SAND2023-05355C

Sandia National Laboratories

Exceptional service in the national interest

An Efficient Graded Approach for the Design of Secure I&C Systems

Lee T. Maccarone, Jacob R. James, Daniel R. Sandoval, Alexandria W. Haddad, Michael T. Rowland

ICONE30; 21-26 May 2023; Kyoto, Japan

Sandia National Laboratories
U.S. DEPARTMENT OF ENERGY NNSA

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.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and wholly owned subsidiary of Honeywell International Inc. for the U.S. onal Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY
NNSA

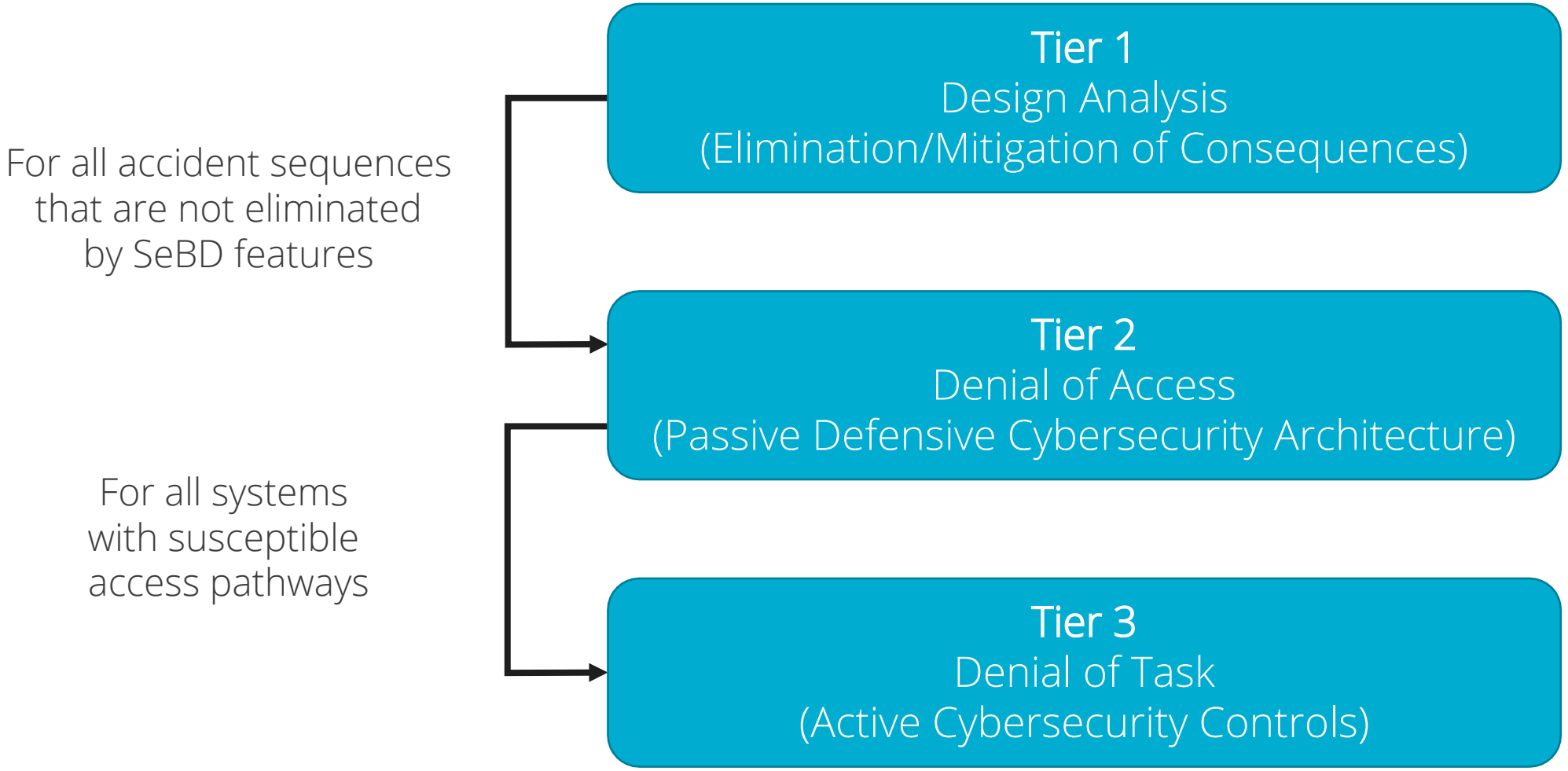
Why use the Tiered Cybersecurity Analysis (TCA)?

- The TCA provides a structured approach to analyze the cybersecurity of nuclear power plant I&C systems
- The TCA allows plant physics or security-by-design (SeBD) features to be credited for cybersecurity before applying passive or active controls
- Implementation of the TCA may result in reduced cybersecurity costs and improved cybersecurity posture
- The TCA was presented by the US NRC at the IAEA Technical Meeting on I&C and Computer Security for SMRs and Microreactors

What is the TCA?

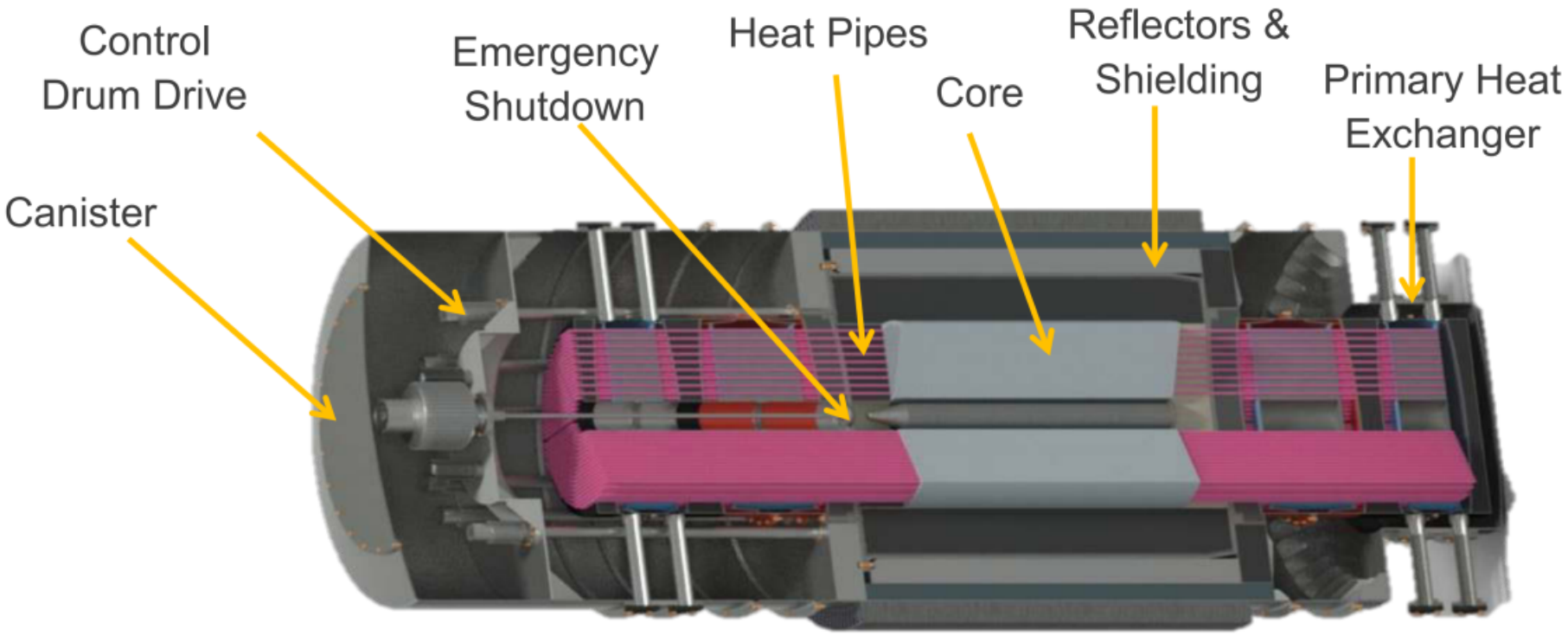
Security-by-design (SeBD) is a core component of the draft US NRC advanced reactor regulatory guide

Tiered Cybersecurity Analysis (TCA)



How is the TCA applied?

Candidate System: Heat-Pipe Microreactor



All analysis is based upon publicly available documentation and engineering judgment

Citation: Southern Company, "Westinghouse eVinci Micro-Reactor Licensing Modernization Project Demonstration," 2019.

Tier 1: Design Analysis

Systems-Theoretic Process Analysis (STPA)

1. Define the purpose of the analysis
2. Model the control structure
3. Identify unsafe control actions (UCAs)
4. Identify loss scenarios

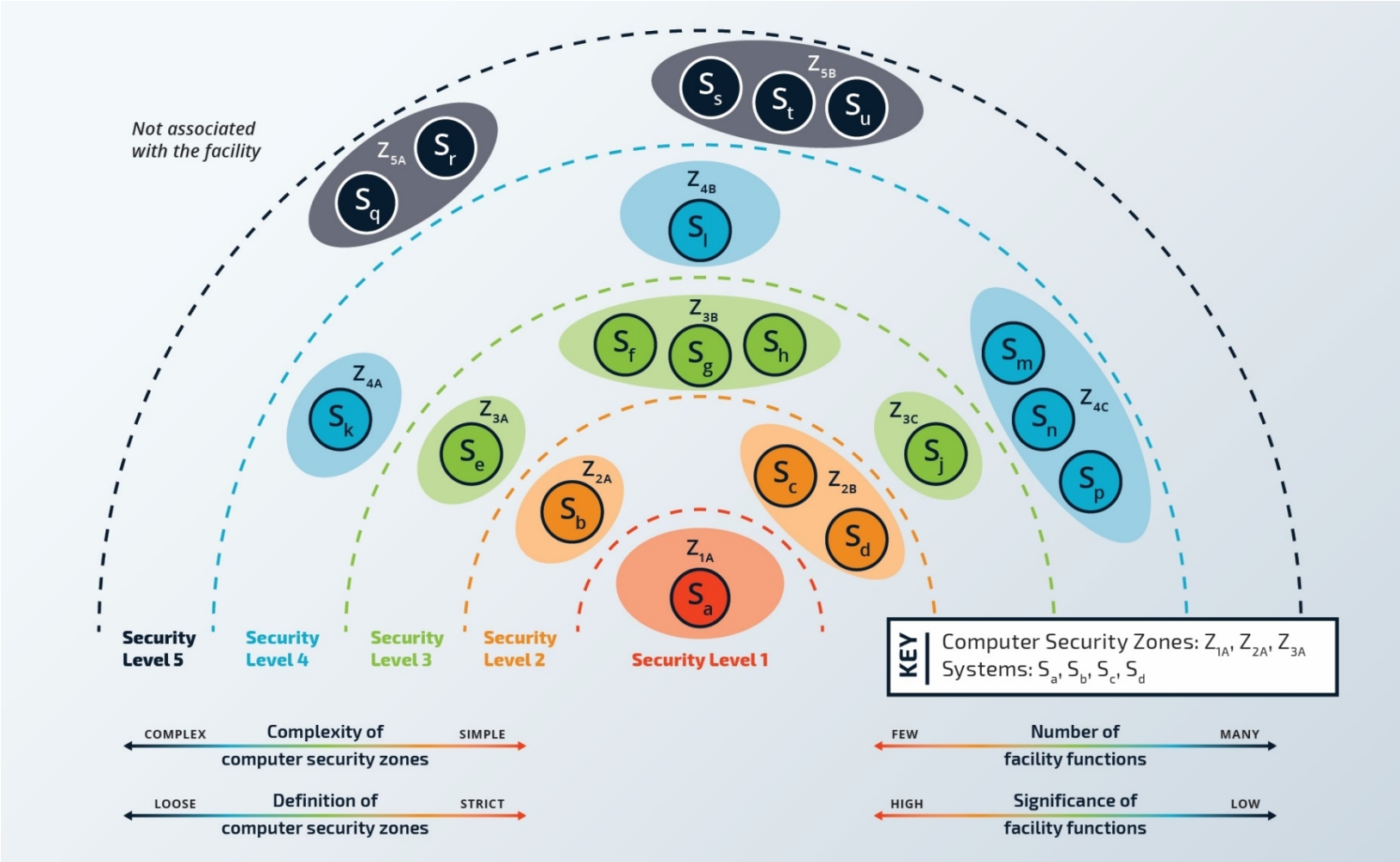
Citation: N. G. Leveson and J. P. Thomas, "STPA Handbook," 2018.

Example Impact Scenario: Feedback of Control Drum Position

Tier 1
Tier 2
Tier 3

Compromise	Unsafe Action	Design Basis	Design Requirement
Adversary sends false CD position to controller to keep the CD in turned in position when the plant is at power	CD controller fails to provide “turn out” signal to CD when reactivity insertion is not needed	Defense-in-depth with sensor diversity and redundancy	The feedback signal for the CD position shall be collected from multiple polled sensors

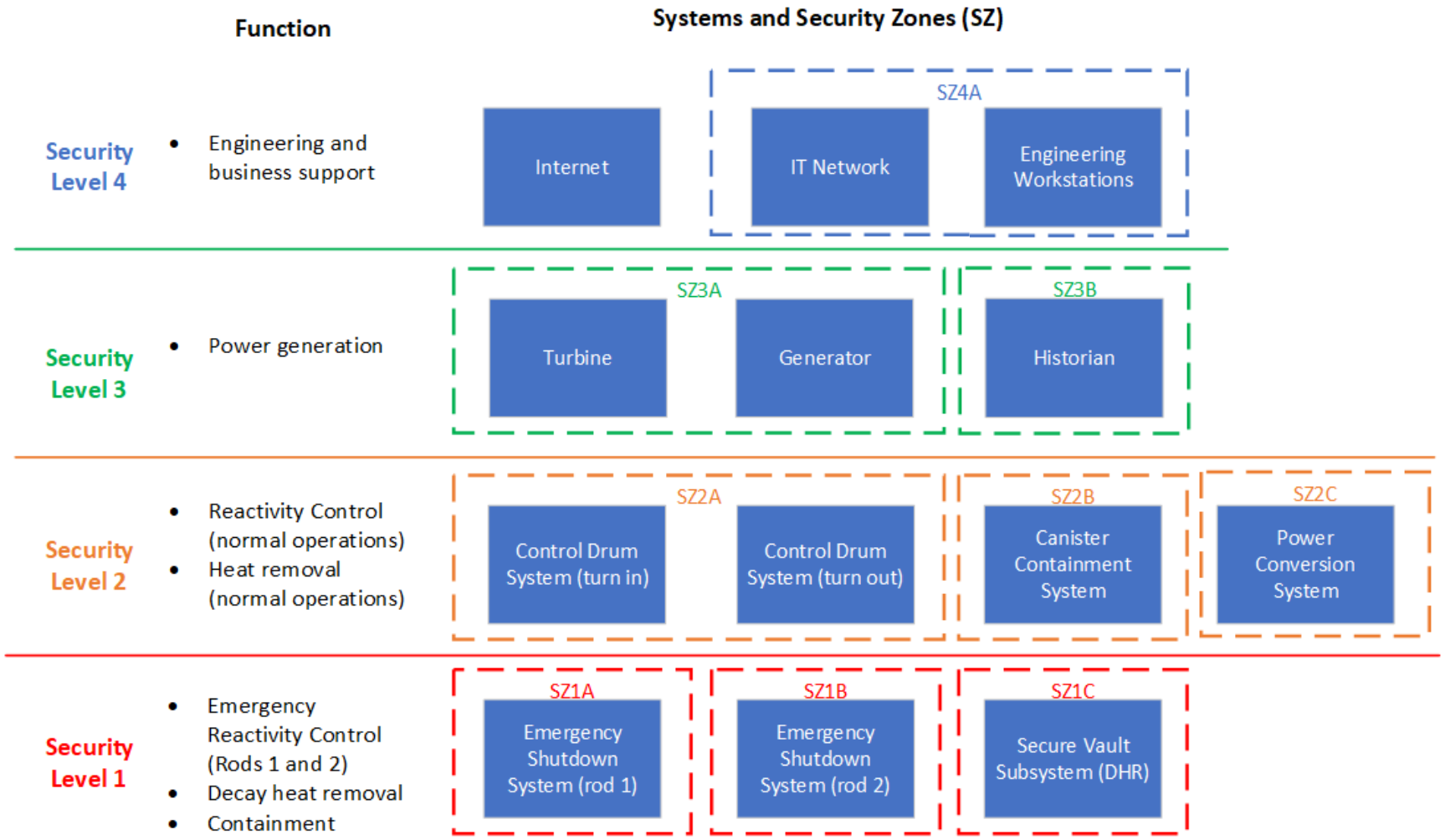
Tier 2: Denial of Access



Defensive Cybersecurity Architecture (DCSA)

Citation: International Atomic Energy Agency, "NSS 17-T: Computer Security Techniques for Nuclear Facilities," IAEA, Vienna, Austria, 2021.

DCSA Implementation



DCSA Policies

SL	Policies
SL 1	• Strict physical barriers in place. Staff access should be highly monitored. • Network communication between SL1 and a lower security level is prohibited. • Wireless communication prohibited in SL1. • Routine monitoring for detection of rogue wireless access points is required.
SL 2	• Physical access to devices in this region is strictly controlled and monitored. • Only one-way network communication between SL2 and lower security levels is allowed. • Wireless devices are allowed but must only be used for sensing and cannot have an impact on the control system. The wireless network must be separate from any process-critical control networks.
SL 3	• Physical access to devices in this region is controlled and monitored. • Bidirectional communication between SL3 and lower-security levels is not prohibited for zones which contain digital I&C components. • Wireless devices are allowed for non-I&C communication.
SL 4	• Internet connection is allowed and controlled. • Wireless communication is allowed and controlled. • Access control lists are reviewed periodically.

Tier 3: Denial of Task

- Tier 3 not completed in this analysis due to extensive component-level assumptions required
- Supporting toolset examples:
  - MITRE ATT&CK for ICS
  - MITRE D3FEND
  - Lockheed Martin Cyber Kill Chain

Concluding Remarks

1. The TCA is a performance-based cybersecurity approach
2. The TCA enables advanced reactor designers to credit plant physics towards cybersecurity before applying passive and active controls
3. The TCA has the potential to reduce cybersecurity costs and improve cybersecurity posture
4. Future research will examine optimal alignment of the TCA with phases of plant design maturity

Thank you for your time and attention

Contact Information:
Lee Maccarone
lmaccar@sandia.gov