ADVANCED REACTOR SAFEGUARDS & SECURITY

DCSA for HTGRs

Defensive Cyber Security Architecture

PRESENTED BY

Lee Maccarone

14 May 2024

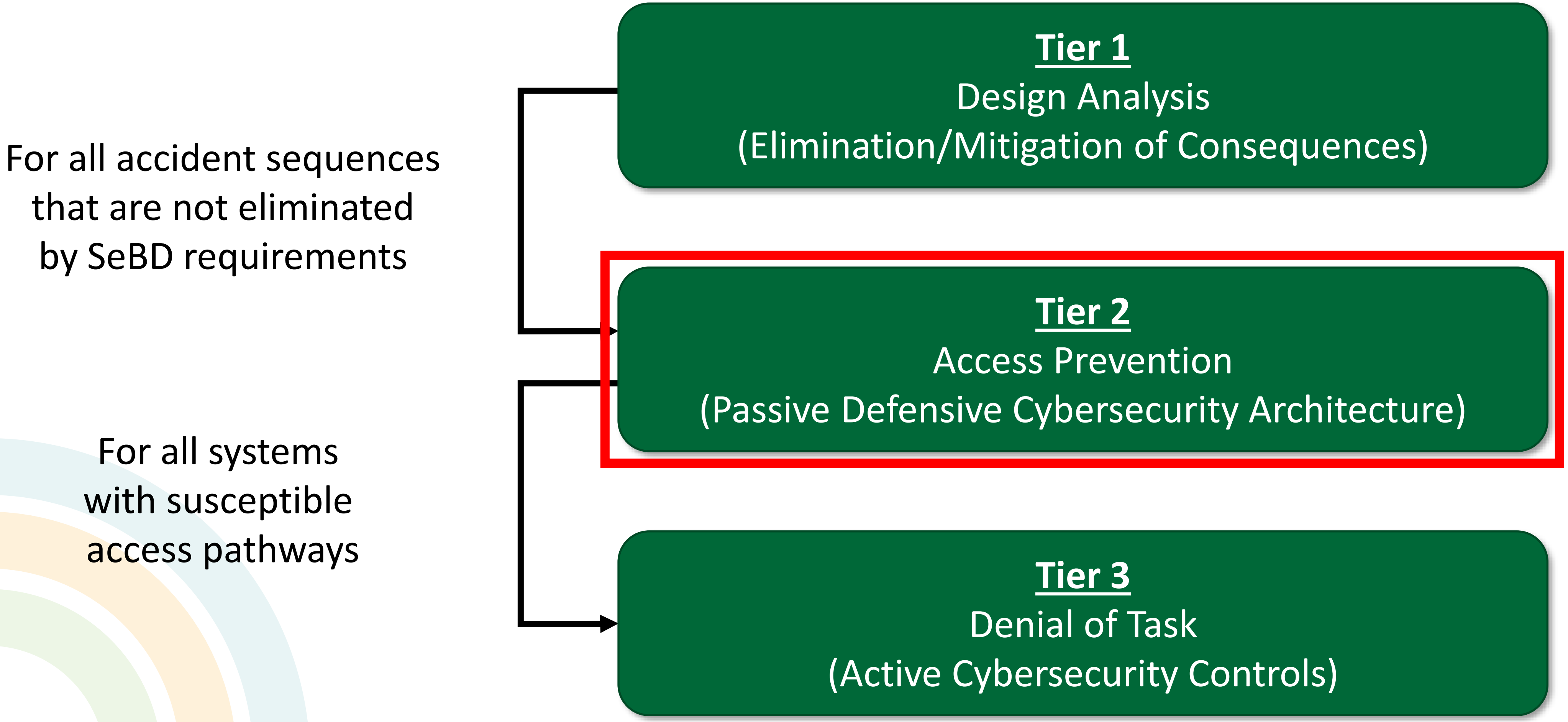
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2024-06070PE

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 architect our systems to maximize our opportunity to detect a cyber-intrusion?
- How can we leverage safety analyses to inform cybersecurity designs?
- Goals:
  - Demonstrate DCSA design approach (part of the draft AR cybersecurity reg. guide)
  - Provide HTGR DCSA template as starting point for industry

DCSA is a key part of the draft AR cybersecurity reg guide (DG-5075)



For all accident sequences that are not eliminated by SeBD requirements

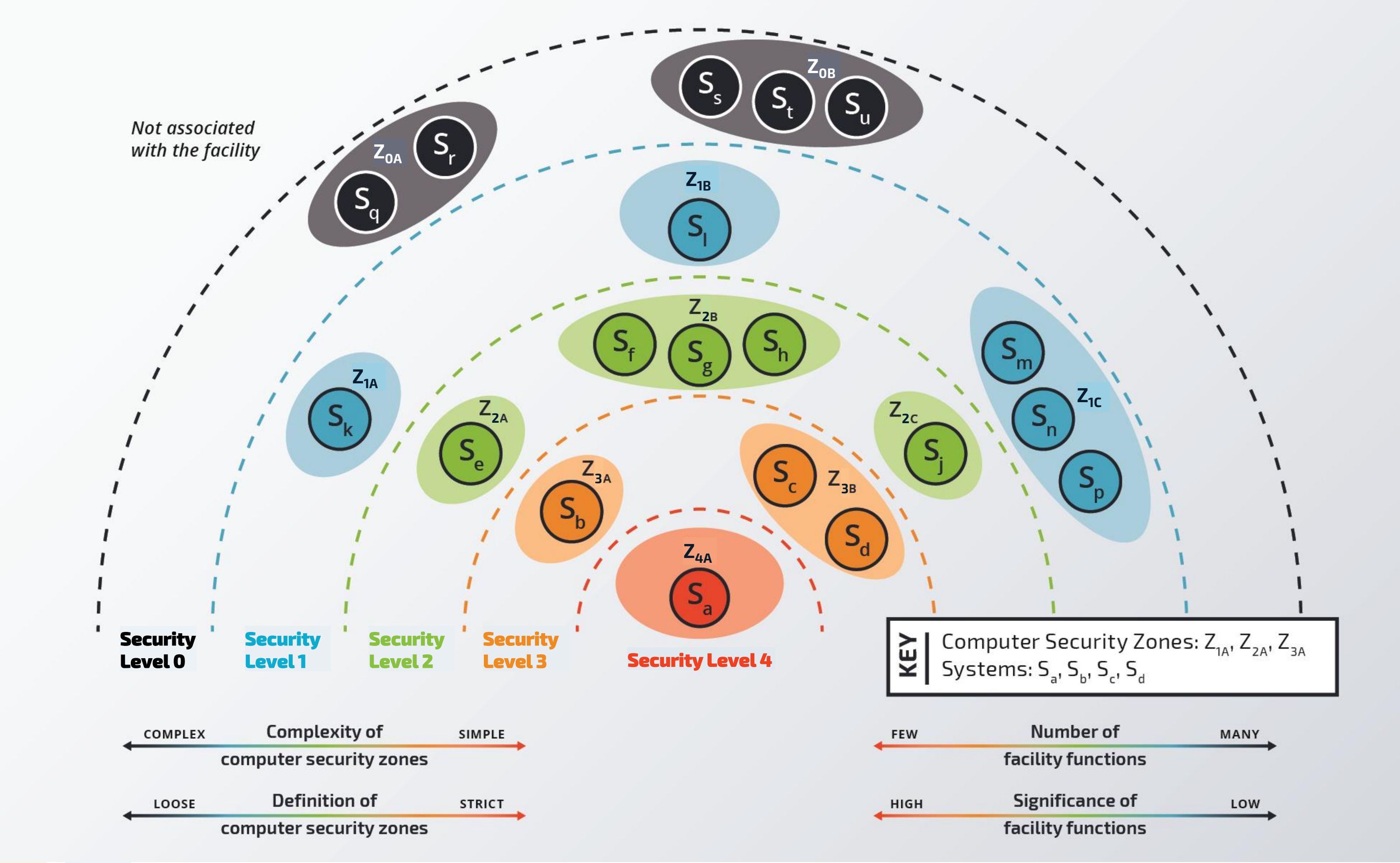
For all systems with susceptible access pathways

Tier 1
Design Analysis
(Elimination/Mitigation of Consequences)

Tier 2
Access Prevention
(Passive Defensive Cybersecurity Architecture)

Tier 3
Denial of Task
(Active Cybersecurity Controls)

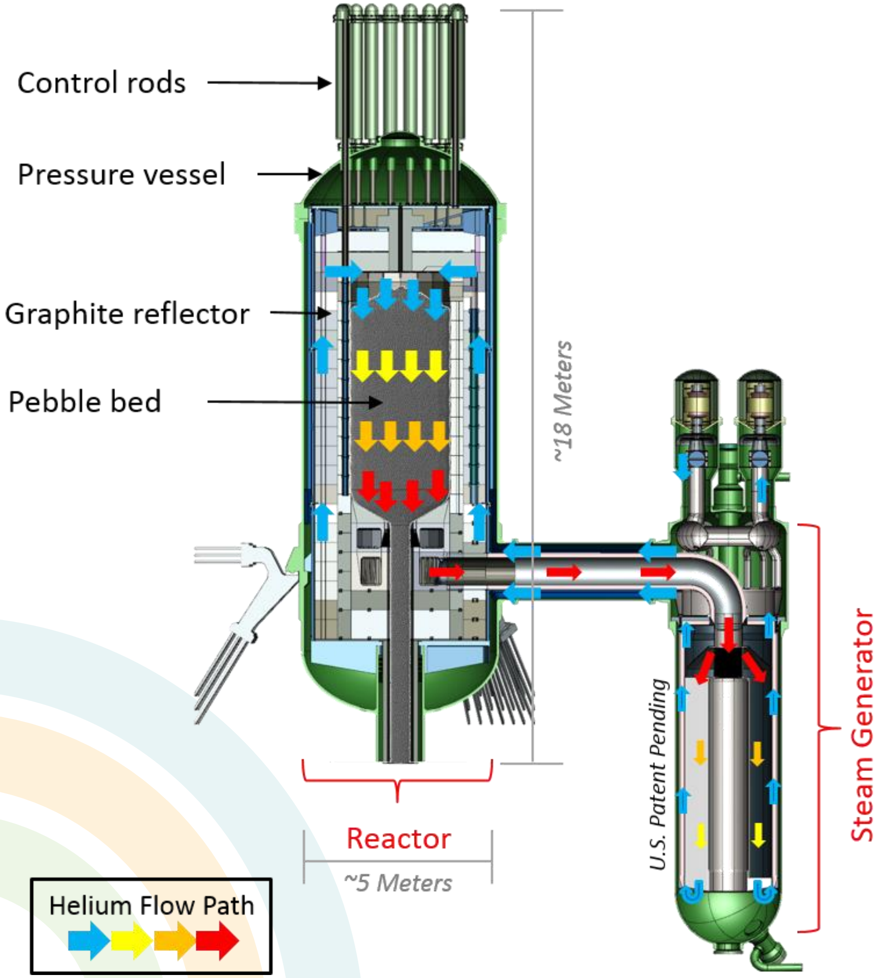
DCSA Model


Not associated with the facility
Z_{0A}
S_r
S_q
Z_{0B}
S_s
S_t
S_u
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_{4A}
S_a
Z_{3B}
S_c
S_d
Z_{2C}
S_j
Z_{1C}
S_m
S_n
S_p
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 HTGR documentation
2. Identify plant functions and their corresponding systems
3. Assign functions to security levels
4. Assign systems to basic security zones
5. Analyze basic zone dependencies
6. Assign cybersecurity controls to the DCSA design

HTGR Overview



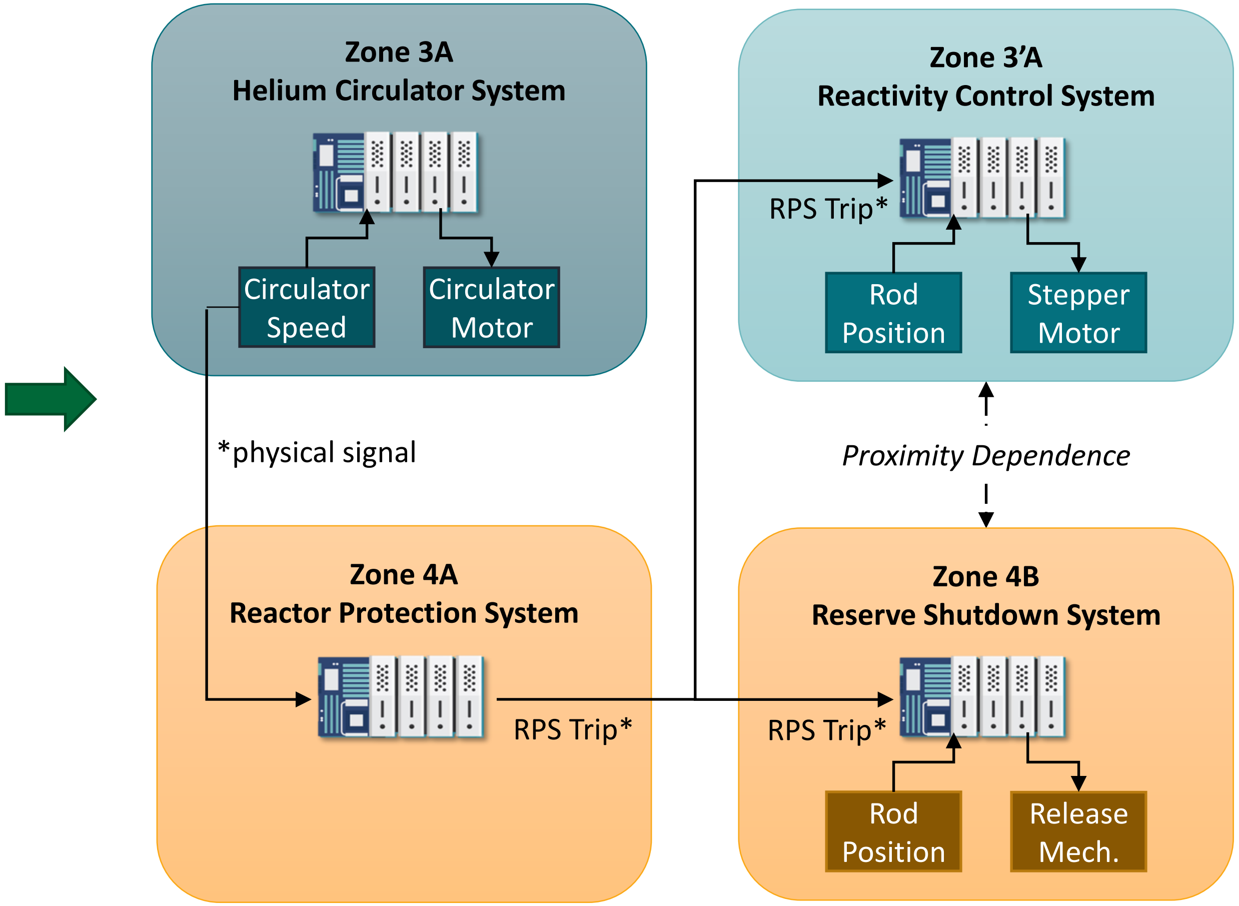
How do we protect facility functions to minimize the impact of an adversary who has gained access to plant systems?

Citation: K. Fehrenbacher, “Meet a Startup Making a New Kind of Safer, Smaller Nuclear Reactor.” *Image provided by X-energy,* 2016.

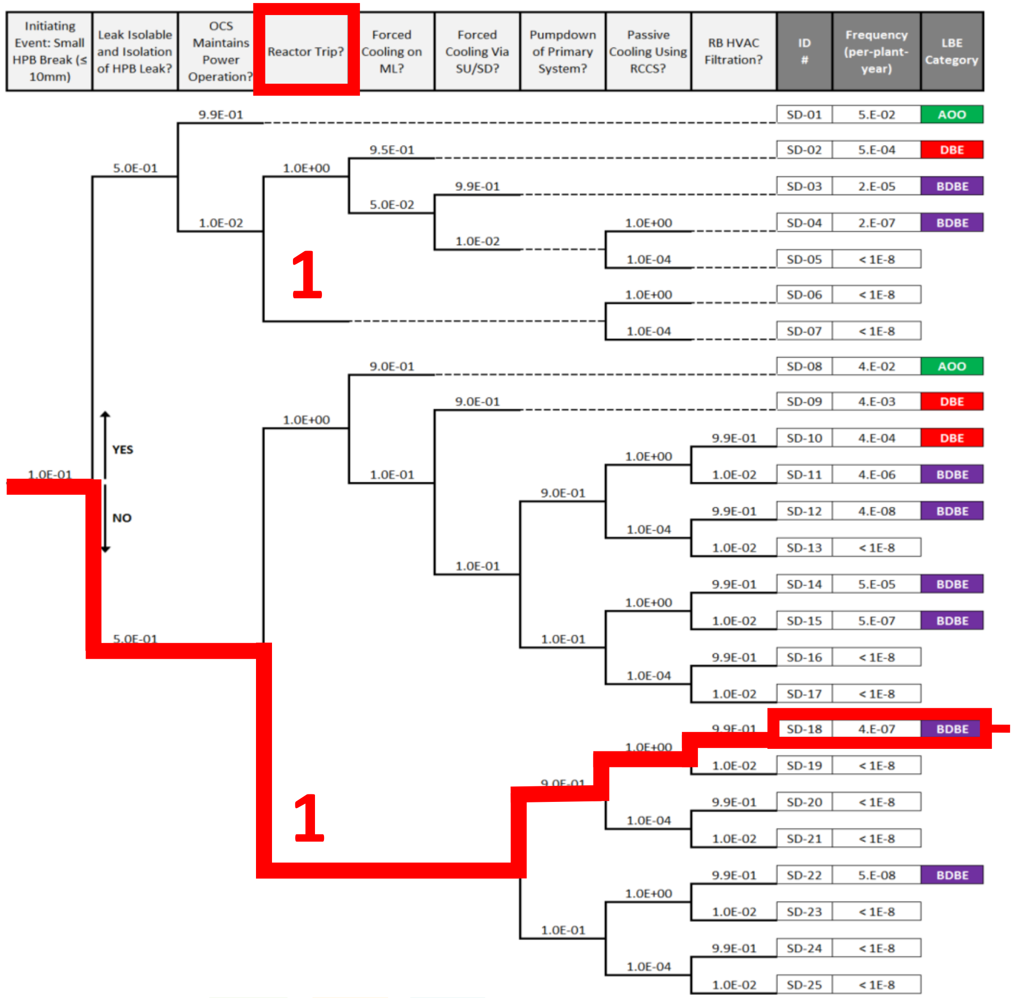
Ideal Defensive Cyber Security Architecture

Level 1	IT Systems			
Level 2	Data Historian	Maintenance	Work Control	
Level 3	Helium Circulator System	Fuel Handling System	Start-Up & Shutdown System	NI Feedwater System
Level 3’	Reactivity Control System	NI HVAC System	NI Steam System	Reactor Cavity Cooling System
Level 4	Reactor Protection System	Reserve Shutdown System	Helium Service System	

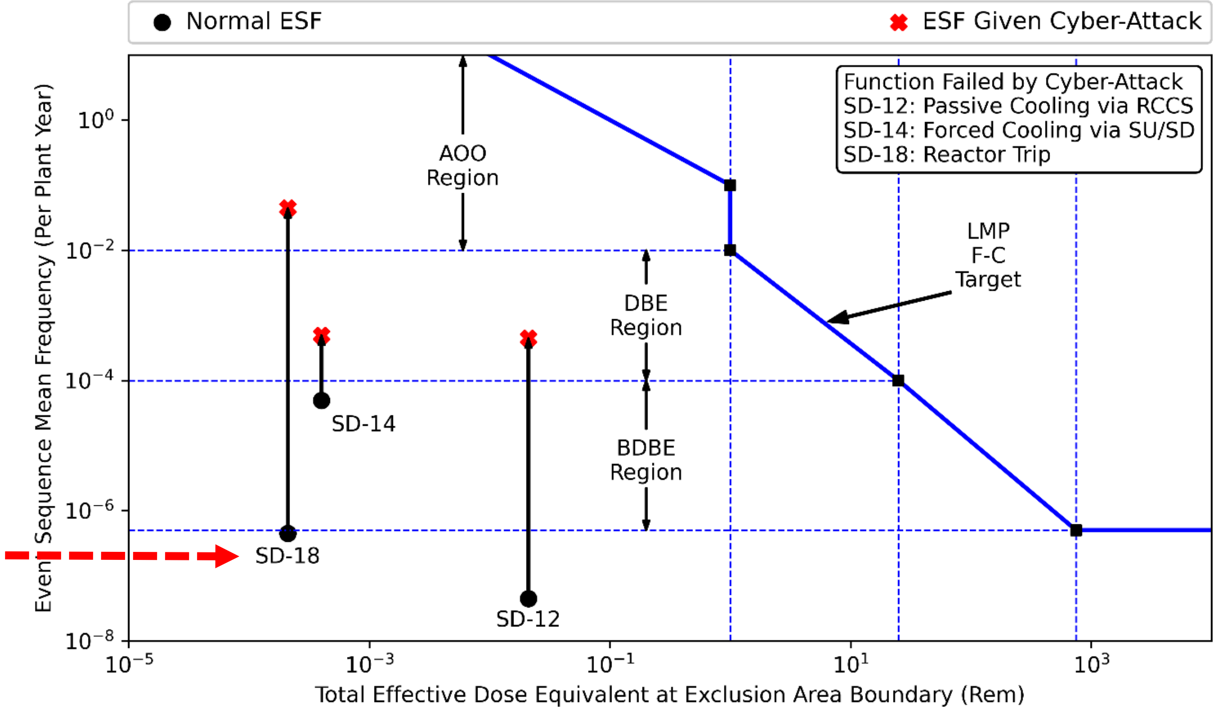
Example Basic Zone Detail



Event tree analysis informs DCSA zones



ID #	Frequency (per-plant-year)	LBE Category
SD-01	5.E-02	AOO
SD-02	5.E-04	DBE
SD-03	2.E-05	BDBE
SD-04	2.E-07	BDBE
SD-05	< 1E-8	
SD-06	< 1E-8	
SD-07	< 1E-8	
SD-08	4.E-02	AOO
SD-09	4.E-03	DBE
SD-10	4.E-04	DBE
SD-11	4.E-06	BDBE
SD-12	4.E-08	BDBE
SD-13	< 1E-8	
SD-14	5.E-05	BDBE
SD-15	5.E-07	BDBE
SD-16	< 1E-8	
SD-17	< 1E-8	
SD-18	4.E-07	BDBE
SD-19	< 1E-8	
SD-20	< 1E-8	
SD-21	< 1E-8	
SD-22	5.E-08	BDBE
SD-23	< 1E-8	
SD-24	< 1E-8	
SD-25	< 1E-8	



Citation: Southern Company, "High Temperature, Gas-Cooled Pebble Bed Reactor Licensing Modernization Project Demonstration." 2018.

Project Status

- Assigned functions to levels
- Wrote code to perform combinatorial analysis of compromising events and identify where design constraints are violated
- Dependency analysis in progress
- ANS Annual Conference paper:
  Demonstrates event tree design approach for DCSA
- On track for FY24 M2 report

Tasks to Conclude the FY

1. Complete automated event tree analysis code
2. Complete dependency analysis
3. Complete pathway analysis
4. Assign cybersecurity controls

Impact & Future Work

- Impact
  - Detailed demonstration of Tier 2 analysis for industry
  - Template of DCSA as starting point for HTGR designs
- Demonstrate another DCSA design approach for another class of advanced reactor
- Integration with other ARSS projects:
  - DCSA analysis scripts can feed ARCADE cyber-attack simulator
  - DCSA analysis scripts can inform blended cyber-physical attack simulation
  - Physical protection system DCSA

ADVANCED REACTOR SAFEGUARDS & SECURITY

Questions?

Team: Lee Maccarone, Mike Rowland, Bob Brulles