ADVANCED REACTOR SAFEGUARDS & SECURITY

Defensive Cybersecurity Architecture (DCSA)

2026 ARSS Spring Program Review

PRESENTED BY

Lee Maccarone

29 April 2026

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.

SAND2026-20509PE

Research Questions & Goals

- How do we protect facility functions to minimize the impact of an adversary who has gained access to plant systems?
- How can we provide evidence to assure the efficacy of our DCSA designs?
- Goals:
  - Provide starting point for industry with microreactor DCSA template
  - Demonstrate DCSA design as part of a security-by-design (SeBD) approach

DCSA is a key part of the Part 53 cybersecurity regulatory guide (RG 5.96)

For all accident sequences that are not eliminated by SeBD requirements

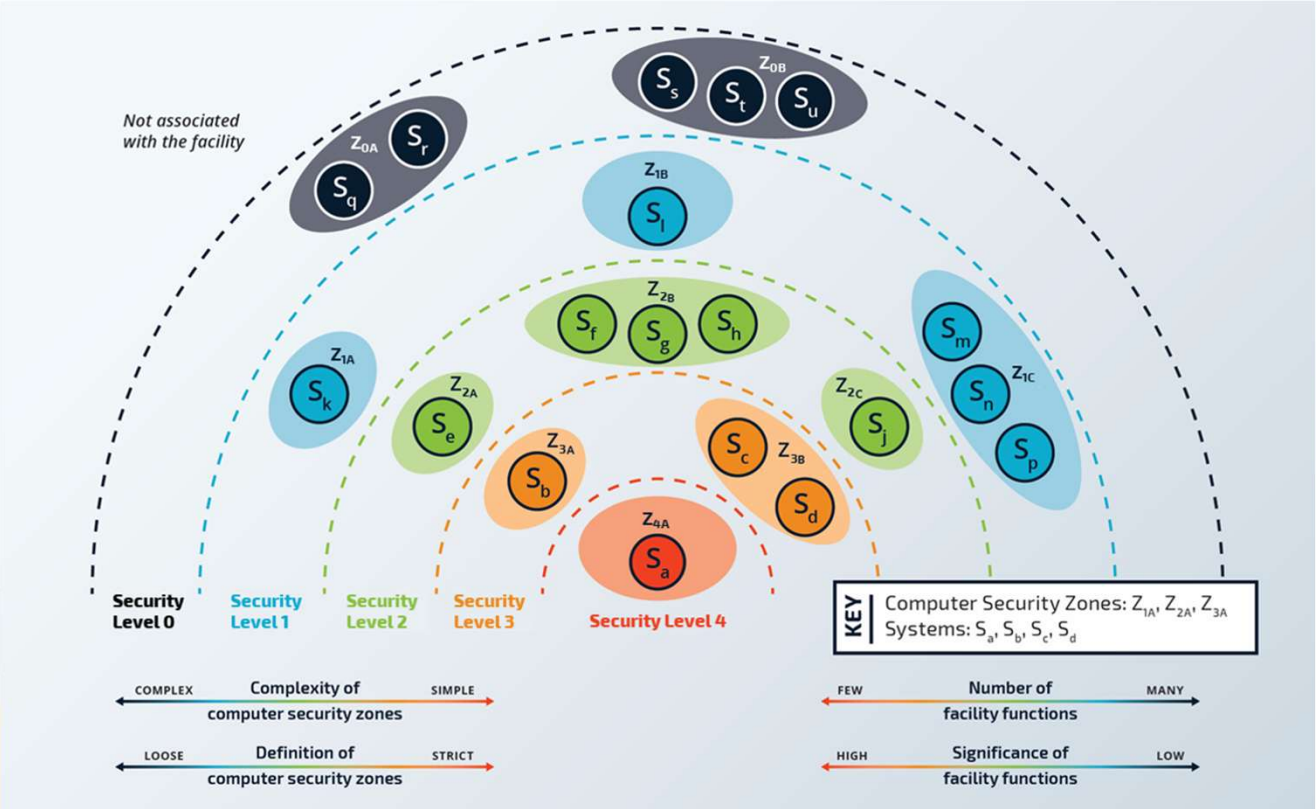
For all systems with susceptible access pathways

Tier 1
Design Analysis
(Elimination/Mitigation of Consequences)

Tier 2
Denial of Access
(Passive Defensive Cybersecurity Architecture)

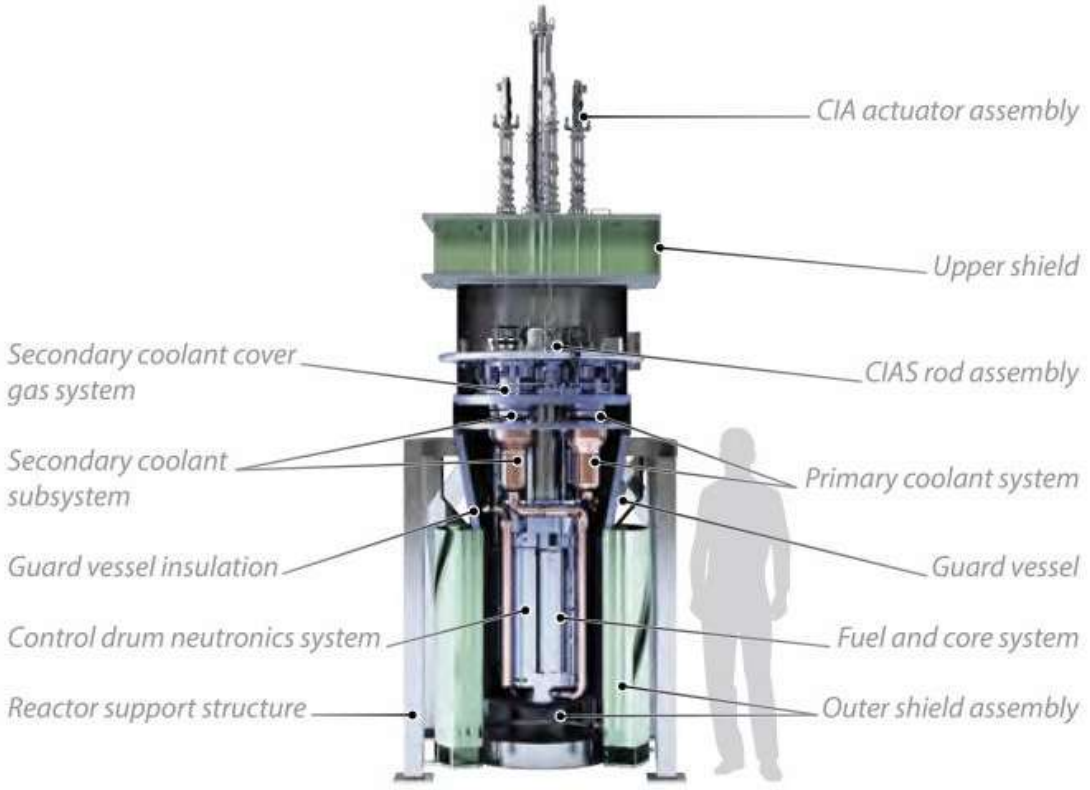
Tier 3
Denial of Task
(Active Cybersecurity Controls)

DCSA Model


Not associated with the facility
Z_{0B}
S_s S_t S_u
Z_{0A}
S_r S_q
Z_{1B}
S_l
Z_{2B}
S_f S_g S_h
Z_{1A}
S_k
Z_{2A}
S_e
Z_{3A}
S_b
Z_{2C}
S_j
S_m S_n S_p
Z_{1C}
S_c Z_{3B} S_d
Z_{4A}
S_a
Security Level 0
Security Level 1
Security Level 2
Security Level 3
Security Level 4
KEY
Computer Security Zones: Z_{1A}, Z_{2A}, Z_{3A}
Systems: S_a, S_b, S_c, S_d
COMPLEX
Complexity of computer security zones
SIMPLE
LOOSE
Definition of computer security zones
STRICT
FEW
Number of facility functions
MANY
HIGH
Significance of facility functions
LOW

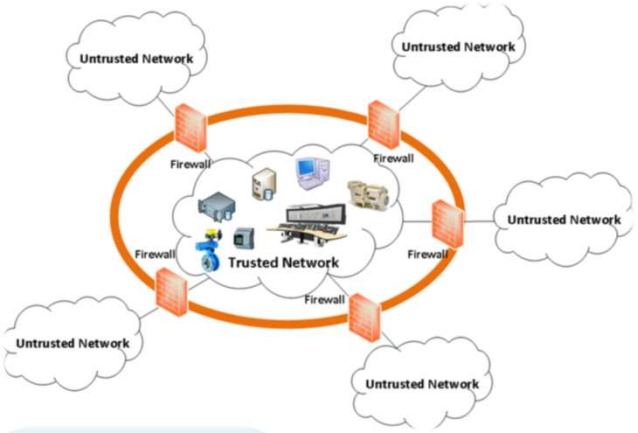
Technical Approach

1. Literature review of microreactor documentation
2. Identify plant functions and their corresponding systems
3. Identify the most significant function performed by each system
4. Place systems into security zones
5. Conduct pathway and dependency analysis
6. Assign cybersecurity controls to DCSA design

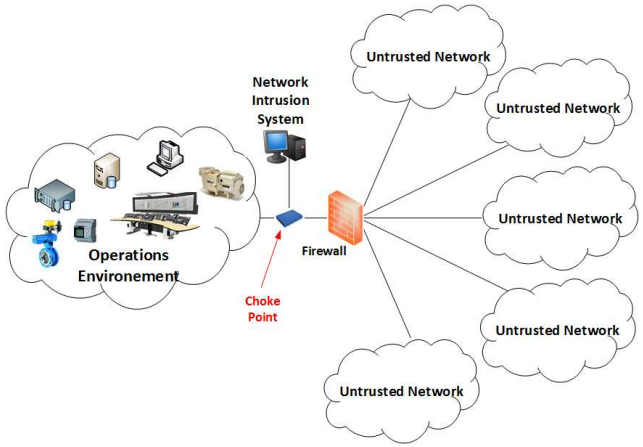


Citation: ANS. https://www.ans.org/news/article-7600/inl-announces-five-teams-for-marvel-project/, 2026.

Defensive Strategies



Fortification



Choke-Point

Access Control

Demonstrated selection of passive cybersecurity controls

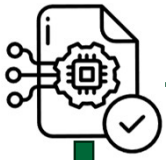
Table X. Portable Media and Mobile Devices Attack Pathway Cybersecurity Controls

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
1	B.1.19	Access Control for Portable Media and Mobile Devices	Establish usage restrictions for portable media and enforce mobile devices are only used in one security level and that mobile devices are not mobile between security levels	Fortification, Access Control	Restrict mobile devices to a single security zone: Define zones by hardware and network layers, issue zone specific X.509 certificates and bind them to the device TPM. 8021.X/NAC admits the device only to its home virtual local area network (VLAN).
				Fortification, Chokepoint	1. Physical segregation and access points: Utilize Faraday-caged cabinets at each zone boundary, enforcing personnel to deposit devices before crossing to another level. Apply tamper-evident seals 2. One-zone-only firmware settings: Lock BIOS to disable WiFi/Bluetooth adapters not used in the assigned zones. Use Mobile device management solutions to force geofencing or SSID fencing by locking the device if it associates with an unapproved access point.

Formal methods provide mathematically rigorous guarantees that a system satisfies its specified safety and security properties

Formal Methods

Techniques grounded in mathematical logic for the specification, modeling, and verification of system requirements.



Translate specifications into a mathematical logic

Develop a formal model of the system (finite state machine, proof, etc.)

QED

Verify formal model of system complies with the specifications

Demonstrated Success in Mission-Critical Systems

HACMS
High Assurance Cyber Military Systems
DARPA

Proved security properties for a military aerial vehicle

Publication
How Amazon Web Services uses formal methods
By Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, Michael Deardeuff

Proved security and functional guarantees for cloud infrastructure

LANGLEY FORMAL METHODS

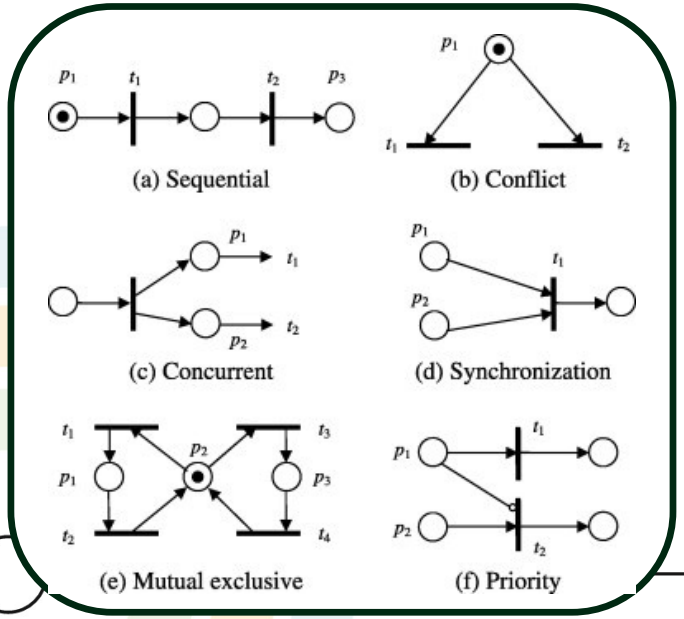
Proved safety properties for spacecraft autonomy

A Petri net is a formal method where reachability analysis can verify denial of adversary access

Petri Nets

A directed bipartite graph with an exact mathematical definition of its execution semantics, used to model concurrent, distributed, and event-driven systems.

Petri Nets Properties



Application to DCSA

DCSA element	Petri Net Element
Security Zone	Place
Interconnection / Pathway	Transition
Adversary Access in a Zone	Token in a place
Initial Attacker Condition	Initial Marking
Unacceptable Access Pattern	Target Marking

Formal Verification through Reachability Analysis

Exhaustively check all states of our DCSA modeled with Petri Net Elements. Analysis verifies that the DCSA denies access iff the target marking is unreachable from the initial marking.

Citation: Murata, Petri nets: properties, analysis and applications

Project Accomplishments & Status

- IAEA CyberCon paper:
  Presents risk-informed DCSA design approaches
- ANS Global Conference paper:
  Presents semantic structure for RG 5.96 cybersecurity analysis
- On track for FY26 M3 report
- Tasks to conclude FY:
  1. Complete dependency analysis
  2. Complete Petri net analysis
  3. Assign cybersecurity controls

Impact & Future Work

- Impact
  - Detailed demonstration of Tier 2 analysis for industry
  - Template of DCSA as starting point for one class of advanced reactor

- Integration with other ARSS projects:
  - ARCADE: Directly leverage ARCADE outputs as inputs for DCSA analysis, and automate DCSA analysis given those ARCADE results
  - Cyber-Physical Attack: Cyber-physical modeling and simulation data may be used for DCSA design for physical protection systems

Questions?

Contact: Lee Maccarone, lmaccar@sandia.gov

Team: Lee Maccarone, Robert Lois, Robert Brulles, Mike Rowland