Sandia National Laboratories

Exceptional service in the national interest

CYBERSECURITY REGULATIONS, DESIGN AND LICENSING

Presenter: Michael T. Rowland

Minami Tanaka, Sheryl Drake, Titus Gray, Lee Maccarone

February 2026

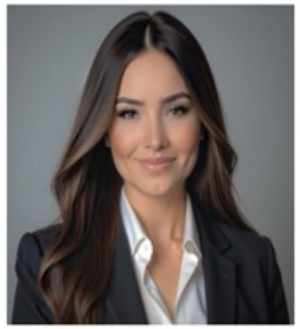
U.S. DEPARTMENT of ENERGY | NNSA National Nuclear Security Administration

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.

SAND2026-17603PE

SANDIA TEAM

Michael T. Rowland, Principal Member of Technical Staff, Sandia National Laboratories
- Controls System Engineer at OPG – Pickering NGS with a focus on cybersecurity since 2008
- Led IAEA Cybersecurity Efforts 2013-2019
- Lead author of US NRC draft RG 5.96 – Cybersecurity Programs for non-LWR
- DOE-NE PI on Wireless Technologies for Nuclear Power Plants
- IEC Task Leader of IEC TR 63468:2024 – Cybersecurity Risk Management



Minami A. Tanaka, Senior Member of Technical Staff, Sandia National Laboratories
- DHS-CISA led industrial control sensor deployments with a focus on cybersecurity since 2021
- DOE-NE led GOTS and COTS wireless cybersecurity testing
- DOE-NE led the development of system specific cybersecurity testing process

Sheryl Drake, Principal Member of Technical Staff, Sandia National Laboratories
- CISSP, CCSP, CRISC, CGEIT, PMP
- Network Engineer with a focus on cybersecurity since 2010
- Experience in securing network architectures, integrating security principles, and implementing protective measures

HISTORY OF NUCLEAR CYBERSECURITY PRACTICE

September 2001
9/11 terrorist attack

2002
US military finds US NPP documents in Afghanistan

November 2005
NEI 04-04 Rev. 1 Cybersecurity Program for Power Reactors is published by NEI

January 2010
Reg. Guide 5.71 is issued by USNRC

2011
IAEA issues NSS 17: first international publication on cybersecurity at nuclear facilities

2015
IEC-IAEA practical arrangement on cybersecurity

2022
IAEA issues NSS 17-T: Focus on functions, architecture, and risk management

March 2024
Draft RG 5.96 Cybersecurity Programs for NPPs Licensed Under 10 CFR Part 53 published by USNRC

Asset-Focused Cybersecurity

Function-Focused Cybersecurity

March 2002
NEI Cybersecurity Task Force is formed

February 2002
USNRC issues EA-02-026 Interim Safeguards & Security Compensatory Measures for NPPs

March 2009
10 CFR 73.54 Protection of Digital Computer and Communication Systems and Networks is issued

April 2010
NEI 08-09 Rev. 6 Cybersecurity Plan for Power Reactors is published

2014
IEC 62645:2014 – first international standard on NPP cybersecurity

2019
IEC 62645:2019 – updated based on draft IAEA NSS-17T

2021
CSA N290.7:21, function-focused prioritizing architecture, and adds detection & response

Cybersecurity by Design

Asset-focused timeline modified from: G. Landine. "US NRC – Case Study". IAEA Presentation.

EXISTING FLEET AND FUTURE RIPB APPROACHES

Existing Fleet

- Prescriptive, controls-based, check-list approach
- Heavy reliance on physical isolation(i.e., air gap)
- Limited use of cryptography

Future Risk-Informed Performance-Based (RIPB) Approach

- Consequence-prioritized
- Cybersecurity by Design
- Functional Approach
- Conceptual Defensive Model simplifies reliance on logical boundaries over physical isolation
    - Enables Wireless, Remote Operations

CURRENT LICENSING REQUIREMENTS

Main Licensing Regulations

CFR 10 CFR Part 50

- Two-step licensing process
- Key Elements:
  - General Design Criteria (Appendix A)
  - Quality Assurance Criteria (Appendix B)
  - Cybersecurity Program License

CFR 10 CFR Part 52

- Combined licensing process
- Key Elements:
  - Principal Design Criteria
  - Quality Assurance Program
  - Cybersecurity Plan

Cybersecurity Requirements

CFR 10 CFR 73.54

- Protect SSEP
- Requirements for Digital Technology Protection
- Related Guides:
  - NRC RG 5.71 Rev 1
  - NEI 08-09 Rev 7

- Limitations on Current Approach:
  - Limited Innovation and Flexibility
  - Need for RIPB Approaches

NON-LWR CURRENT AND FUTURE LICENSE AND REGULATIONS

Non LWR Regulations

Design Review Guide (DRG) for I&C in Non-Light Water Reactors (non-LWR)

- Guidance for NRC Staff to Review I&C Reactor Portions
- Insights on Interactions Between Safety Design Review and Cybersecurity
- Cyber-Attribute Examples:
  - Fail-Safe vs. Fail-Secure
  - Adoption of Encryption for Data Security and Integrity
  - Increased Determinism and Robustness through Cryptographic Measures

RG 1.232 (Developing Principal Design Criteria (PDC) for non-LWR)

- Provide example Advanced Reactor Design Criteria
- Guidance for developing PDC for non-LWRs applications for:
  - Construction Permit
  - Design Certification
  - Combined License
  - Standard design approval, or
  - Manufacturing License

RG 1.233 (NEI 18-04 Rev 1)

- Licensing Basis and Application Content
- Classification and Special Treatment of SSCs
- Assessment of Defense in Depth

Future Regulations

CFR 10 CFR Part 53

- Risk-Informed, Technology Inclusive Regulatory Framework
- Objectives:
  - Addresses Non-LWR technologies
  - Recognizes Technological Advances
  - Credit Advanced Reactor Responses to Accidents
- Major Provisions Impacting Cybersecurity:
  - Licensing and Regulating NPP
  - Performance-Based Approach to Cybersecurity
  - Guidance in NEI 18-04 Rev 1

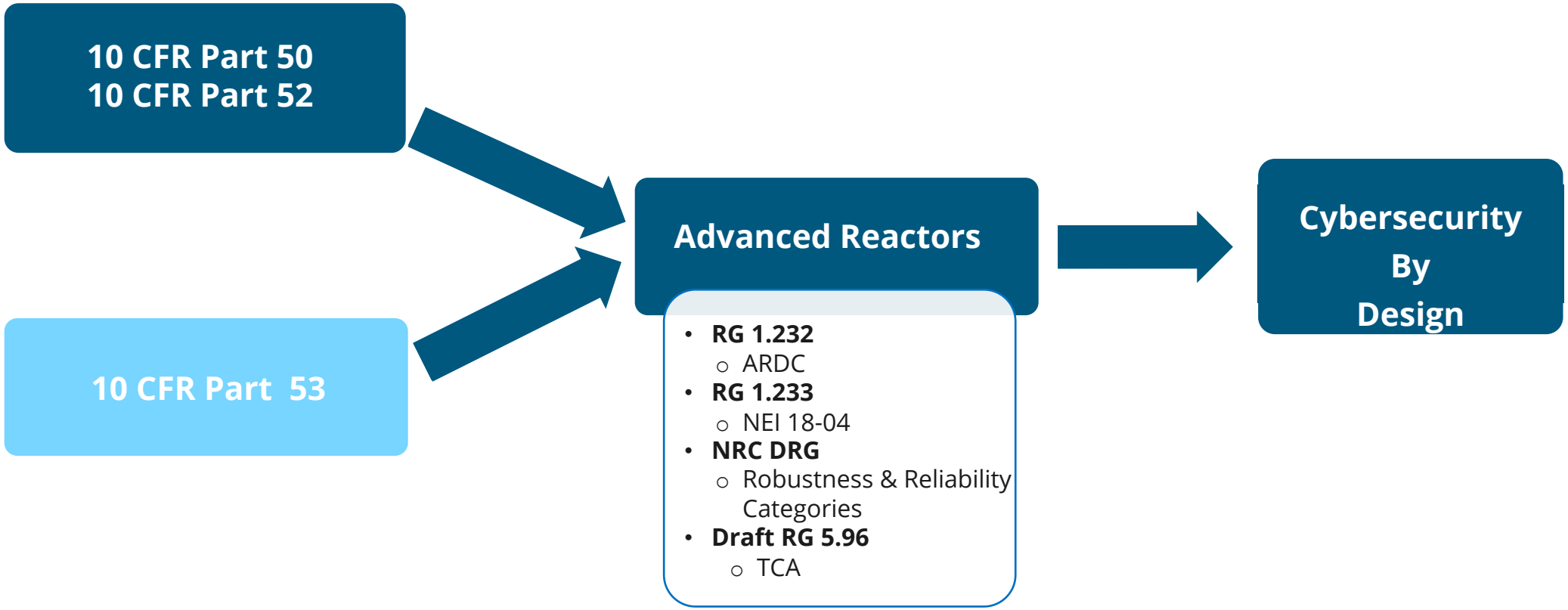
CFR 10 CFR 73.110

- demonstrate protection against cyberattacks commensurate with the potential consequences from those attacks
- does not prescribe specific methods that must be used to demonstrate protection.

Draft RG 5.96

- tiered cyber analysis (TCA)
- cybersecurity by design
- follows SMR Design Maturity

INTEGRATING EXISTING APPROACHES WITH FUTURE REGULATION

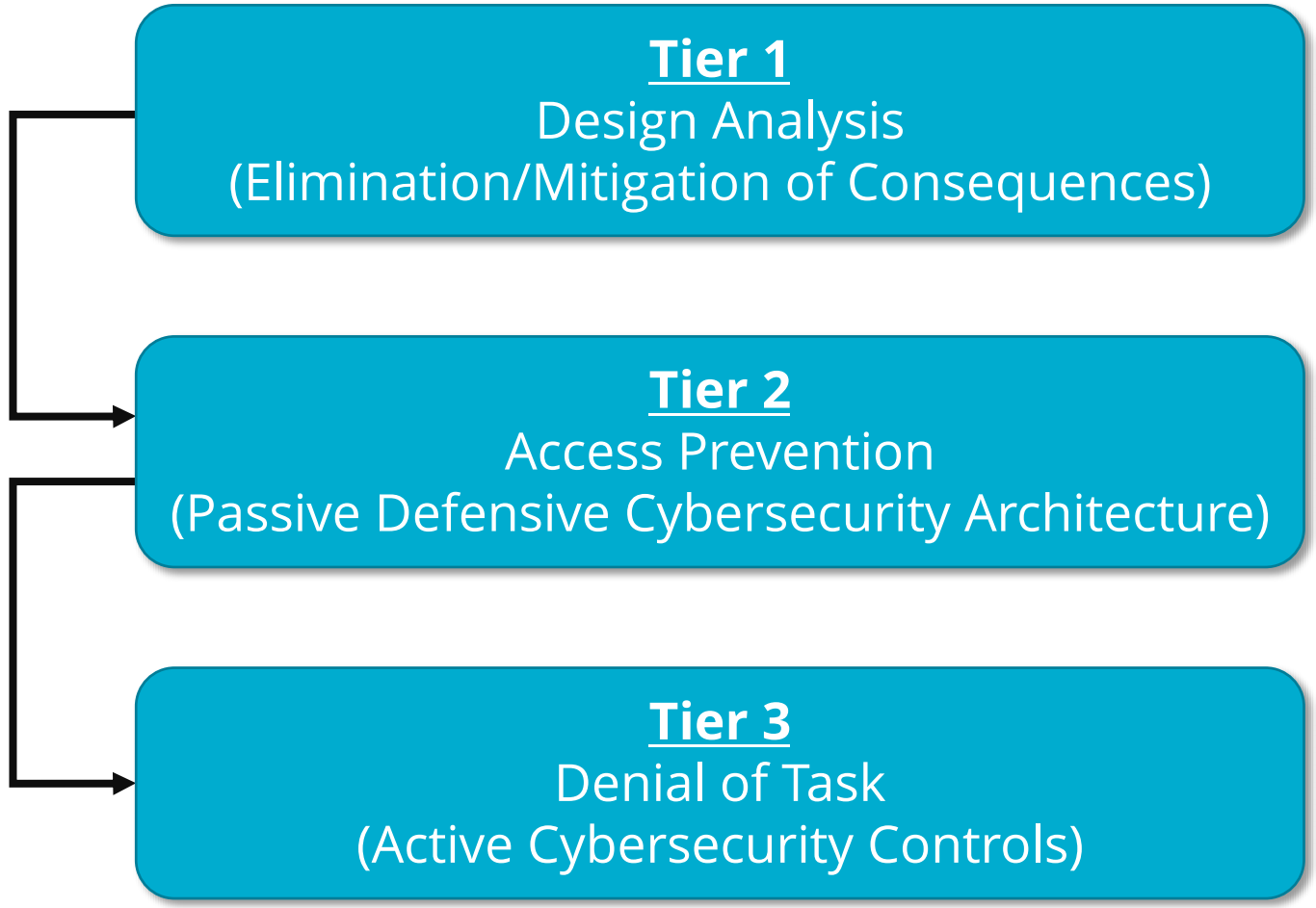


CYBERSECURITY REGULATION RG 5.96

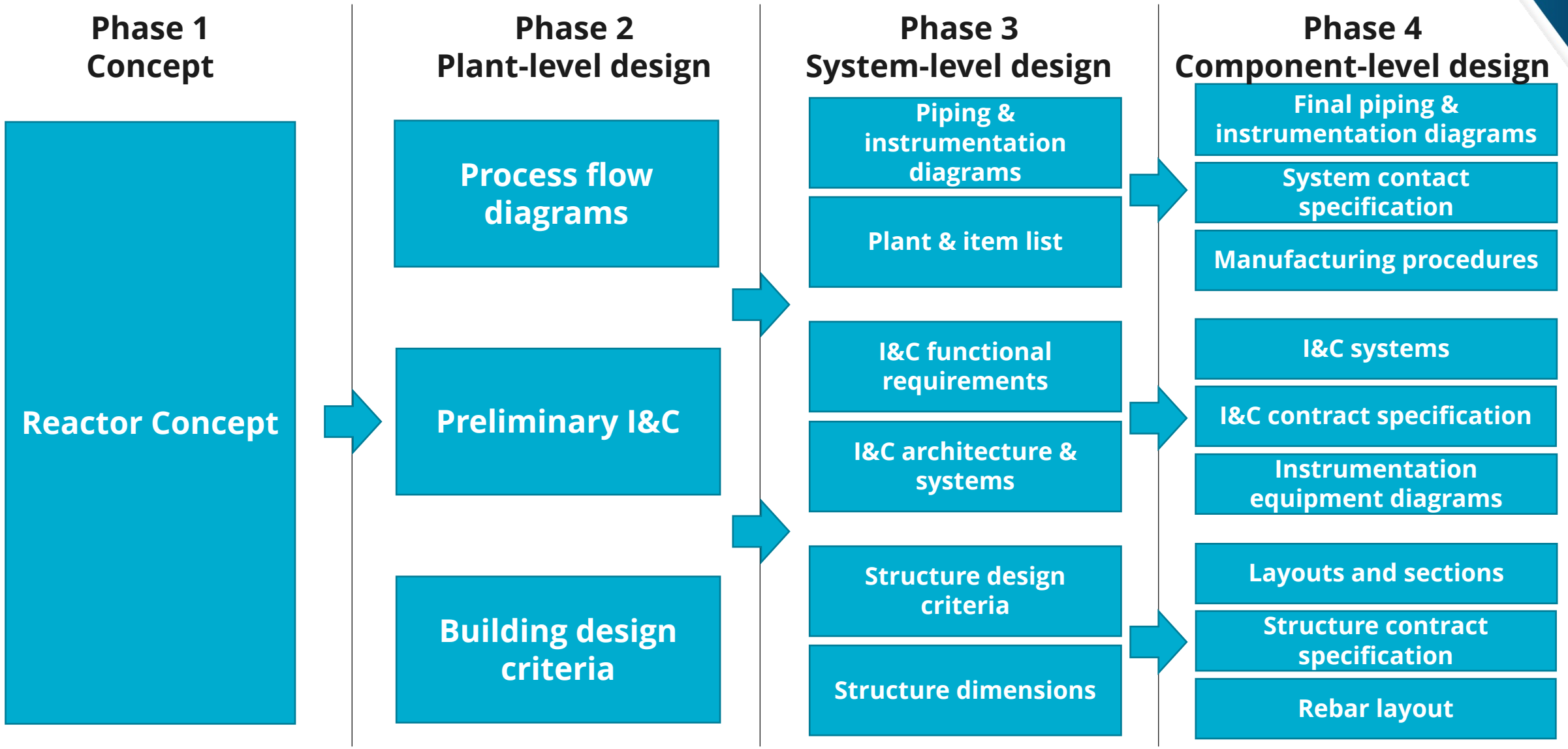
The Tiered Cybersecurity Analysis (TCA) in RG 5.96 leverages security-by-design (SeBD) features

For all accident sequences that are not eliminated by SeBD requirements

For all systems with susceptible access pathways



TCA Algins with WNA Phases Of Design Maturity



Citation: World Nuclear Association, “Design Maturity and Regulatory Expectations for Small Modular Reactors”, 2021

TIER 1 – CONSEQUENCE PRIORITIZATION/AVOIDANCE

- Goal: Risk avoidance; avoid or eliminate severe and unacceptable consequences
- Adversary characteristics: omnipotent, omniscient, and ever-present – able to change any digital information at will.
- Identify robustness factors - elements within the design that leverage physical phenomena to counteract cyber-attacks
- Effects of Robustness Factors may:
  - Limit the adverse impacts of the cyber-attack (e.g., shutdown to prevent accident conditions)
  - Introduce negative feedback that act against the cyber-attack, thereby allowing for process control to be re-established.
  - Attenuate the response to the cyber-attack making other measures, like non-cyber Independent Protection Layers (IPL) more effective.
- Identify non-cyber IPLs (e.g.., pressure release valves, pump speed governors) that complement or reinforce robustness factors
- Cyber-attacks with impacts/consequences not avoided or eliminated flow down to Tier 2.

TIER 2 – PASSIVE DEFENSIVE ARCHITECTURE & PROHIBITIONS

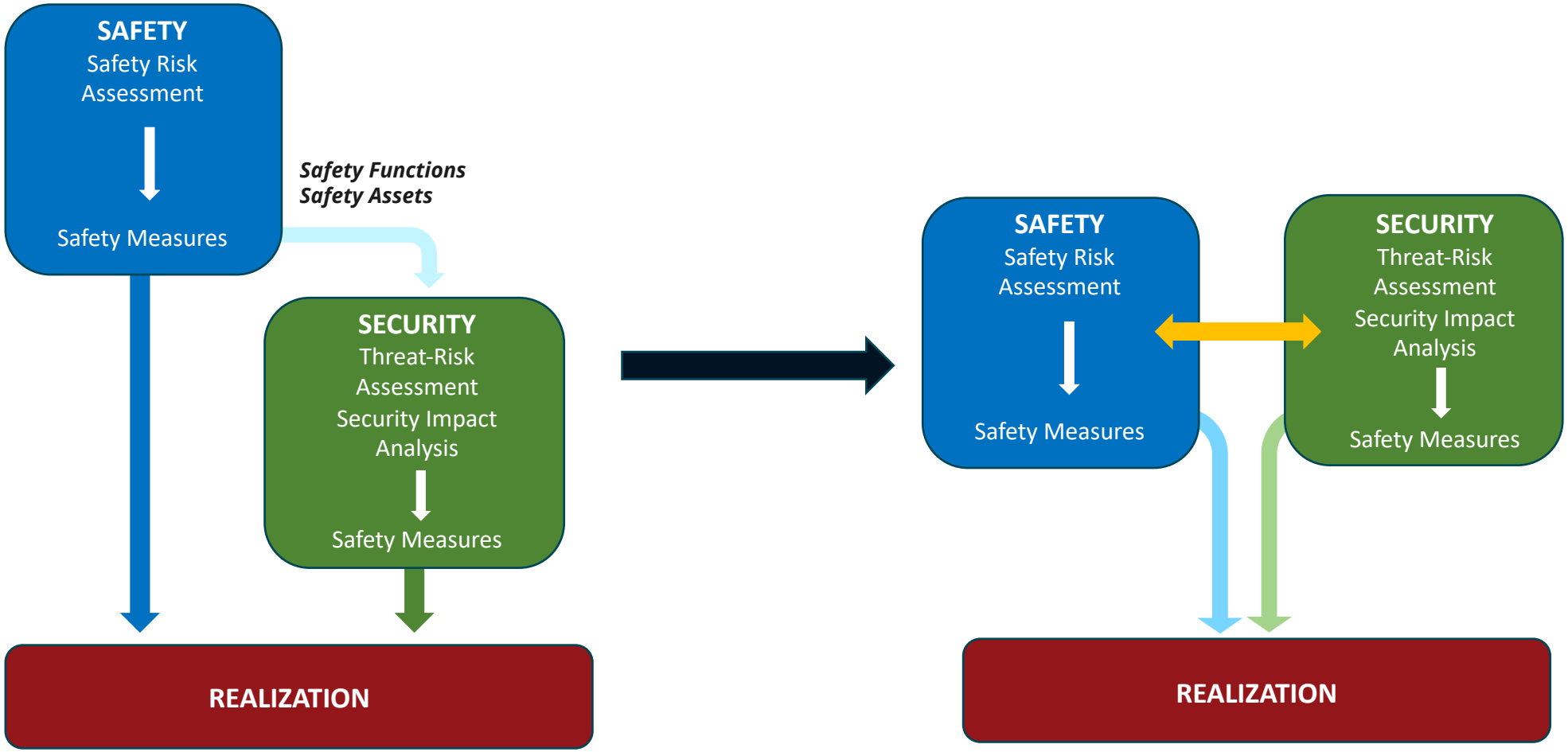
- Goal: Eliminate a sufficient number of pathways to ensure no possible manner for adversary to gain the accesses necessary to complete the scenario (e.g., similar to removing dominos to stop a sequence of dominos falling)
- Adversary characteristics: If the pathway is available on a system, the adversary is able to progress the scenario in the most advantageous manner.
- Focus on 4 attack pathways
  - Physical
  - Wired Network
  - Wireless Network
  - Portable Media and Mobile Devices
- Requires a Control System Architecture (System of Systems)
- Implement layered defense in depth
- Scenarios that can be completed will flow down to Tier 3

TIER 3 – ACTIVE DEFENSE (DETECT, DELAY, RESPOND, RECOVER)

- Goal: Implement and sustain protection (Detect, delay, and response) to ensure an adversary cannot successfully complete all the tasks prior to effective response to achieve the scenario outcome.
- Adversary characteristics: Credible adversary based on current threat intelligence (continually evolving)
- Detection and Response measures and processes are prioritized
- Requires a complete design as detection and response are heavily dependent on specific technology.
- Prevention activities that require management such as system hardening, patching vulnerabilities and eliminating exposures are necessary to improve detection and response.
- Unprotected scenarios associated with unacceptable consequences will demand remedial action.

INTEGRATED SAFETY-CYBERSECURITY DESIGN & LICENSING

SEQUENTIAL VS. PARALLEL DESIGN OF SECURITY AND SAFETY REALIZATION



Sequential Design of Security and Safety Realization

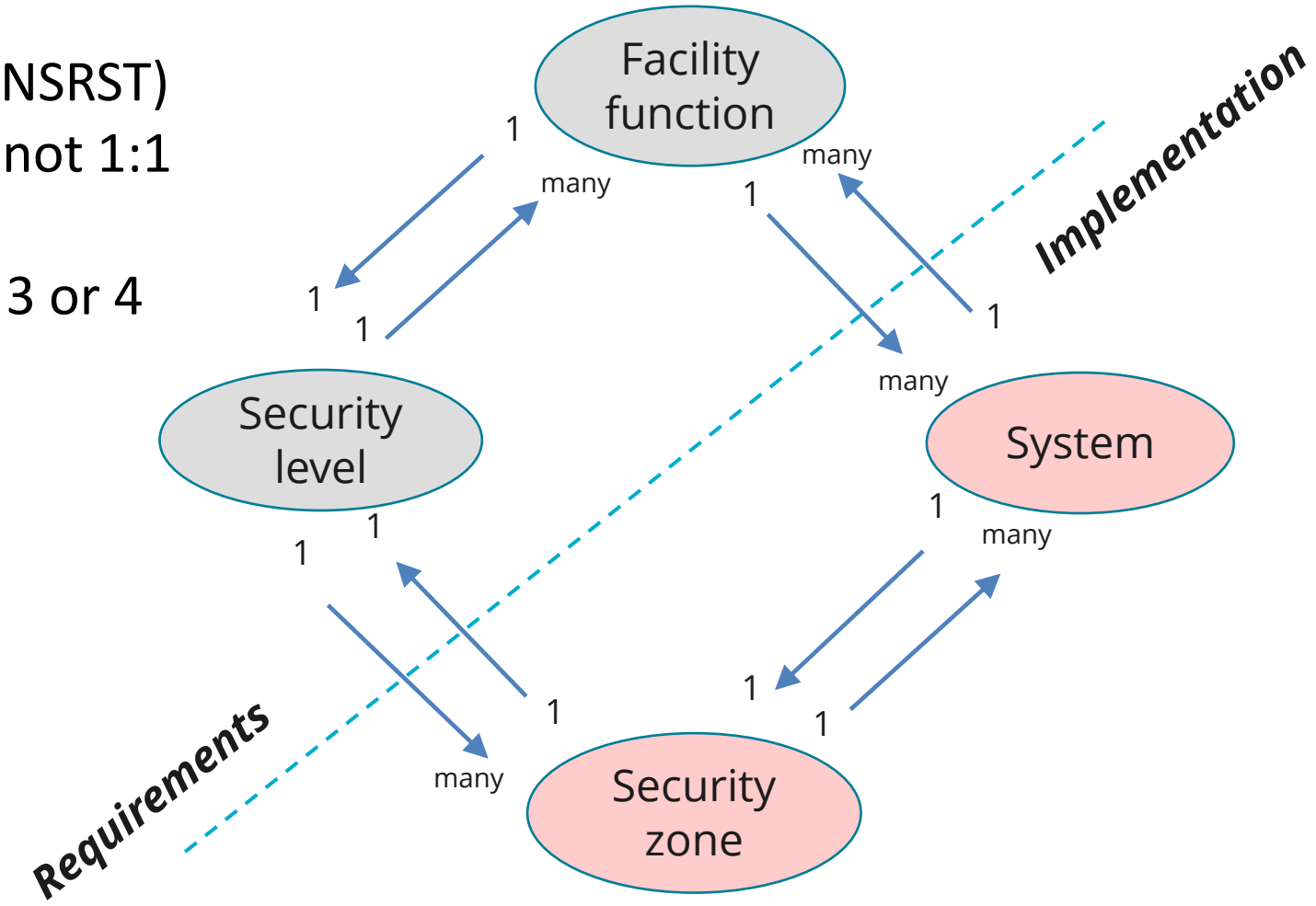
- Historical approach leading to bolt-on cybersecurity
- Less effective potential for non-compliance redesign

Parallel Design of Security and Safety Realization

KEY CYBERSECURITY CONCEPTS

Facility Functions

- Safety Categorization (SR, ITS, NSRST)
- Security Levels are similar but not 1:1
- SR assigned Security Level 4
- NSRST assigned Security Level 3 or 4



NRC DESIGN REVIEW GUIDE I&C SYSTEM REVIEW FRAMEWORK

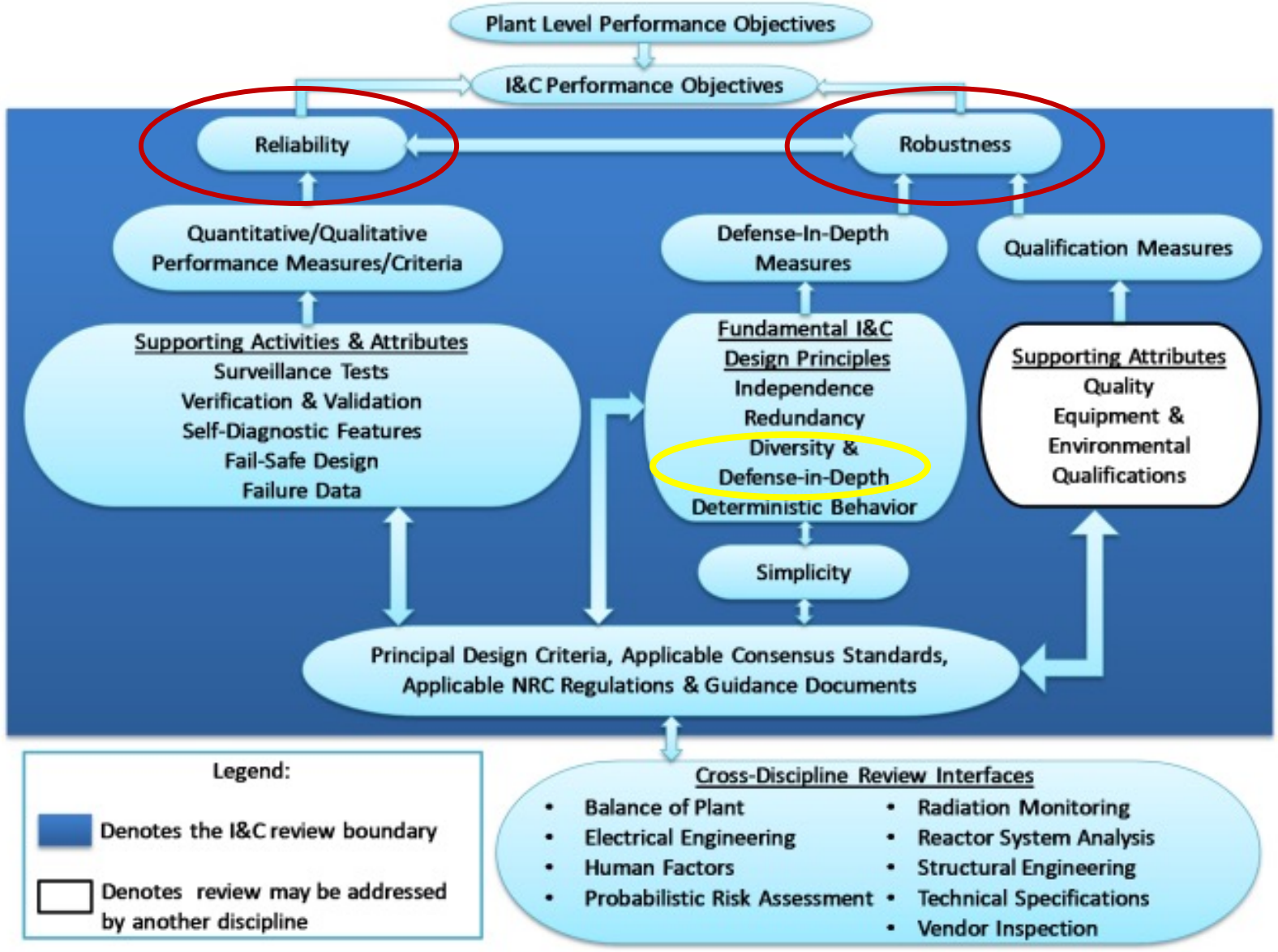


Figure X-1. I&C System Review Framework

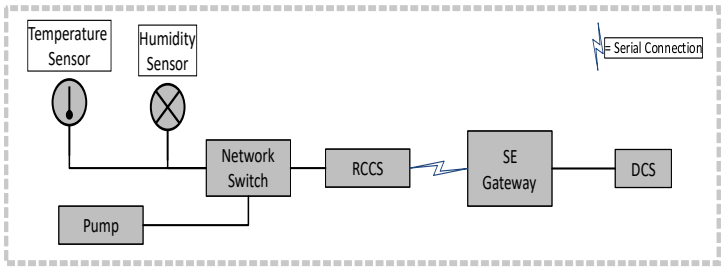
Cybersecurity Resilience = Robustness & Reliability

IDENTITY EVALUATION CRITERIA TAXONOMY AND EXAMPLE LIST

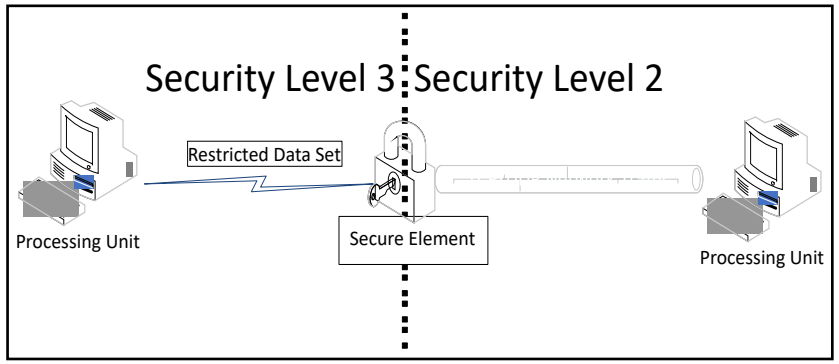
Property – Reliability	
Category	Attribute
Diversity	Layered Defense
	Cryptographic Mechanisms
	Tamper Resistance
Fail-Safe / Secure	Secure Error Handling/Recovery
	Integrity Protection Measures
	Fail Secure / Robust Error Handling
Independence	Information Independence
	Design Longevity
	Minimal Administrative Controls
	Proximity Effect Protection
Determinism	Rigidity
	Causality
	Minimalist Design

IDENTITY EVALUATION CRITERIA PROCESS EXAMPLE

Flow Diagram



Digital Design Candidate



Attributes of the Category of Diversity

Attribute	Score	Justification
Tamper Resistance	High	The design will implement a Common Criteria certified secure element. Common Criteria establishes requirements and testing specifically targeting tamper resistance on the device.
Cryptographic Mechanisms	High	SEs have access to many hardware-based encryption algorithms, secure random number generation and are beginning to have access to post-quantum algorithms [65]. These provide high fortification for this design.
Layered Defense	Low	The introduction of the Secure Element adds a new layer to the defense-in-depth of the design, securing the keys and cryptographic operations behind a hardened device. This design has direct connection between the two devices, providing no direct defense between the two. This improves on a software based device, but the use of a direct connection greatly hurts the design.
Secure Key Management	Medium	Keys are stored in a very secured manner and typically generated by the manufacturer. Secure Elements are designed with this feature in mind. In the event of a breach of keys, each device would need to have its keys revoked and rolled, which may increase outage times as each device has its own SE.
Summary	Medium	

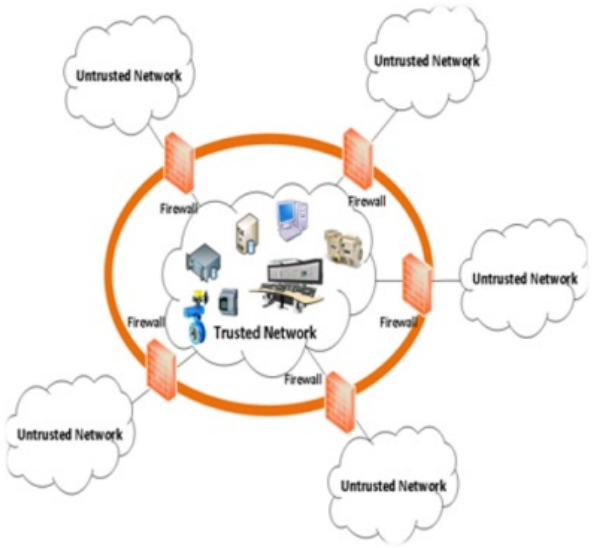
QUESTIONS?

THANK YOU

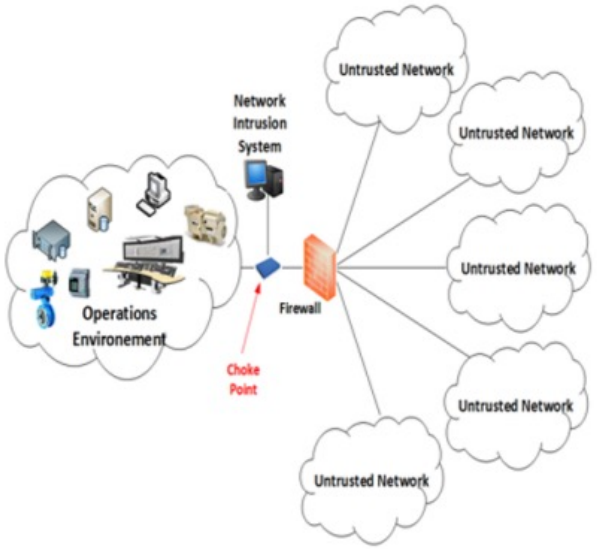
REFERENCES

CONCEPTUAL DEFENSIVE MODEL

RIPB - DEFENSIVE STRATEGIES



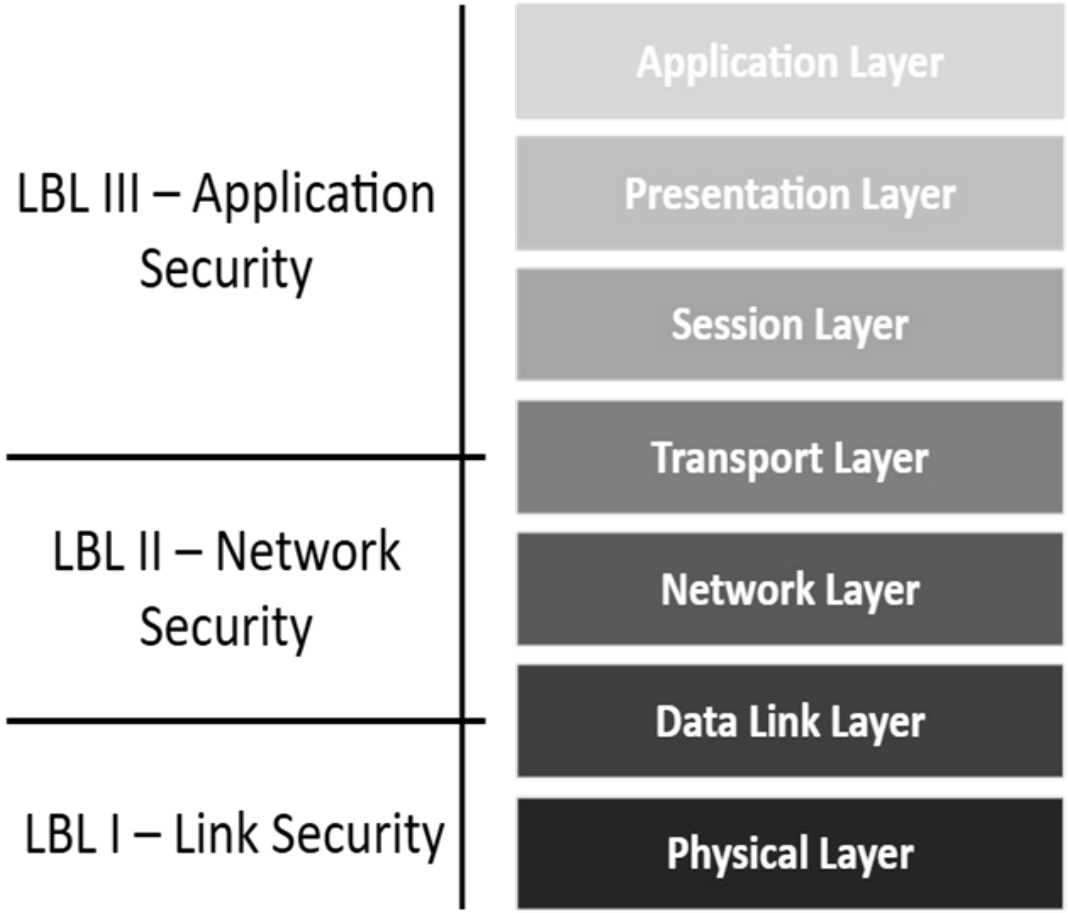
Fortification (F)



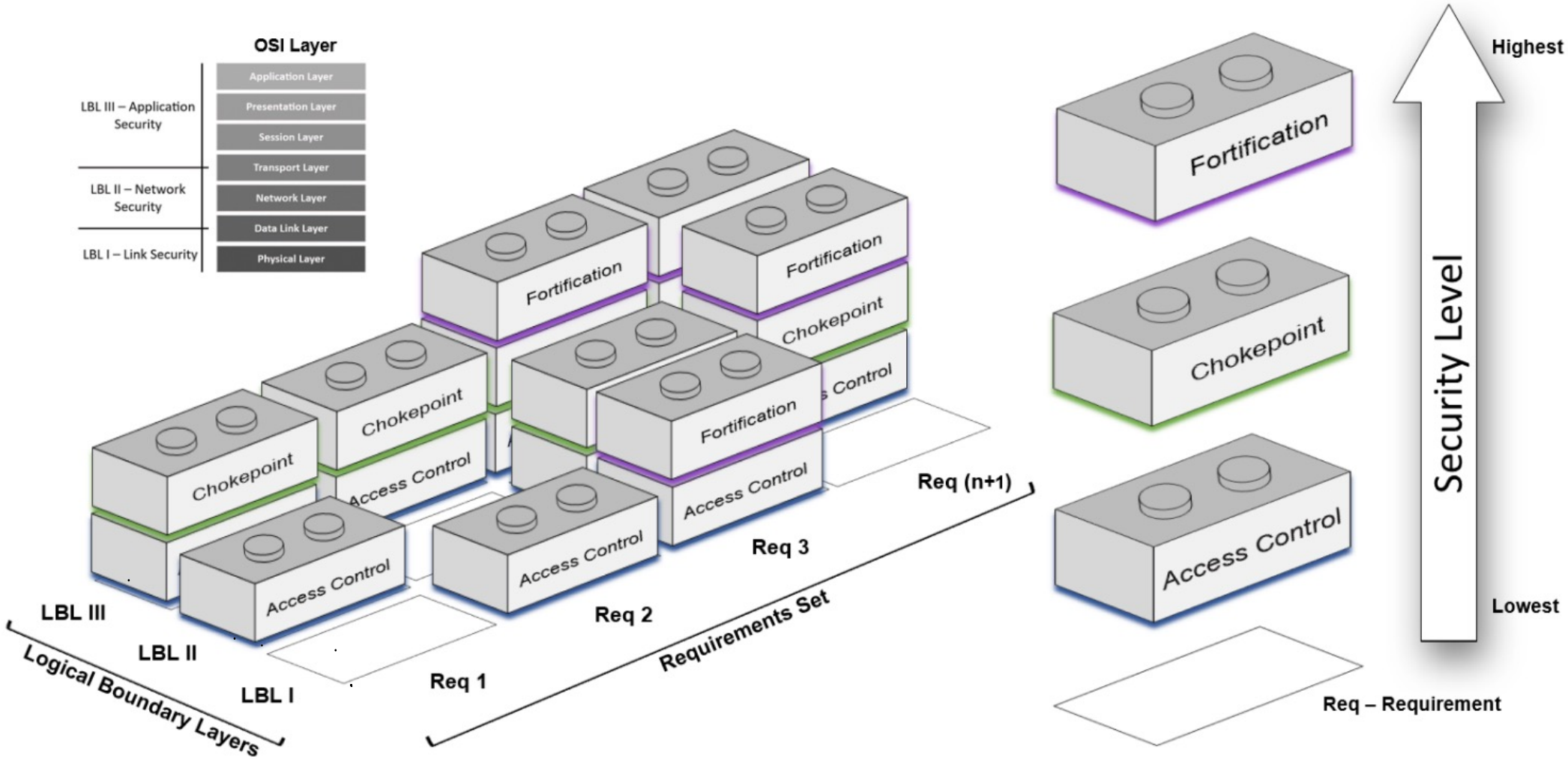
Chokepoint (CP)

Access Control (AC)

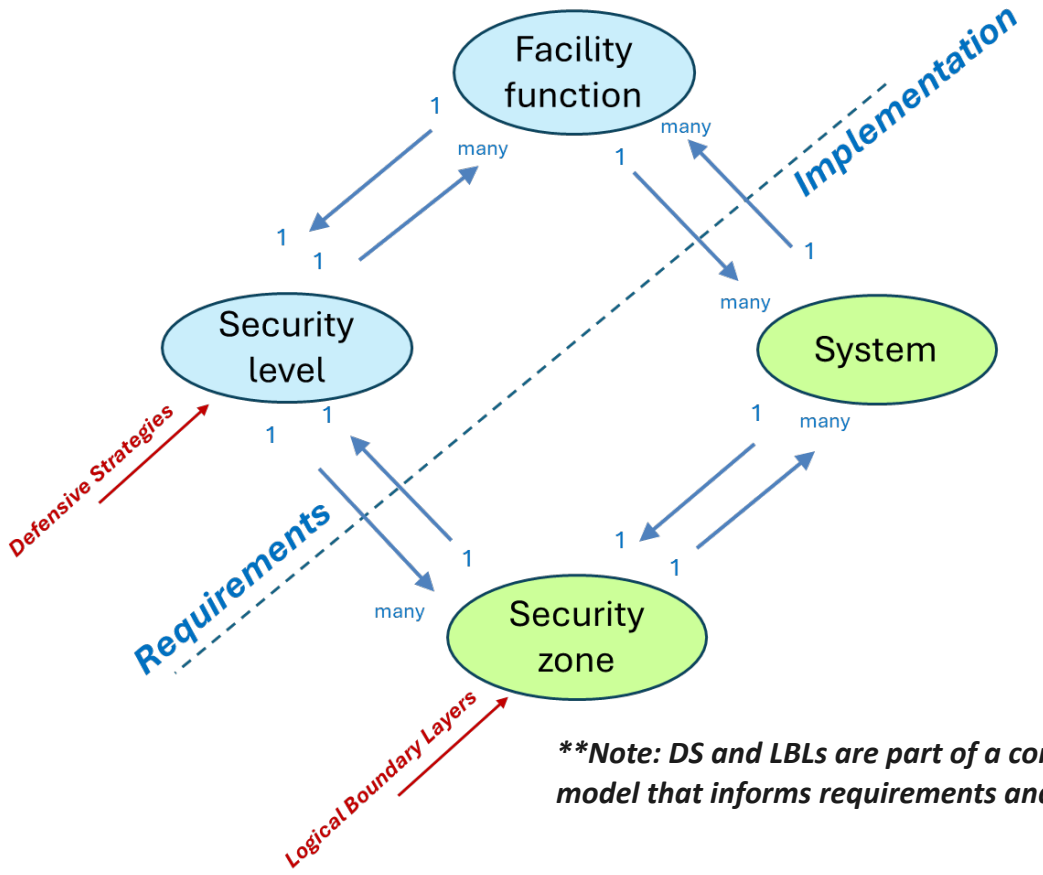
RIPB - LOGICAL BOUNDARY LAYERS



RIPB - DEFENSIVE STRATEGY AND LOGICAL BOUNDARY LAYER ALIGNMENT



RIPB – RELATIONSHIPS BETWEEN FACILITY FUNCTION, SECURITY LEVEL AND SECURITY ZONE



***Note: DS and LBLs are part of a conceptual defensive model that informs requirements and design features*

Facility Functions Inform Safety Categorization

- A, B, C
- SR, ITS
- SR, NSRST, NST
- Mirrored Process for Safety

INTEGRATION OF DESIGN PROCESS PHASES WITH I&C LIFECYLE AND CYBERSECURITY CONSIDERATIONS

Design Process Phase [EPRI DEG Rev 1]	I&C Lifecyle Phase(s) [IAEA NR-T-3.30]	Cybersecurity [IAEA NR-T-3.30]	Rationale
Strategic Planning	N/A	N/A	Occurs prior to the overall I&C lifecycle.
Initial Scoping	Process Planning	Cybersecurity Program (CSP) Design Basis Threat and Security Risk Assessment	Programmatic requirements that impose cybersecurity demands.
Conceptual Design	I&C Design Basis	Security Levels	Application of graded sets of requirements for cybersecurity. Establishes the number of graded levels that will be imposed by the program.
	I&C Architecture Design	Defensive Cybersecurity Architecture (DCSA) Specification	Architectural (common) requirements that when implemented provide defense in depth.
	Functional Assignment to Systems	N/A	Although not explicit, both Security Levels and DCSA contain requirements for functional assignment to systems.
Detailed Design	Process Planning	Contingency plans for development Requirements for Secure Development environment	The cybersecurity outputs are associated with the entire system lifecycle. Process planning would need to consider these outputs that impose common demands upon all detailed design phases.
	Requirements Specification	Cybersecurity Requirements	Specific system requirements that may be common to the security level or additional or deviations from them.
	Selection of Pre-Developed Items	Security Qualification	Similar to safety SIL certification, Common Criteria, ISA-Secure provide key tests and results to support selection of pre-developed items [35].
	System Specification Detailed Design and implementation	Computer Security Assessments Verification Reports	These cybersecurity outputs are assigned to multiple phases; however, these outputs have particular importance to these phases, particularly verification reports, which confirm the results of each phase.
	System Integration & Validation	Validation Report Baseline Security information	Validates and provides information on security measures and system behaviors when attacked.

INTEGRATION OF DESIGN PROCESS PHASES WITH I&C LIFECYLE AND CYBERSECURITY CONSIDERATIONS

Design Process Phase [EPRI DEG Rev 1]	I&C Lifecyle Phase(s) [IAEA NR-T-3.30]	Cybersecurity [IAEA NR-T-3.30]	Rationale
Detailed Design	Process Planning	Contingency plans for development Requirements for Secure Development environment	The cybersecurity outputs are associated with the entire system lifecycle. Process planning would need to consider these outputs that impose common demands upon all detailed design phases.
	Requirements Specification	Cybersecurity Requirements	Specific system requirements that may be common to the security level or additional or deviations from them.
	Selection of Pre-Developed Items	Security Qualification	Similar to safety SIL certification, Common Criteria, ISA-Secure provide key tests and results to support selection of pre-developed items [35].
	System Specification Detailed Design and implementation	Computer Security Assessments Verification Reports	These cybersecurity outputs are assigned to multiple phases; however, these outputs have particular importance to these phases, particularly verification reports, which confirm the results of each phase.
	System Integration & Validation	Validation Report Baseline Security information	Validates and provides information on security measures and system behaviors when attacked.