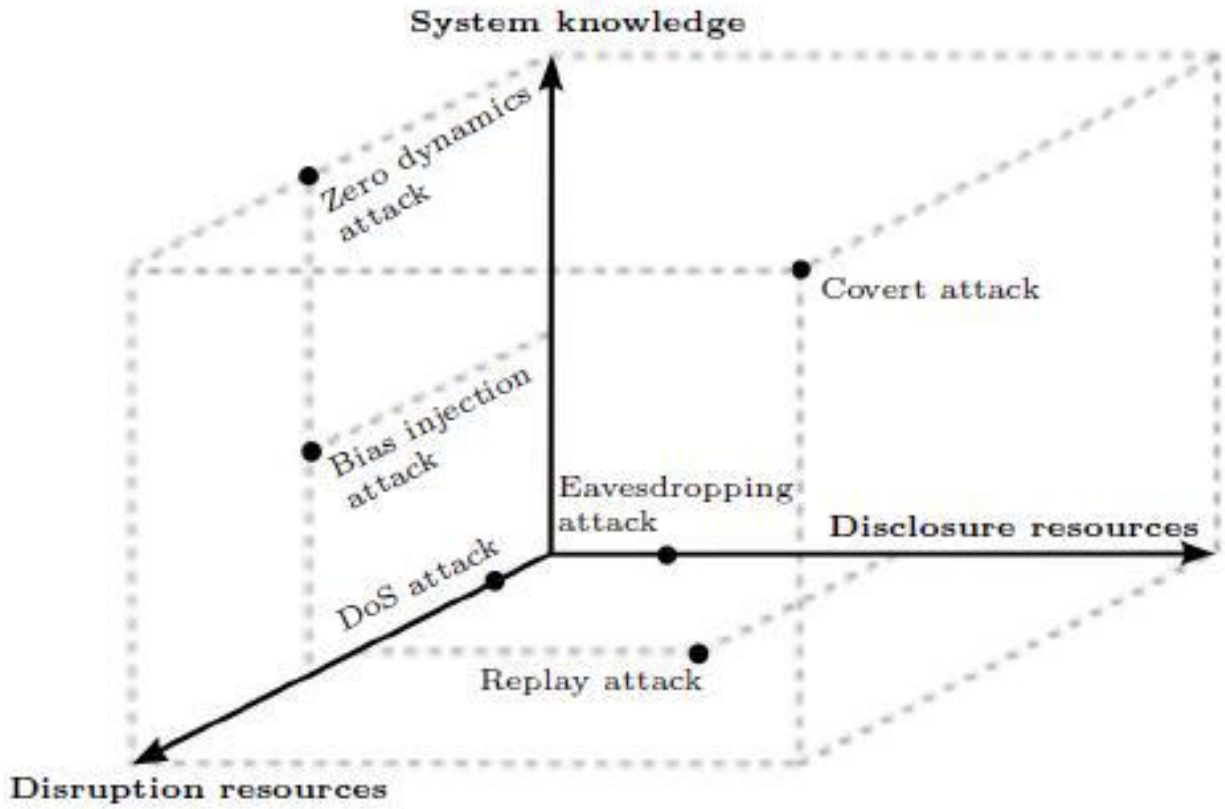
(IAEA SSG 30)

Selected Safety Classifications

Organization/ Country	Safety Classification of I&C Functions in NPP			
IAEA SSG-30	Safety Category 1	Safety Category 2	Safety Category 3	Items not important to safety
IEC 61226	Category A	Category B	Category C	Non-categorized
Canada	Category 1	Category 2	Category 3	Category 4
USA	System Important to Safety			not specified
	Safety Related	not Safety Related		

Threat Model and Adversary Characterization

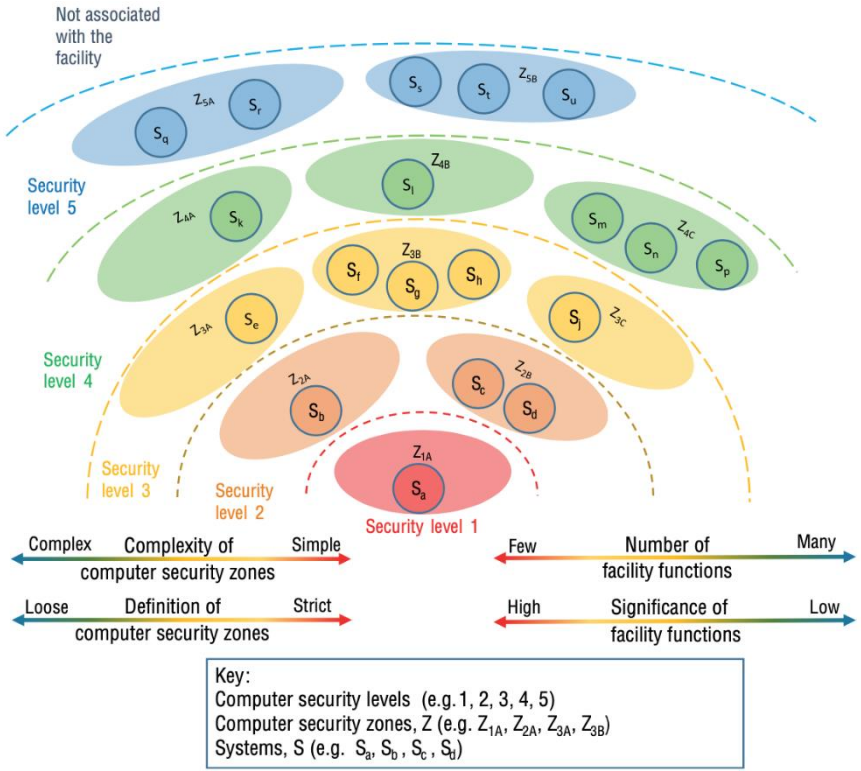
- 4D Approach
  - Deny
  - Distort
  - Disclose
  - Deceive
- Cyber-Physical Attack Space
  - System Knowledge
  - Disclosure Resources
  - Disruption Resources
- Proposed requirements based on limiting attacker access to 4D impacts and access to resources in Cyber-Physical Attack Space



(Teixeira, et al, 2015)

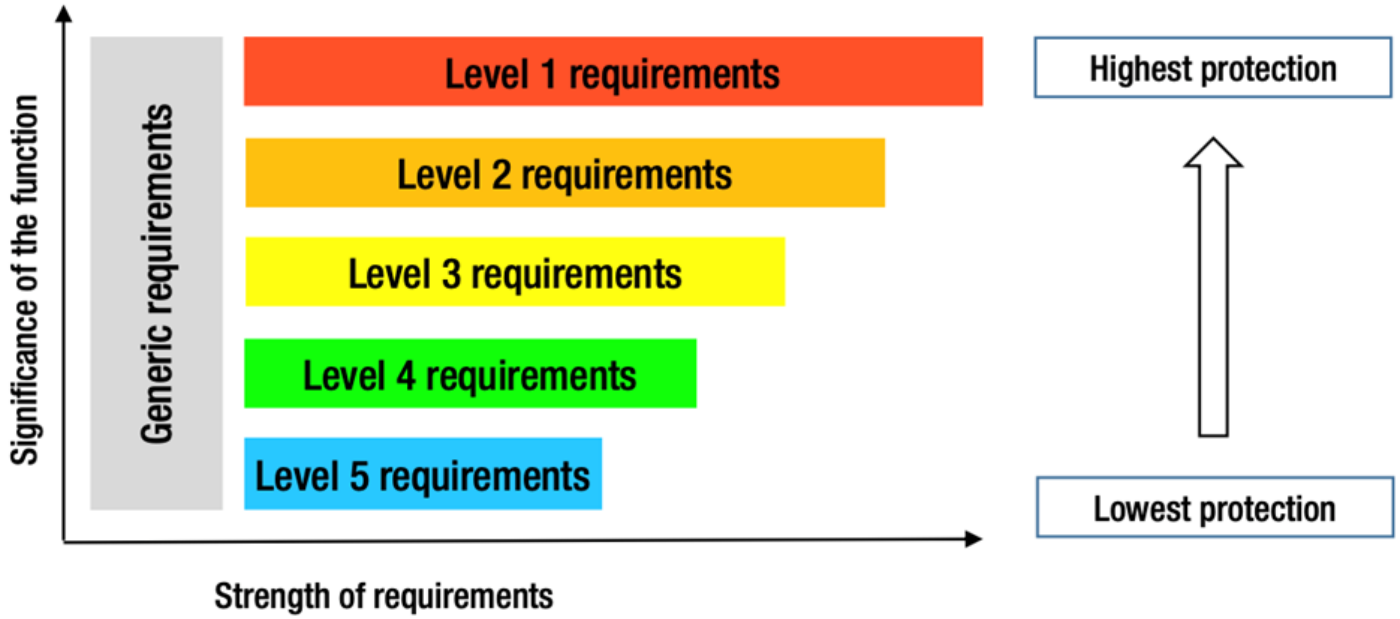
Requirements Structure

- Risk informed performance-based approach
  - Prior to considering wireless technologies a risk assessment must be performed
- Consequence Prioritized Design
  - The categorization of functions into acceptable and unacceptable classes is critical
- Defense Computer Security Architecture
  - Devices must be organized according to specific constraints
  - Specific "D" impacts must be addressed for wireless
- Implementing security zones and levels
  - Traditionally physical boundaries must transition to be logical and wireless



Impact

- Provides an approach to identify and evaluate risks associated with wireless technologies based upon the category of function
- Preliminary set of requirements based on safety classification and use case
- Path forward to demonstration and refinement of the methodology



(IAEA NSS 17-T)

FY24 and Future Work

- Review test beds for wireless
  - Various test beds from universities and organizations are under analysis: POWDER, COLOSEUM, CyberSIM, Minimega
  - Systems evaluated according to various metrics: virtualization, networking, usability
- Test subset of requirements
  - Simulations of typical wireless networks will be created
  - Agents will be added to these systems to perform blue vs. red teaming scenarios
- Need to validate requirements
  - These scenarios will allow us to assess wireless security
  - Also enables the team to validate or fine tune necessary requirements for a wireless system

Relation to Other ARSS Project Work

- SLDA / SeBD
  - Enabling methodologies
  - Utilize to lower risk of wireless use, determine security and reliability requirements per unique application within plants
- ARCADE
  - Enabling technology
  - Provides platform to analyze effects of cyber attacks unique to or made possible by introduction of wireless
- Secure Element
  - Enabling technology
  - Allows for integration of requirements related to cryptography and key storage / maintenance

Discussion