INL/MIS-25-86970-Revision-0

Internship Presentation: Integrating Safety and Cybersecurity: Security-by-Design with SOWT Analysis for Reactor Testing

August 2025

Jo'Onna Banks, Palash Kumar Bhowmik

Changing the World's Energy Future

Idaho National Laboratory

INL/MIS-25-86970-Revision-0

Internship Presentation: Integrating Safety and Cybersecurity: Security-by-Design with SOWT Analysis for Reactor Testing

Jo'Onna Banks, Palash Kumar Bhowmik

August 2025

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

August 4, 2025
INL/MIS-25-86970

Integrating Safety and Cybersecurity: Security-by-Design with SOWT Analysis for Reactor Testing

Jo'Onna Banks (CONCISE Intern), Palash Kumar Bhowmik (Mentor, C130)

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

Content

- Project objective, motivation, problem statement and scope
- Overview of the reactor system: safety and security (only focusing cybersecurity)
- Supporting Organizations and R&D
  - NNSA, Sandia, INL, and others
- Supporting R&Ds and testing facilities
  - R&D related to simulating specific cyber-attack scenarios using reactor simulator
  - Reactor system demonstration facilities at DOE INL site
- SOWT analysis
  - for repurposing reactor testing facilities to cyber security testbeds
- Recommendation and conclusion

Objective

- Leveraging reactor testing facilities that are mostly designed focusing safety to cybersecurity testing
  - Incorporate reactor security-by-design with reactor safety-by-design principles
  - Defense-in-depth principles:
    - Safety focused
    - Security focused
- Evaluating cyber tools, models, and solutions that are applicable
- Simulating specific cyber-attack scenarios using reactor simulator
- Performing strengths, weakness, opportunities and threats (SOWT) analysis

Motivation

- Core role in energy infrastructure
  - Enable safe, controlled nuclear fission for stable electricity generation
  - Support national energy security by reducing reliance on fossil fuels

- Critical need for cyber protection
  - Cyber compromises can lead to accidents or radioactive material release
    - Threats endanger public safety, environmental health, and system reliability
    - Damage to industry reputation can impact stakeholder trust and future investment
  - Reactor systems are critical infrastructure tied to national security

- Economic implications of cyber attacks
  - Operational downtime causes major financial losses
    - Infrastructure repairs or replacements can cost millions
  - Legal liabilities, fines, and IP theft increase financial risk
    - Investor and stockholder confidence may be significantly reduced

Problem Statement

- The increasing frequency and sophistication of cyber threats targeting nuclear facilities pose significant risks to the safety and reliability of reactor systems.
  - However, current protective measures may be inadequate, necessitating a comprehensive review of existing cybersecurity practices and strategies so that the necessary actions can be taken to reinforce security at both operational technology (OT) and information technology (IT) levels.
    - Failure to address these vulnerabilities could compromise public safety, national security, and the integrity of the nuclear energy sector.

Scope

- This report analyzes the cybersecurity needs of reactor system facilities, focusing on test environments, cyber tools, and simulation technologies.
  - It addresses rising cyber threats to nuclear infrastructure and highlights the role of facilities like
    - The U.S. DOE advanced Reactor Demonstration Project (ADRP)
    - Demonstration of Microreactor Experiments (DOME)
    - Laboratory for Operation and Testing in the U.S. (LOTUS)
    - INL's Operation Technology Cybersecurity R&D

- The report explores tools for OT/IT protection, use of simulators for cyber-attack testing, and includes a SWOT analysis to assess current posture.
  - It emphasizes integrating cybersecurity from design through operation to meet regulatory standards and ensure system resilience.

Overview of the Reactor System: Safety and Security

(only focusing cybersecurity)

Reactor System: Security-by-Design

First Principle: Shift Responsibility to the Most Capable Stakeholders

- Transfer security responsibility from less capable entities (e.g., customers, government) to major tech manufacturers
- Manufacturers must be accountable for all security outcomes related to their products
- Routinely adapt and update products to address emerging threats

Second Principle: Lead with Transparency and Accountability

- Share insights from product deployments and discovered vulnerabilities
- Publish relevant statistics, such as the percentage of users on the latest version
- Release detailed vulnerability advisories and CVE records
- Enable other manufacturers to learn from shared data and avoid common pitfalls

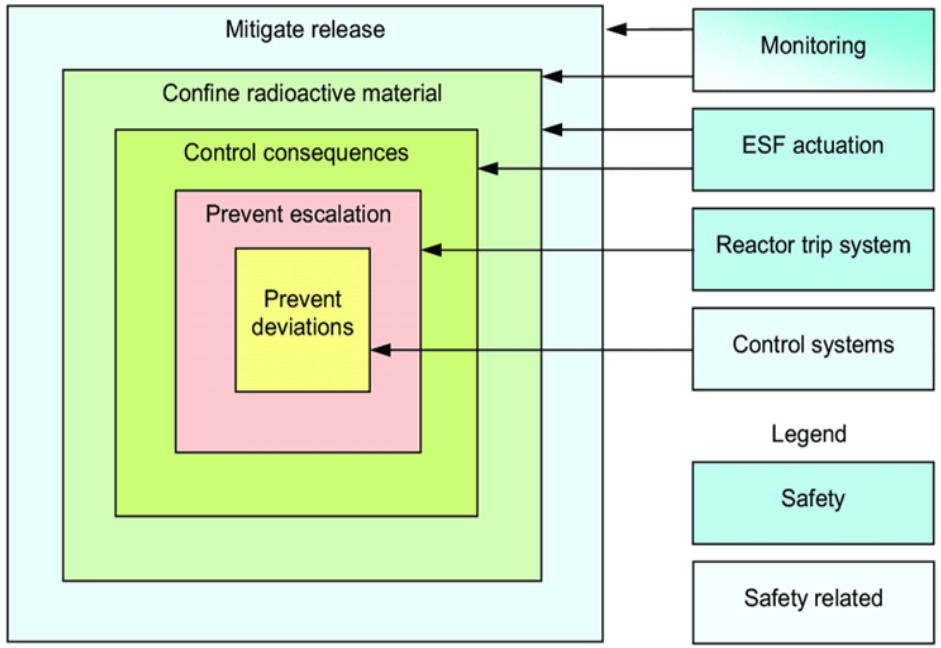
Third Principle: Secure Executive-Level Commitment

- Treat security as a business priority, not just an IT concern
- Allocate resources to embed security in early design and development
- Create internal incentives to support secure software practices
- Promote a security-first culture and maintain open communication channels for feedback

Source: https://energy.sandia.gov/programs/nuclear-energy/safety-security-and-safeguards-for-advanced-nuclear-power/

Reactor System: Defense-in-Depth

- Defense-in-depth is a cybersecurity strategy that layers multiple tools, controls, and policies to prevent single points of failure.
  - Rather than targeting specific threats, it builds a multi-layered defense to ensure system resilience.
- Implementing defense-in-depth involves layering security measures like
  - Network segmentation, access controls, and monitoring to reduce risk and protect I&C systems from evolving cyber threats.



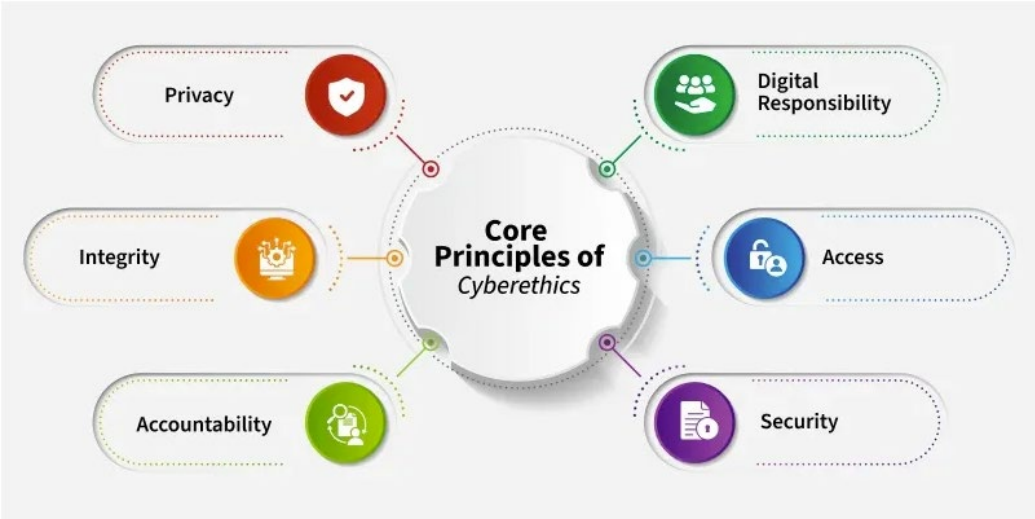
Source: https://energy.sandia.gov/programs/nuclear-energy/safety-security-and-safeguards-for-advanced-nuclear-power/

Reactor System: Cyber Tools, Methods, and Solutions

- **Cybersecurity Evaluation Tool (CSET)**
  - Provides structured cybersecurity assessments
  - Aligns with industry standards and regulatory frameworks
  - Tailored for IT and OT systems in nuclear facilities

- **Industrial Protocol Simulators**
  - Test OT communication protocols like Modbus, DNP3, OPC UA
  - Include fuzzing to inject malformed data and detect vulnerabilities
  - Help assess system resilience against protocol-specific threats

- **Hybrid Cybersecurity Integration Tools**
  - Combine traditional IT tools (firewalls, IDS) with OT requirements
  - Enable deployment within hybrid testbeds
  - Address unique challenges of deterministic, safety-critical systems



Source: https://www.geeksforgeeks.org/computer-networks/what-is-cyberethics/

- **AI and Digital Twin Technology**
  - AI and cyber ethics has similar core principles.
  - Ensure safe, secure, and efficient integration of AI/ML in nuclear power plants by identifying cyber vulnerabilities, developing secure integration guidelines, and creating validation standards for AI/ML models.
  - Establish a continuous monitoring framework to address emerging cyber threats and maintain regulatory compliance, facilitating the adoption of AI/ML technologies in reactor operations while minimizing risks and ensuring safety and reliability.

Reactor System: Cyber Tools, Methods, and Solutions (cont.)

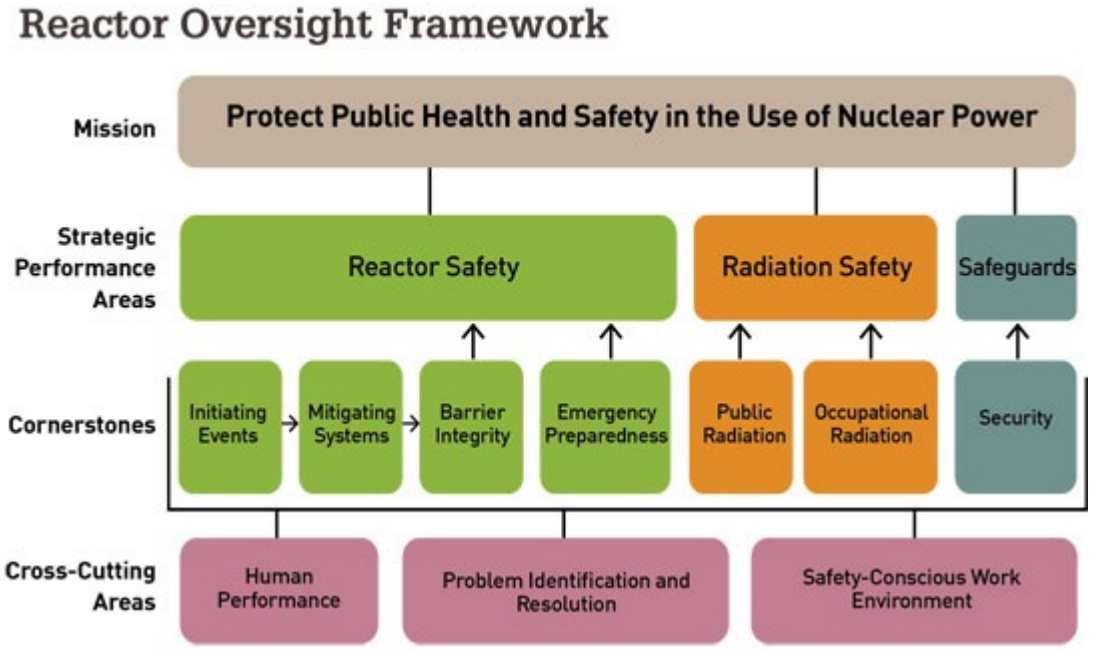
- **Simulation Limitations**
  - Simulations often fail to reflect real-world conditions, limiting the applicability of gathered data to operational scenarios.
  - Unrealistic scenarios and insufficient participant training contribute to confusion and reduce simulation effectiveness.
  - Many simulators have limited capabilities, reinforcing concerns about lack of realism and comprehensive coverage.

- **Facility Infrastructure Challenges**
  - Effective simulation and testing require robust, adaptable infrastructure.
  - Outdated or inflexible facilities hinder the ability to model diverse scenarios and evolving threat landscapes.

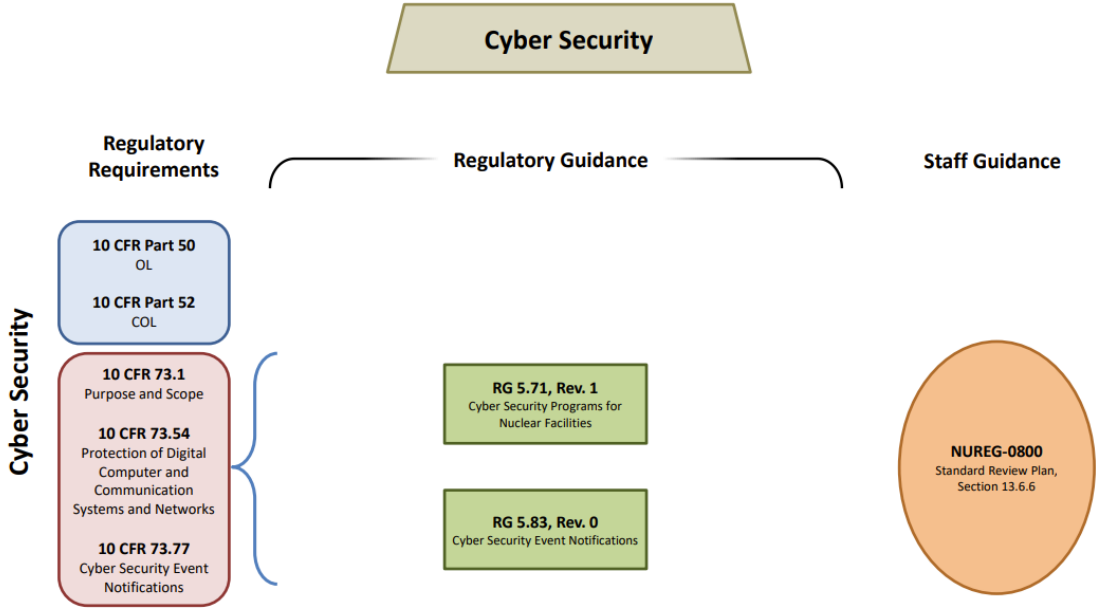
- **Tool and Methodology Gaps**
  - While current tools are useful, there is a need for additional and more advanced resources.
  - Physical security measures are underdeveloped, increasing vulnerability.
  - Many tools lack Security-by-Design (SbD) principles, leading to long-term reliability and integration issues.

Reactor System: Safet-to-Cybersecurity Regulation

- The United States Nuclear Regulatory Commission (U.S. NRC) develops and enforces regulations to ensure the cybersecurity of nuclear power plants and other nuclear facilities
  - conduct regular audits, inspections, and provide guidance to licensees on implementing effective cybersecurity programs.



Source: https://www.nrc.gov/reactors/operating/oversight/rop-description/cornerstone.html



Cyber Security requirements and guidance

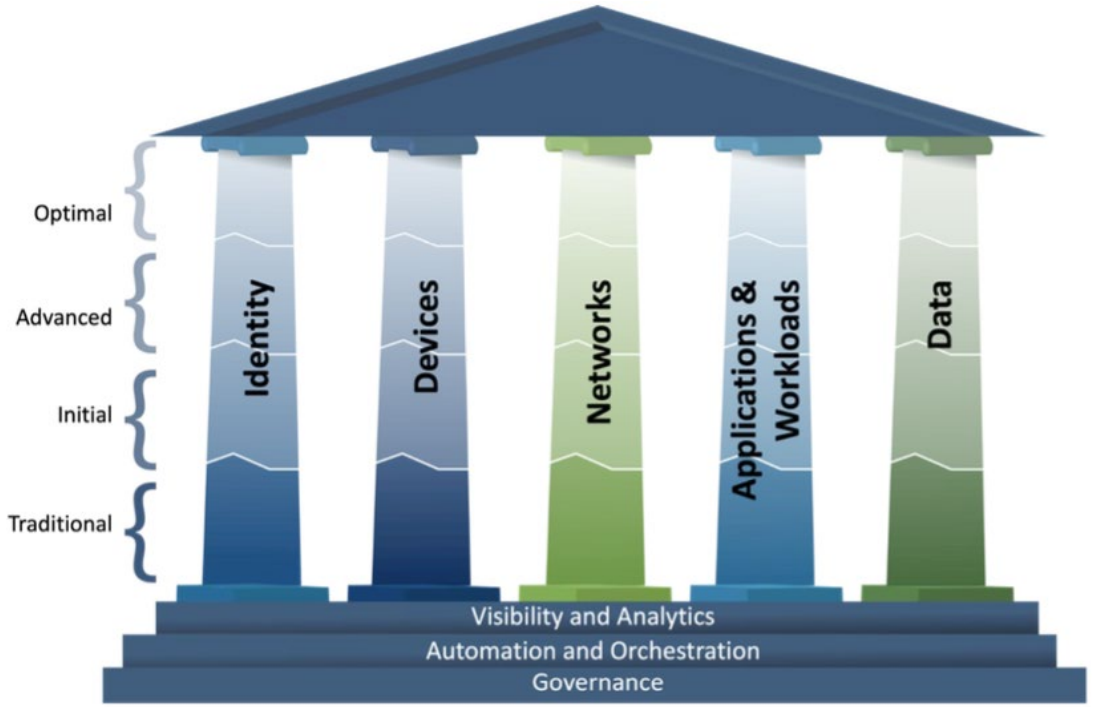
Source: https://www.nrc.gov/docs/ML2332/ML23326A045.pdf

Supporting Organizations and R&D

(for reactor system safety and cybersecurity)

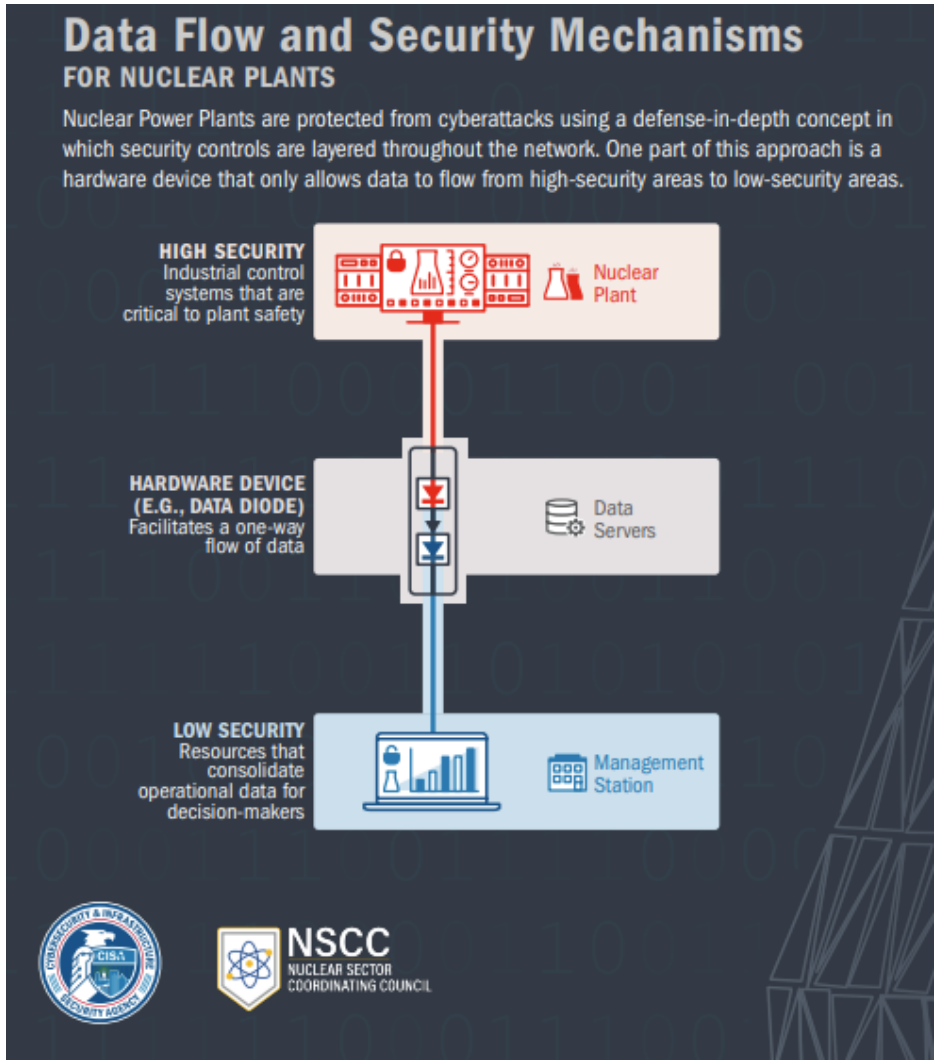
Cybersecurity and Infrastructure Security Agency (CISA)

- Supports research and development of nuclear reactor technology safety and security
  - through funding and collaboration with national laboratories, academia, and industry.



CISA's Zero Trust Model.

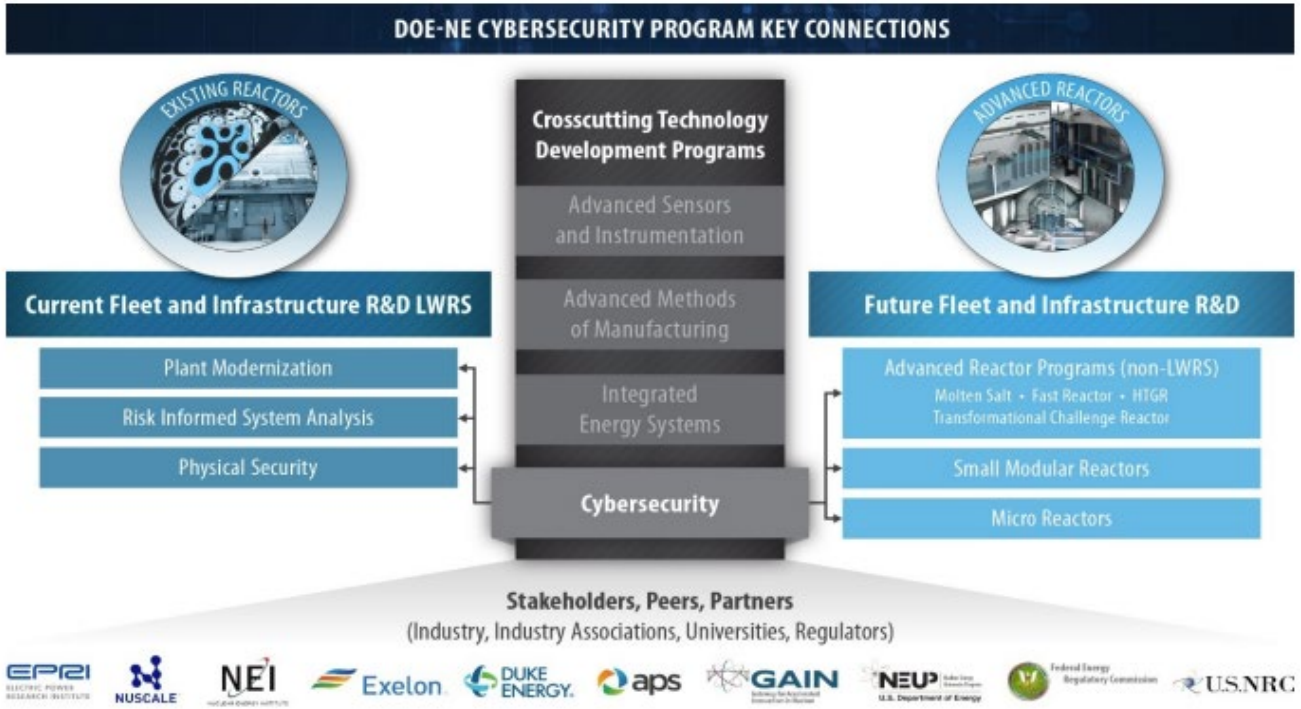
Source: https://www.sternsecurity.com/blog/category/cybersecurity-frameworks/



Source: https://www.cisa.gov/sites/default/files/publications/Nuclear%2520Sector%2520Cybersecurity%2520Infographic%25204.13.21_508c.pdf

Department of Energy (DOE)

- Supports research and development of nuclear reactor technology safety and security
  - through funding and collaboration with national laboratories, academia, and industry.



Cybersecurity RD&D Program crosscut connections.

Source: https://www.osti.gov/servlets/purl/1821961

Advanced Reactor Types

The Department of Energy Office of Nuclear Energy (NE) and its national laboratories support research and development on a wide range of new advanced reactor technologies to help meet the nation's energy, environmental, and national security needs.

Advanced Reactor Features

Walk-Away Safety
Requires no or minimal operator intervention to remain safe in the event of an accident.

Versatility
Can provide heat energy for industrial processes, water desalination, and load-following to support intermittent power sources.

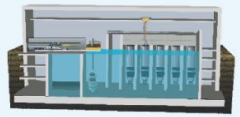
Waste Re-use and Disposal
Can greatly reduce the amount of spent fuel requiring disposal, and some technologies can re-use spent fuel.

Financeability
Can employ factory manufacturing and be made with less capital cost.

Advanced Reactor Sizes

Microreactors
Range: 1 MW to 20 MW
Can fit on a flatbed truck, and are mobile and deployable.

Small Modular Reactors
Range: 20 MW to 300 MW
Can be scaled up or down by adding more units.



Full-Size Reactors Range:
300 MW to 1,000+MW
Can provide reliable, emissions-free baseload power.

MW refers to one million watts of electricity.

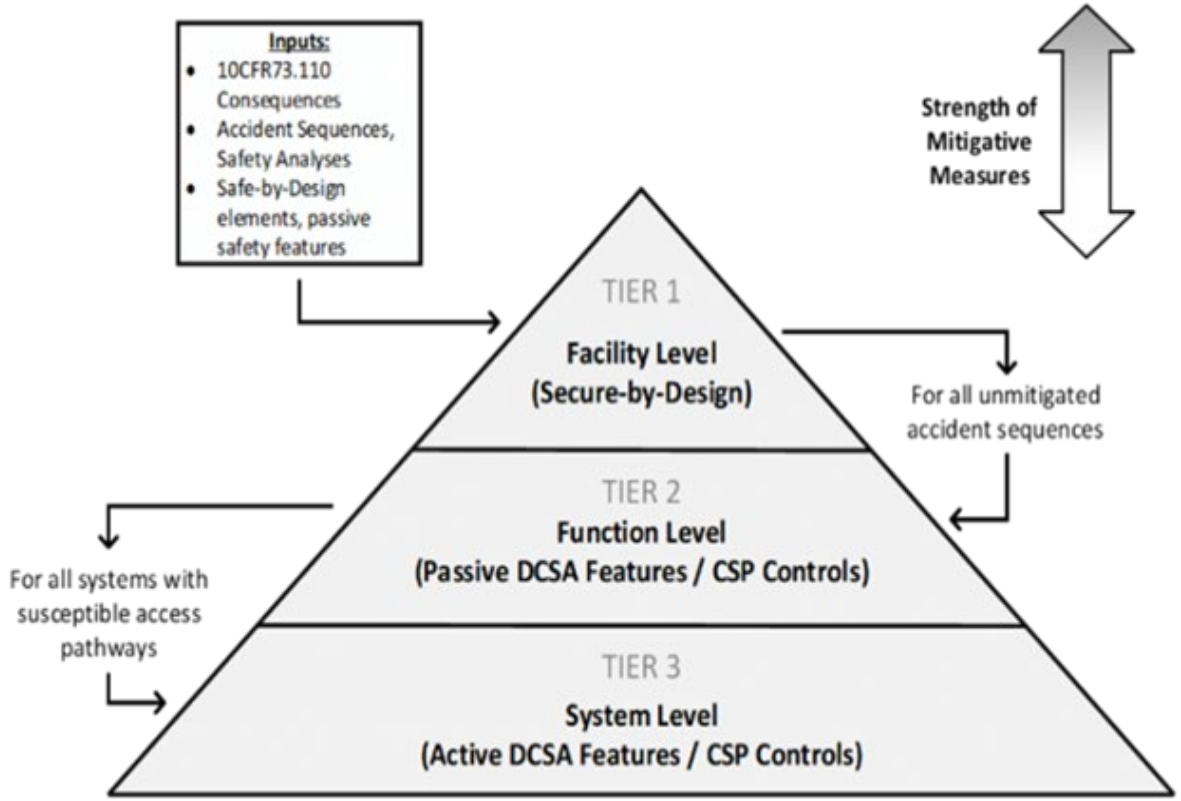
Source: https://www.energy.gov/sites/default/files/2020/05/f74/Advanced-Reactor-Types_Fact-Sheet_Draft_Hi-Res_R1.pdf

National Nuclear Security Administration (NNSA)

- Established by Congress in 2000, NNSA is a semi-autonomous agency within the U.S. DOE that protects by designing and delivering a safe, secure, reliable, and effective U.S. nuclear stockpile.

SANDIA National Laboratories

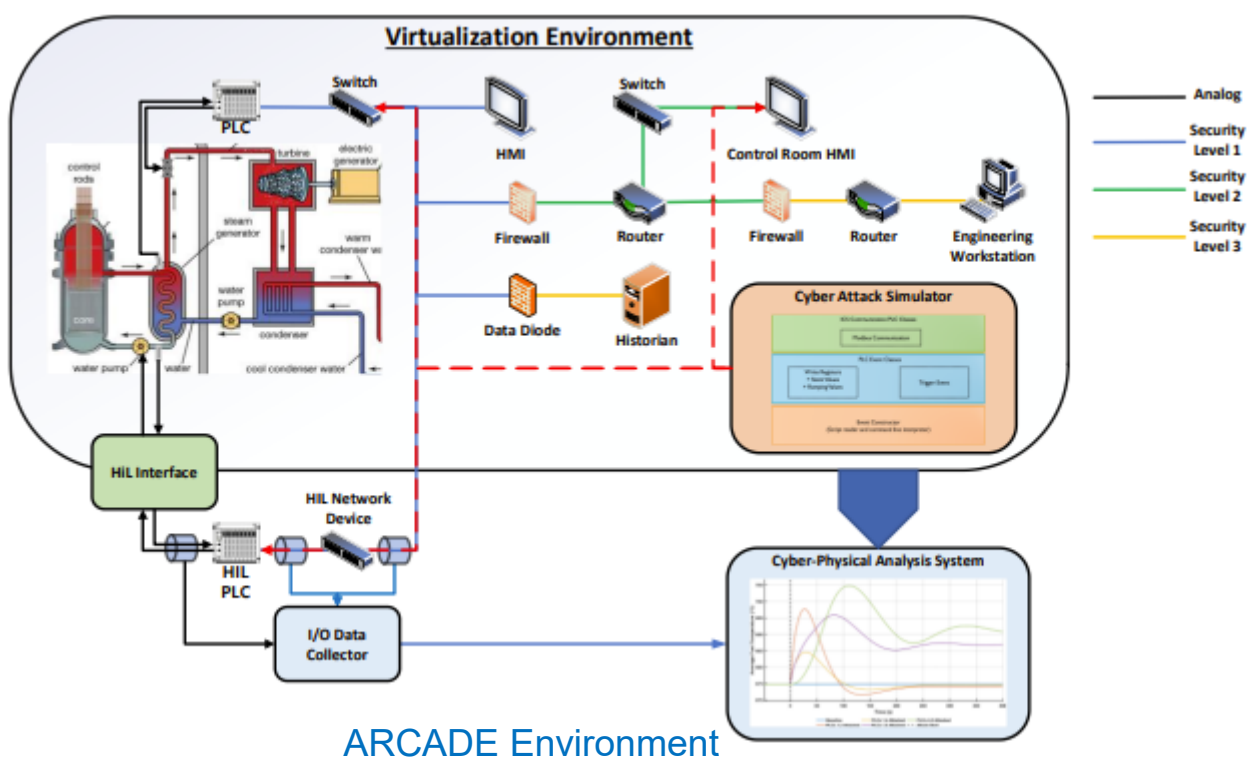
- Focuses on the development of advanced cybersecurity solutions for critical infrastructure, including nuclear reactors.
  - They work on threat analysis, secure system design, and advanced cybersecurity technologies to protect reactor systems.
    - anomaly detection
    - machine learning
- Developing advanced reactor safeguards and security (ARSS) program



Source: https://energy.sandia.gov/programs/nuclear-energy/nuclear-energy-security/nuclear-energy-cybersecurity-by-design/

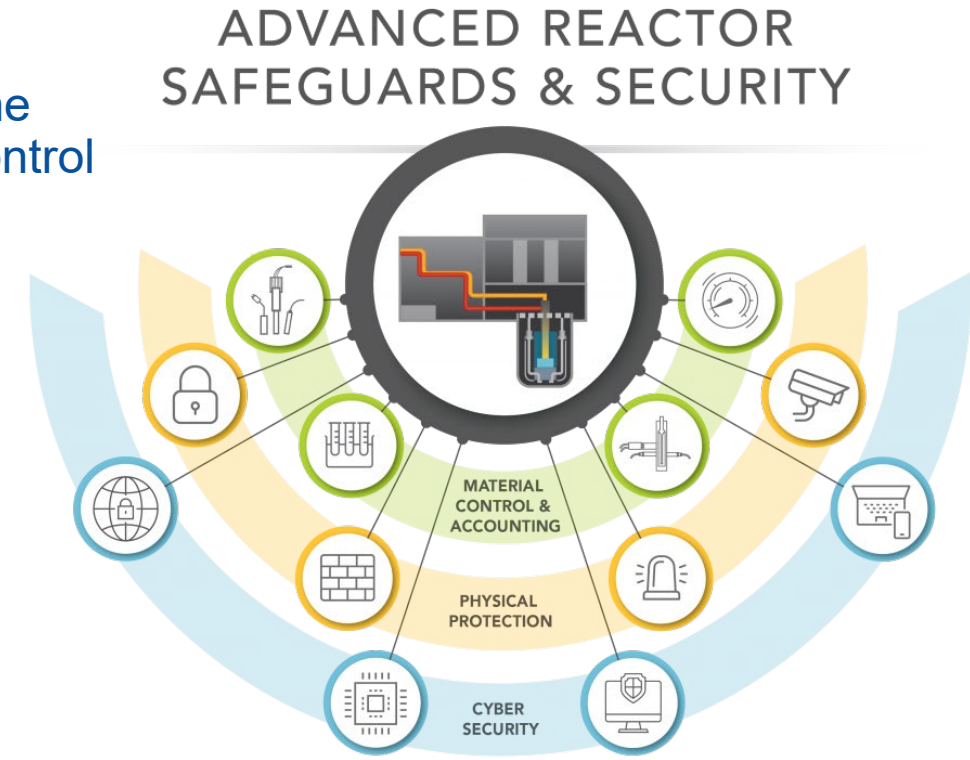
SANDIA National Laboratories (cont'd)

- Advanced reactor safeguards and security (ARSS) program
  - Developing Advanced Reactor Cyber Analysis and Development Environment (ARCADE)
    - Analysis performed with ARCADE is used to assess the consequence and inform the risk of cyber-attack on control system functions and network architectures.



ARCADE Environment

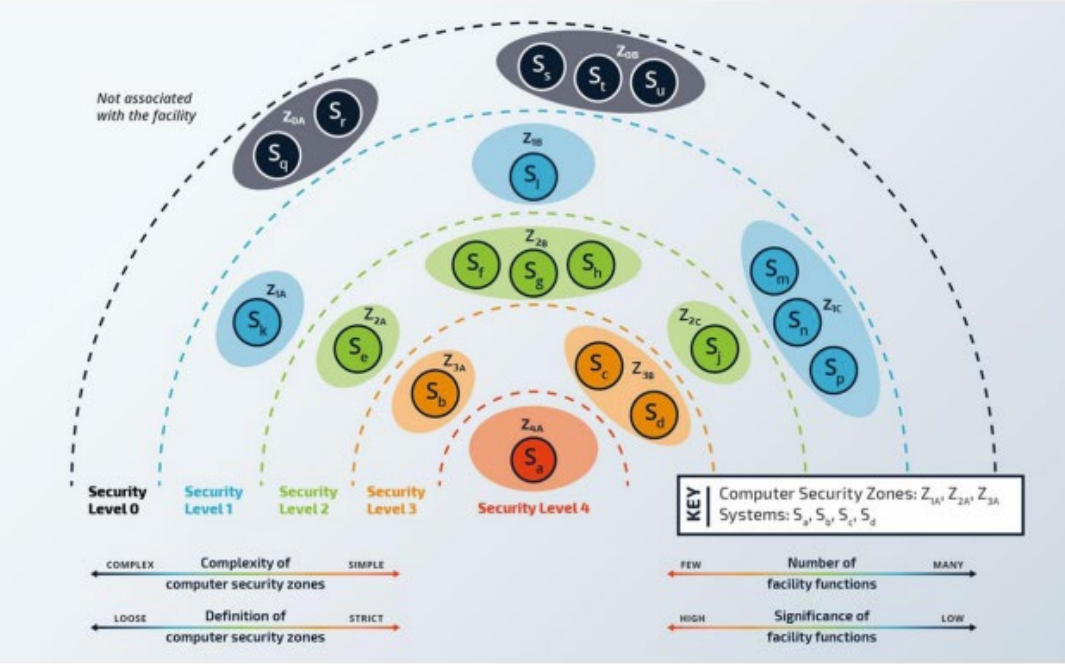
Source: https://www.sandia.gov/app/uploads/sites/273/2024/08/ARSS-Roadmap-SAND2024_FINAL.pdf



Source: https://energy.sandia.gov/programs/nuclear-energy/safety-security-and-safeguards-for-advanced-nuclear-power/advanced-reactor-safeguards-and-security/

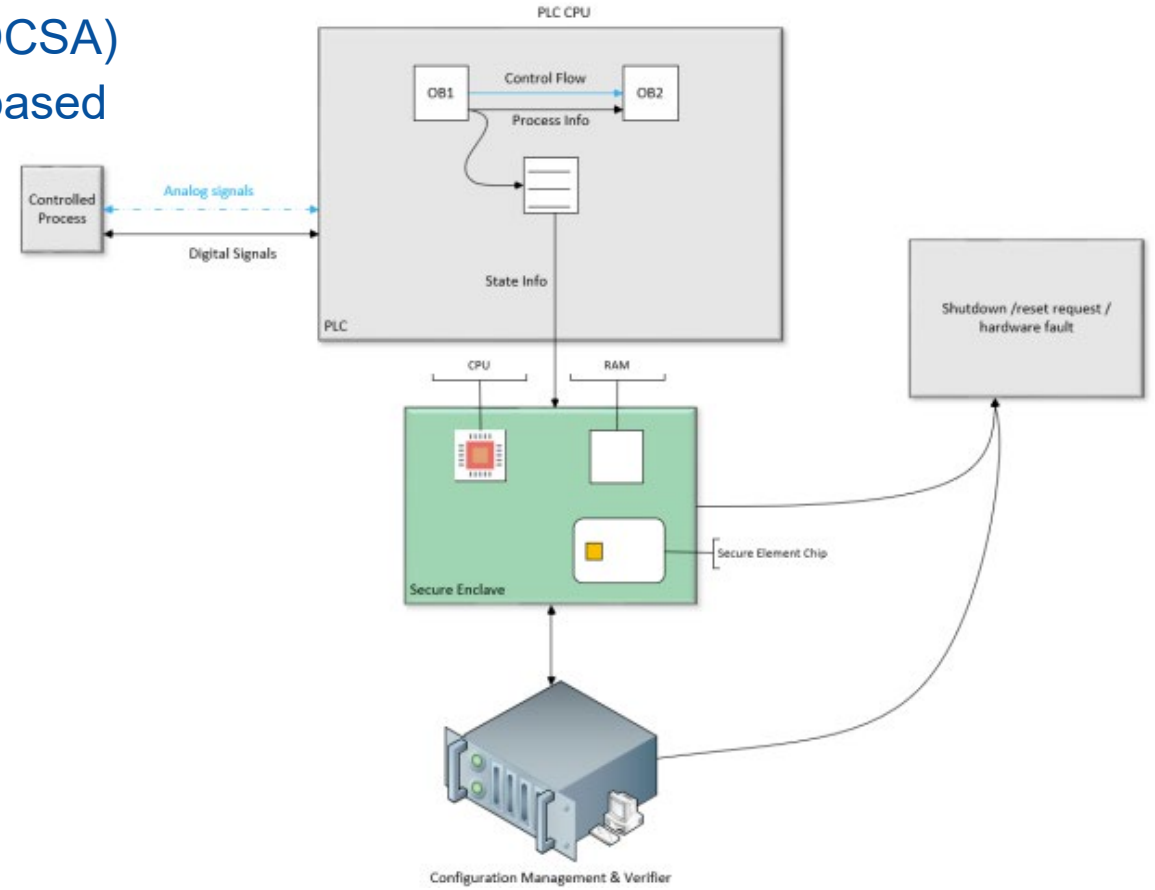
SANDIA National Laboratories (cont'd)

- ARSS program
  - Developing defensive cyber security architecture (DCSA)
    - a method of architecting a system of systems based on the functions executed by each system.



DCSA Model

Source: https://www.sandia.gov/app/uploads/sites/273/2024/08/ARSS-Roadmap-SAND2024_FINAL.pdf



Source: https://www.sandia.gov/app/uploads/sites/273/2024/08/ARSS-Roadmap-SAND2024_FINAL.pdf

National Reactor Innovation Center (NRIC)

- Facilitates the testing and demonstration of advanced reactor technologies, including cybersecurity measures.
  - They provide platforms for evaluating the resilience and security of new reactor designs against cyber threats.

Source: https://nric.inl.gov/partnerships/

Idaho National Laboratory (INL)

- A leader in nuclear cybersecurity research: they develop advanced cybersecurity technologies and methodologies for protecting nuclear reactors.
  - INL conducts vulnerability assessments, risk analyses, and collaborates with other organizations to enhance the cybersecurity posture of nuclear facilities.

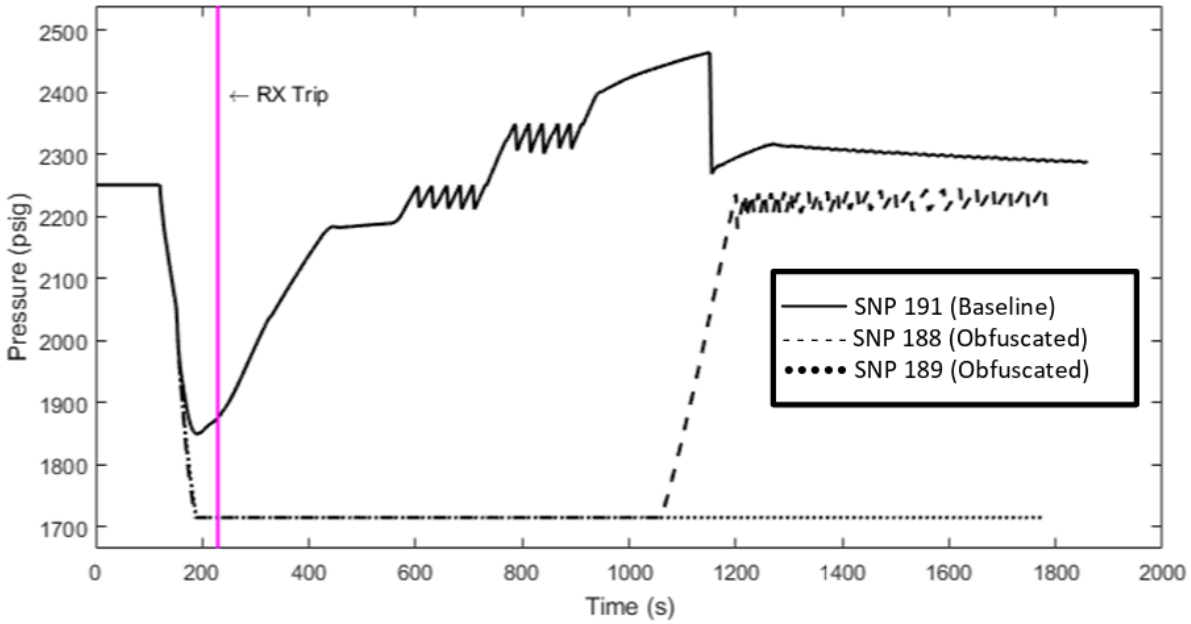
Source:https://gain.inl.gov/resources/nuclear-security-and-safeguards/nuclear-security/

Supporting R&Ds and Testing Facilities

(for reactor system safety and cybersecurity)

SANDIA - Enhancing Power Plant Safety through Coupling Plant Simulators to Cyber Digital Architecture

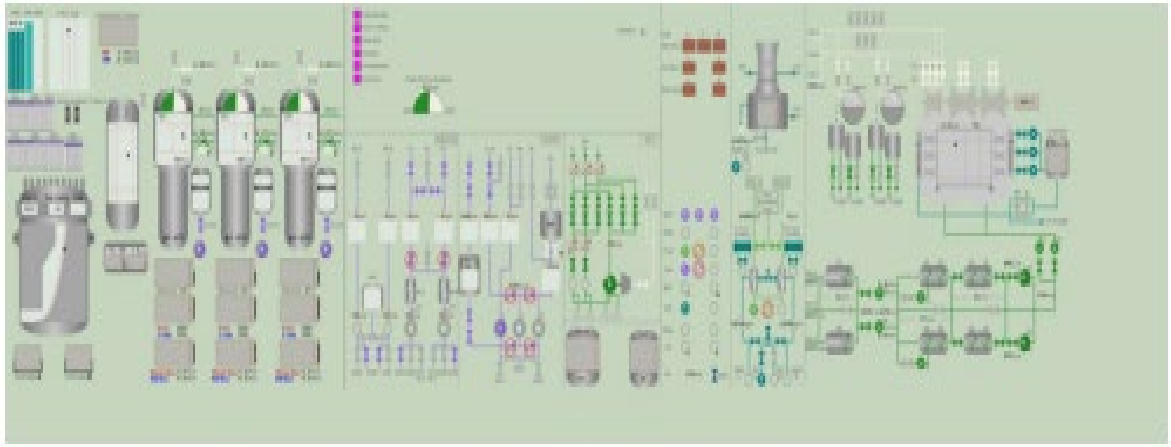
- The report examines how cyber events affect operator response and perception in nuclear power plants as they shift from analog to digital systems. Using a Pressurized Water Reactor simulator, operators responded to scenarios involving normal faults, cyber-attacks, and system malfunctions.
- **Key Findings:**
  - Delays in identifying cyber threats
  - Difficulty following procedures under stress
  - Existing safety controls proved essential
- **Challenges Identified:**
  - Limited operator training
  - Unrealistic or non-localized alarm systems
  - Unfamiliar simulation environments
- **Recommendations:**
  - Develop more realistic simulation scenarios
  - Use larger operator teams and extend training duration
  - Incorporate advanced methods like eye tracking to improve accuracy and safety evaluation



Source: https://www.osti.gov/servlets/purl/1484584

INL- Develop and Document an Advanced Human System Interface with Reactor Simulator

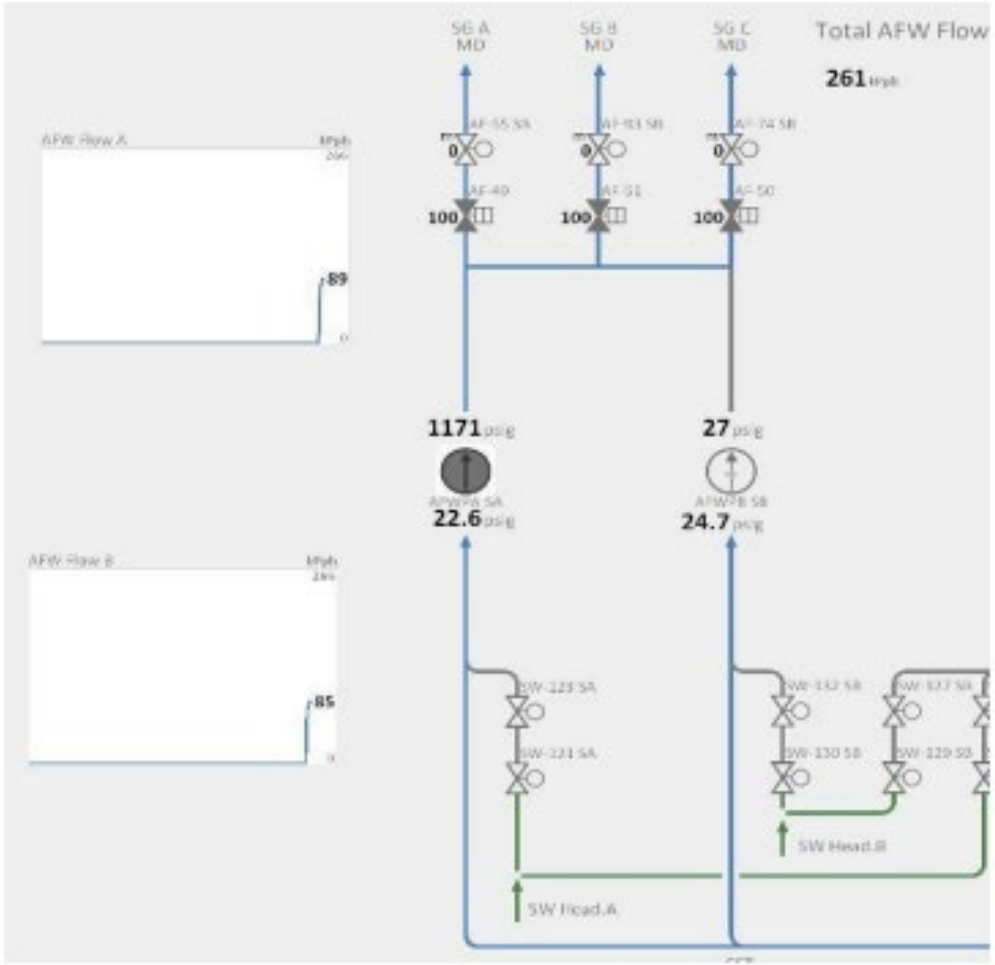
- The report outlines the development and examination of four digital Operator Work Displays (OWDs) recently implemented for the Generic Pressurized Water Reactor (gPWR) simulator at INL. The redesigned displays, chosen include: Charging and Volume Control System (CVCS), Reactor Control (Rx Ctrl), Auxiliary Feed Water (AFW), and Steam Generator (SGN).
- **Goals:**
  - Designed to improve operator interaction with complex systems
  - Enhance usability, especially during emergency scenarios
  - Reduce visual clutter on displays
  - Enable safer and more effective operator interactions



Source: https://www.osti.gov/biblio/1567688

Idaho National Laboratory - Develop and Document an Advanced Human System Interface for the Generic Pressurized Water Reactor Simulator

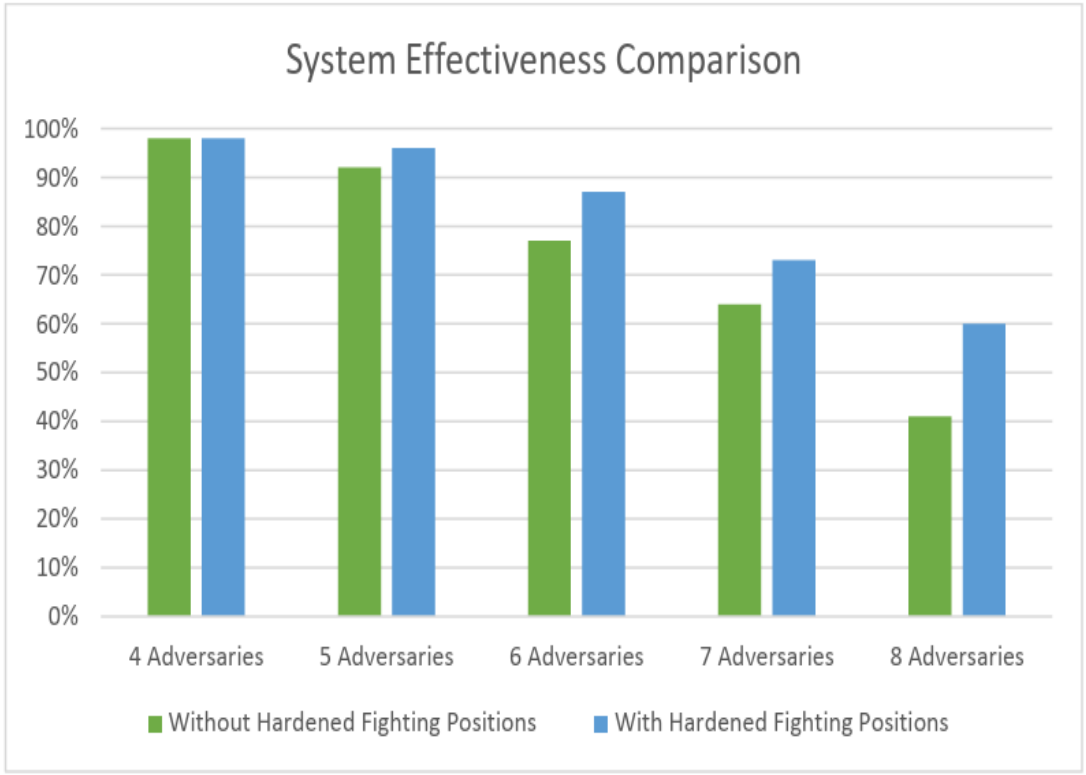
- After being tested in IFE's HAMMLAB and INL's Human System Simulation Lab (HSSL):
- **Results**
  - No negative impact on system functionality
  - Often improved usability
- **Improvements Based on Feedback**
  - Enhanced flow direction indicators
  - Added flow totalizers
- **Final Evaluation by U.S. Nuclear Plant Staff**
  - Provided a balanced view between overview and detailed screens
  - Enabled faster operator response and better decision-making



Source: https://www.osti.gov/biblio/1567688

SANDIA - U.S. Domestic Small Modular Reactor Physical Protection System Analysis (SAND2021-0768)

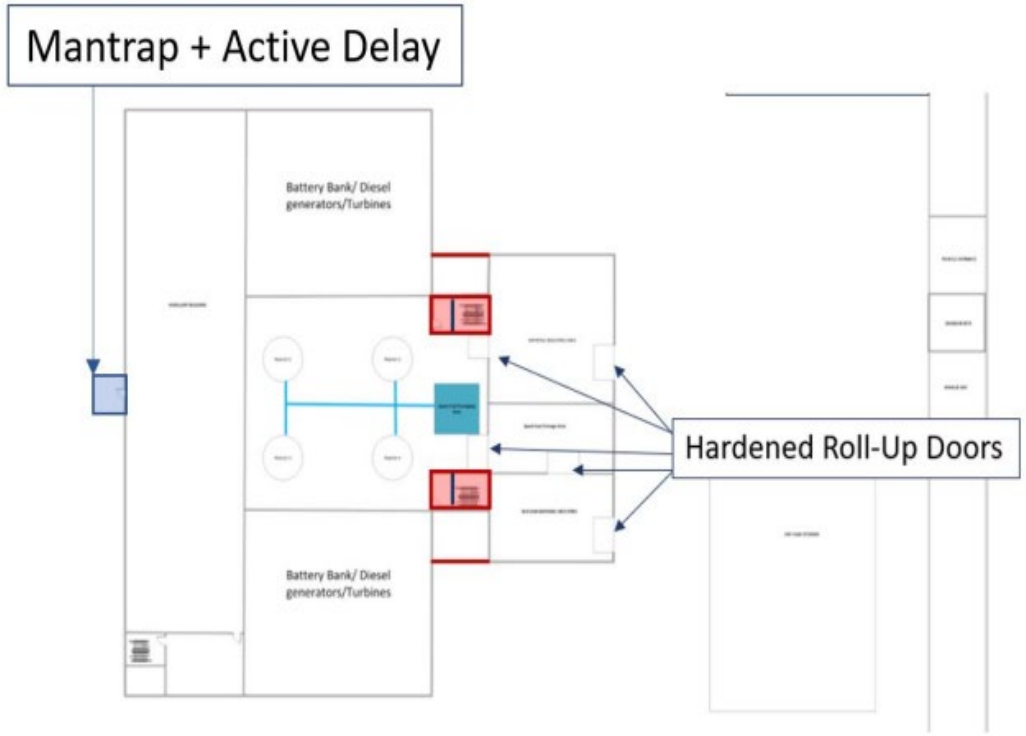
- This report investigates the integration of physical security into the design phase of U.S. Small Modular Reactors (SMRs). A hypothetical site near Portland, Oregon, featuring four light-water reactors and a shared spent fuel pool, was analyzed. Redundant power systems included below-grade battery/diesel generators and rooftop backups, with 48-hour passive cooling via Passive Safety Injection Tanks (PSITs). Simulated attacks targeted reactor cores, the spent fuel pool, battery banks/diesel generator rooms, and PSITs, using tools like Blended, Scribe3D, and PathTrace. Attack scenarios included sequential and split attacks by adversaries with insider knowledge.



Source:
https://www.sandia.gov/app/uploads/sites/273/2022/07/US_DomesticSmallModularReactorPhysicalProtectionSystemAnalysisSAND2021-0768_REV-4.pdf

SANDIA - U.S. Domestic Small Modular Reactor Physical Protection System Analysis (SAND2021-0768)

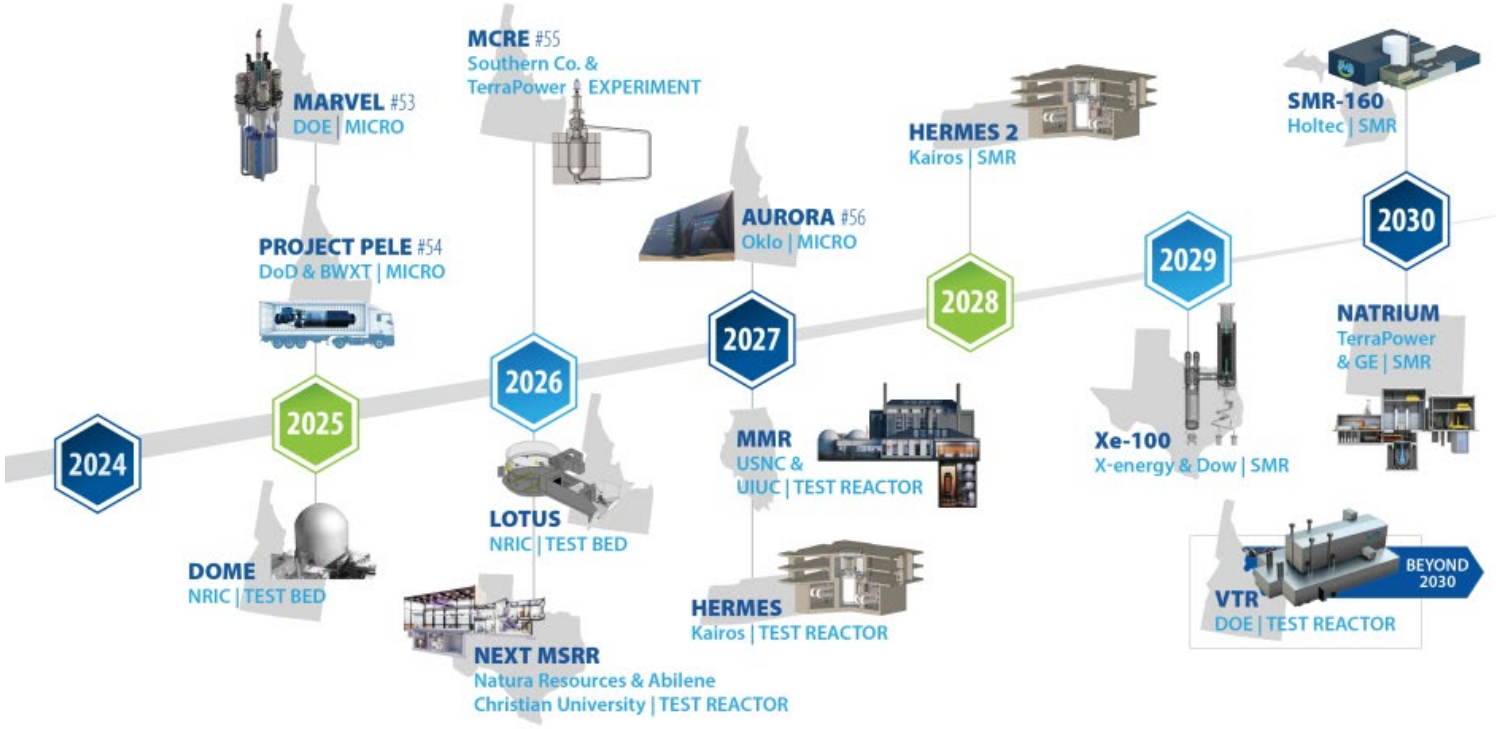
- **Findings:**
  - <95% Probability of Interruption (PI) for all targets with standard PPS and 30-minute offsite response, indicating significant vulnerability
- **Best-case scenarios:**
  - 78% success rate in denying sabotage (sequential attacks)
  - 95% success rate in denying sabotage (split attacks)
- Hardening manned positions greatly improved system effectiveness
- **Suggested Upgrades:**
  - Installation of mantraps and additional structural walls
  - Fused radar/video detection systems
  - Internal barriers and active delay features
- **Strategic Insights:**
  - Emphasize integrating security in the design phase rather than retrofitting
  - Combine physical delay measures with active detection systems for optimal protection
  - Effective offsite response depends on training and coordination with local law enforcement



Source:
https://www.sandia.gov/app/uploads/sites/273/2022/07/US_DomesticSmallModularReactorPhysicalProtectionSystemAnalysisSAND2021-0768_REV-4.pdf

Reactor Testing and Demonstration at DOE INL Site

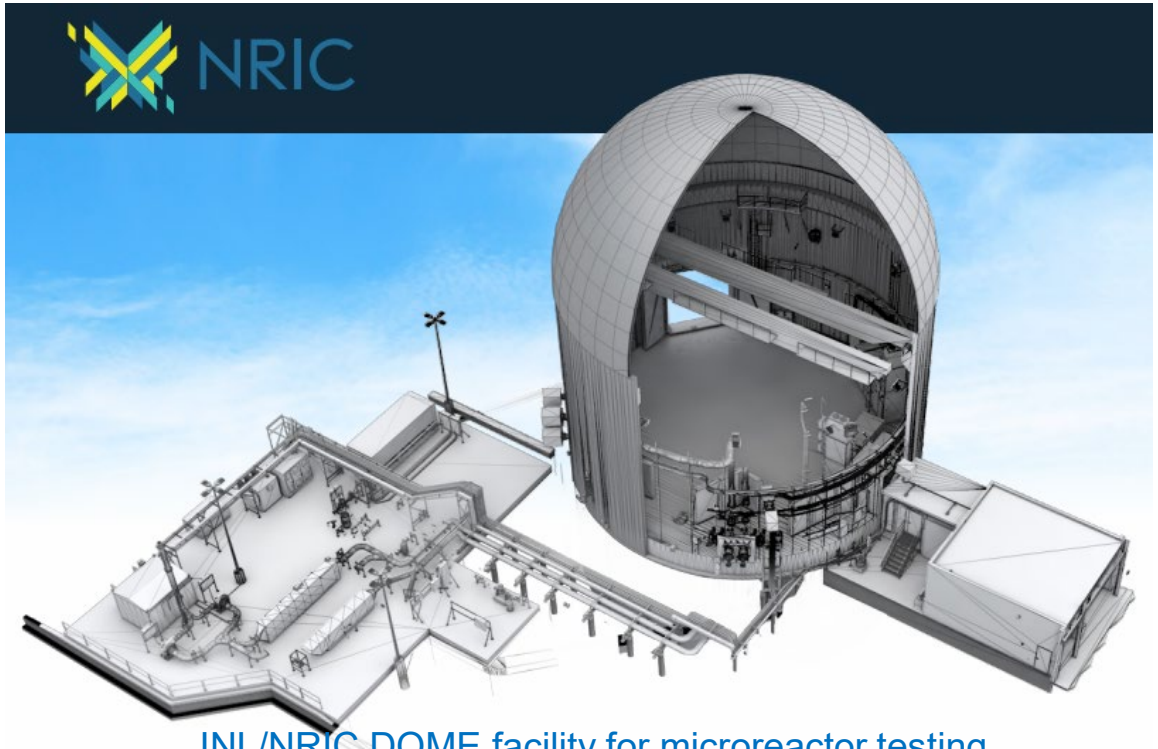
- Supports research and development of cybersecurity measures for nuclear reactors through funding and collaboration with national laboratories, academia, and industry.
- The ADRP focuses on developing and demonstrating next-generation nuclear reactor technologies that enhance safety, efficiency, and sustainability.
  - By integrating digital technologies like digital twins and advanced simulation tools, ADRP aims to optimize reactor operation and maintenance while promoting collaboration among government agencies, national laboratories, academia, and private industry.



DOE site (at INL) reactor system demonstration projects

INL Demonstration of Microreactor Experiments (DOME)

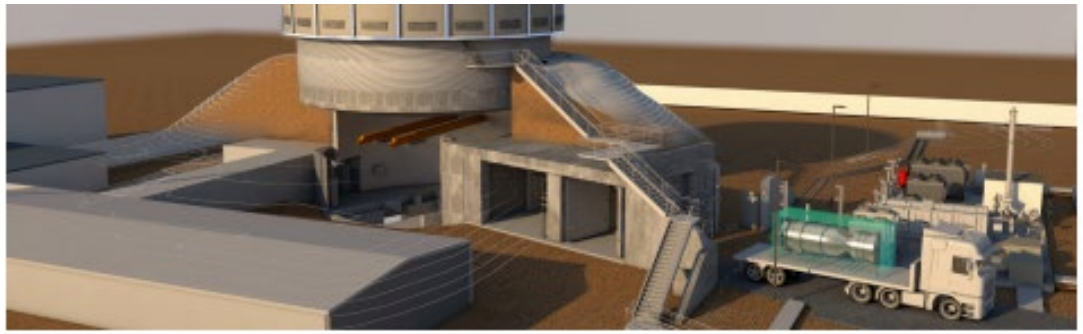
- DOME focuses on enhancing cybersecurity for critical infrastructure, including nuclear reactor systems.
  - It uses advanced monitoring, real-time data analytics, and rigorous testing to detect and mitigate cyber threats.



INL/NRIC DOME facility for microreactor testing

INL Laboratory for Operation and Testing in the U.S. (LOTUS)

- The LOTUS facility is dedicated to advancing cybersecurity for critical infrastructure.
  - It conducts comprehensive testing and evaluation of industrial control systems to identify and address vulnerabilities, including simulating real-world cyber-attack scenarios.



INL/NRIC LOTUS facility for reactor technology testing

INL Operational Technology Cybersecurity

A multi-sector, interdisciplinary approach to securing digital systems and critical functions

- Consequence-Driven Cyber-informed Engineering (CCE)
  - Providing critical infrastructure owners and operators a four-phase process for safeguarding their critical operations.
- Control System Engineering
  - Power, controls, electrical and systems engineering experts that incorporates experience and application of controls in critical lifeline sectors
  - OpDefender – An INL-developed device that filters out dangerous control systems commands, preventing hackers from taking over industrial facilities.
- Cybersecurity Research and Assessment
- Hunt and Incident Response
  - Malcolm Tool Suite – an open-source network traffic analysis tool.
- Cybersecurity Analysis and Controls Laboratory

SOWT Analysis for Repurposing Reactor Testing Facilities to Cyber Security Testbeds

Generic SWOT Study for Reactor System Cybersecurity

	Strengths	Weaknesses	Opportunities	Threats
A: Integrating Security Early (option #1) vs. Later (option #2)				
#1	Designing with security in mind from the start allows for improved resilience and lower long-term costs.	Early security integration increases design overhead, potentially delaying commercialization.	Sealed cores, passive shutdown, and remote monitoring can make Small Modular Reactors (SMRs) and Gen IV systems more secure by default.	Attackers increasingly combine cyber exploits with physical sabotage (e.g., drone incursions, insider threats).
#2	Late-stage design facilitates the incorporation of lessons learned, stakeholder input, and technological advancements.	Mid-to-late project design changes frequently lead to integration issues, increased costs, delays and potential compatibility problems.	Enables alignment with the most current safety, environmental, and cybersecurity standards, increasing compliance and public trust.	Delaying security or core design decisions could leave the system vulnerable to emerging threats and increase risks of cost and schedule overruns due to rework.
B: Leveraging Advanced Digital Tools and Modeling (option #1) vs. Minimal Tool Use (option #2)				
#1	Tools such as Path Trace (focuses on identifying vulnerabilities and calculating security-related probabilities) and AVERT-PS (physical security simulation software) can aid in optimizing plant layouts against intrusion.	Physical protection is prioritized, but embedded cybersecurity in instrumentation and control (I&C) systems is still developing.	Digital twins can continuously model system vulnerabilities and train AI to detect anomalies in real time.	Inconsistent regulatory expectations across countries or election-driven changes in nuclear policy may destabilize deployment.
#2	Easier project workflows with fewer tech dependencies can accelerate early development and decrease initial costs.	Limited foresight into vulnerabilities and inefficiencies, and lack of predictive modeling increases design risk and reduces chances for optimization.	Short-term cost savings may benefit budget-sensitive projects or developing regions with constrained infrastructure.	Lack of simulation and AI-based monitoring leaves systems defenseless to unseen risks, undetected anomalies, and future compliance deficits.

Generic SWOT Study for Rx System Cybersecurity (cont'd)

C: Aligning with Regulatory Security Frameworks (option #1) vs. Prioritizing Speed and Market-Driven Security (option #2)				
#1	Security-by-Design aligns with International Atomic Energy Agency's (IAEA's) INFCIRC/225 Rev.5 and U.S. Nuclear Regulatory Commission's (NRC) performance-based security objectives.	Most evidence is simulation-based; few full-scale deployments have validated these models.	Combining cyber and physical security into one framework increases resilience and simplifies management.	Private developers may deprioritize security features to meet cost or time targets in a competitive market.
#2	Deprioritizing regulatory alignment and complex frameworks, companies can speed up development and offer an early-mover advantage.	Failure to align with IAEA/NRC guidance can lead to licensing delays, costly redesigns, or project rejection.	Prioritizing flexibility over strict compliance can support more responsive product development in emerging global markets.	Omitting integrated cyber-physical security strategies increases exposure to advanced and evolving threats.

D: Unified Security Frameworks (option #1) vs. Decentralized or Custom-Built Systems (option #2)				
#1	Sandia's Advanced Reactor Safeguards and Security (ARSS) program supports integrated safety, security, and safeguards, reducing redundancy.	Designs for pebble-bed high-temperature gas-cooled reactors (HTGR) may not apply easily to molten salt or sodium fast reactors.	Designs can be adapted to protect water plants, microgrids, and critical communication hubs.	Closed-source modeling and assessment tools limit transparency, collaboration, and adaptation by third parties.
#2	Independently managed safety and security systems can be customized for specific reactor designs or mission goals.	Disconnected frameworks can result in duplicated efforts, higher costs, and complex integration challenges.	Avoiding standardized approaches allows for flexible solutions for experimental or niche reactor technologies.	Inconsistent designs increase the likelihood of oversights, conflicting protocols, or exploitable gaps between security domains

Generic SWOT Study for Rx System Cybersecurity (cont'd)

E: Adapting Mature IT Cybersecurity Tools for OT/Nuclear (Option #1) vs. Developing Custom OT-Specific Solutions (Option #2)				
#1	Leverages technology with readily available, cost-effective tools that accelerate implementation (e.g., firewalls, IDS, SIEM).	Designed for high-speed, data-centric IT networks, these tools may be incompatible with legacy OT systems and ill-suited for deterministic environments.	Enables rapid deployment in hybrid testbeds while supporting benchmarking and adaptation for future reactor designs.	Misapplication or overreliance on tools not built for safety-critical systems can result in operational disruptions and false positives.
#2	Specifically tailored for deterministic, safety-critical OT environments, offering greater control over behavior-based detection for legacy protocols.	Involves higher R&D costs, extended development timelines, and the need for a specialized workforce to build and maintain the tools.	Offers the potential to develop purpose-built frameworks recognized by regulators and to lead the advancement of nuclear-specific cybersecurity standards.	May lack the advantages of broad industry testing and patch cycles, with a high barrier to certification or approval due to limited precedent.

F: Converting Existing Safety Test Facilities to Cyber-Physical Environments (Option #1) vs. Building New Cyber-Integrated Facilities from Scratch (Option #2)				
#1	Leverages existing infrastructure and test procedures, enabling faster, more cost-effective implementation while maintaining continuity in mission focus.	Instrumentation and control systems may need substantial retrofitting, potentially causing operational disruptions during the upgrade process.	Serves as a bridge between traditional and modern testing approaches, demonstrating the feasibility of hybrid retrofits to both industry and regulators.	Physical layout constraints or outdated hardware may complicate retrofitting, introducing integration risks and potential system inconsistencies.
#2	Offers full integration of safety and cybersecurity from the outset, free from legacy constraints and enabling a modern architectural design.	Entails higher capital investment and extended build time, potentially requiring duplication of existing assets and capabilities.	Provides an opportunity to develop a secure-by-design testbed free from legacy constraints, potentially establishing a benchmark for future global test facilities.	Greenfield projects carry risks such as delays, cost overruns, and staffing shortages, and may face funding challenges if existing facilities are underutilized.

Generic SWOT Study for Rx System Cybersecurity (cont'd)

G: Building a Modular Cyber-Physical Testbed for OT/Nuclear (Option #1) vs. Retaining Traditional Safety-Only Facilities (Option #2)				
#1	Enables comprehensive cybersecurity testing alongside safety evaluations by integrating HIL, passive monitoring, and digital twins, while supporting red-team/blue-team exercises and scenario replays for resilience assessment.	Requires substantial investment in tools, simulation infrastructure, and workforce training, with potential integration challenges between physical and virtual systems.	Positions NRIC as a leader in secure-by-design testing by enabling proactive validation of cyber and safety co-performance, while fostering collaboration across academia, industry, and government.	System complexity may lead to unforeseen failure modes or interactions, and discrepancies between simulation and real-world conditions could undermine testbed validity.
#2	Simpler setups lower operational complexity, while stable and well-understood legacy designs help minimize the risks associated with change.	Limited capacity to detect or respond to modern cyber threats, coupled with the absence of real-time monitoring and emulation tools, hinders proactive defense development.	Maintains continuity in traditional safety-focused testing while allowing concentrated efforts on physical hazard resilience without added cyber complexity.	The growing sophistication of cyberattacks may render safety-only facilities inadequate, while regulatory pressure to integrate cybersecurity could result in rushed and suboptimal retrofits.

Specific SWOT Analysis for Repurposing NRIC Reactor Test Facilities to Cyber Testbed

Parameters	Strengths	Weaknesses	Opportunities	Threats
NRIC test facilities	Facilities have already been constructed.	Facility was originally focused solely on reactor system safety.	Can be converted into cyber testbed.	Implementing cybersecurity measures in the later stages of design is both costly and challenging
Reactor simulator	INL possesses a range of both digital and physical simulators.	Design changes made during the mid-to-late stages of a project often result in integration challenges, increased costs, schedule delays, and potential compatibility issues.	Enables alignment with the most current safety, environmental, and cybersecurity standards.	Delaying security or core design decisions can leave the system vulnerable to emerging threats and significantly increase the risk of cost and schedule overruns due to necessary rework
Cyber tools	INL has a dedicated cyber group equipped with specialized tools and methodologies for cybersecurity research and implementation.	Not yet been implemented in new and advanced reactor systems.	Can be adopted to support reactor demonstration and deployment.	No prior experience with full-scale reactor facilities.
Policy and Regulations	Policies and regulations are almost developed, with contributions from organizations such as SANDIA, CISA, NNSA, and NRC.	It has not been implemented so there is a lack of user experience from new reactor facilities.	Can be adopted throughout the entire reactor lifecycle.	Modifications may be required in response to evolving cyber incidents and emerging threat landscapes.

How to use IT for OT and nuclear reactor system

Tailored Intrusion Detection Systems (IDS): Adapt IT-focused tools like Snort or Suricata to recognize OT-specific protocols and apply behavior-based detection tailored to industrial environments.

Network Segmentation: Enforce strict zoning and conduit policies according to ISA/IEC 62443 to limit lateral threat movement and enhance containment.

Read-Only Monitoring: Deploy passive sensors and anomaly detection tools that monitor network traffic without disrupting time-sensitive or safety-critical operations.

ICS-Specific SIEM: Use centralized logging platforms configured to filter for OT-relevant events and set context-aware alert thresholds based on physical system behavior.

How to Convert Test Facilities and Simulator to Cyber Testbed which are Primarily Designed for Safety

Baseline Modeling: Create a digital representation of the system architecture, including process flows and control logic within the test facility.

Instrumentation Upgrade: Install mirrored interfaces such as SPAN ports or optical taps to enable data capture without affecting existing safety functions.

Cyber-Physical Mapping: Integrate virtual PLCs, emulated I&C devices, and traffic replay tools to simulate cyber interactions and test malicious scenarios.

Data Capture and Replay: Enable time-synchronized recording of operational and network data to support scenario replays and red-team exercises.

Controlled Injection of Faults: Introduce simulated cyber faults or anomalies to test system resiliency without risking physical infrastructure.

How to Connect HIL, Human Factor Engineering and CIE Within the Simulated Environment: Integration Strategy

Hardware-in-the-Loop (HIL): Link actual control components such as PLCs and HMIs to the simulator to enable realistic interactions with digital twin environments.

Human Factors Engineering (HFE): Implement advanced Human-System Interface (HIS) mock-ups to assess operator behavior and response under simulated cyber conditions, such as spoofed alarms or delayed commands.

Cyber-Informed Engineering (CIE): Embed cyber threat models and detection mechanisms into the early design stages of the simulation to jointly evaluate both safety and cybersecurity performance.

How to Connect HIL, Human Factor Engineering and CIE Within the Simulated Environment: Tooling Options

Digital Twin Platforms (e.g., ANSYS Twin Builder, MATLAB Simulink): These platforms allow for high-fidelity modeling and simulation of physical systems, enabling real-time co-simulation with hardware-in-the-loop (HIL) components. They support scenario testing, system validation, and performance benchmarking under both normal and cyber-compromised conditions.

Industrial Protocol Simulators and Fuzzers: Tools that simulate and test communication protocols commonly used in OT environments (such as Modbus, DNP3, or OPC UA). Fuzzing capabilities help identify vulnerabilities by injecting malformed or unexpected data into network traffic, allowing engineers to evaluate system robustness against cyber threats.

Cognitive Modeling Tools for Human Operator Behavior: Software frameworks that simulate human decision-making and behavior in response to dynamic system states, including stress or deception from cyber events. These tools support the evaluation of Human-System Interface (HSI) designs and help improve training, workload management, and situational awareness in control room settings.

Hybrid Cybersecurity Integration Tools*:* These solutions integrate established IT cybersecurity tools like firewalls and IDS with the specific needs of OT environments. They enable IT tool adaptation and benchmarking in hybrid testbeds while addressing the constraints of deterministic, safety-critical nuclear systems. Careful configuration is key to minimizing false positives and ensuring compatibility with legacy infrastructure.

Implementation Roadmap

Phase 1

System Assessment:
- Conduct a thorough mapping of existing equipment and control (I&C) systems, network infrastructure, and safety simulation assets.
- Identify and document critical digital assets, communication pathways, and interdependencies.

Phase 2

Interface IT and OT Cybersecurity:
- Deploy passive network monitoring tools (e.g., Zeek, Claroty) to capture baseline traffic and detect anomalies.
- Create virtual PLCs and I&C components to simulate and test cyber attack and defense scenarios.

Phase 3

Simulator and Hardware Interface
- Connect real control hardware to simulated plant environments for realistic hardware-in-the-loop (HIL) interaction.
- Integrate cyber threat scenarios into human factors engineering and usability studies, following Cyber-Informed Engineering (CIE) principles.

Phase 4

Validation and Training:
- Design and conduct red-team/blue-team exercises in the testbed to assess system defenses under adversarial conditions.
- Validate detection, response, and recovery protocols within realistic operational constraints to ensure field deployment readiness.

Conclusion

- This study highlights the urgent need to integrate advanced cybersecurity into both new and existing nuclear reactor systems from the earliest design stages. Various organizations and R&D initiatives are involved. A specific SWOT analysis was performed, focusing on how the reactor testing facilities at the DOE INL site could be repurposed as cyber testbeds.
- The specific findings from SWOT analysis (options and potential solutions) are as follows:
  - **Integrating Security Early vs. Later**
    - Early-stage integration is the best option due to all around lower costs and increased resilience;
    - However, it is best to continually update security practices to prevent zero-day attacks.
  - **Leveraging Advanced Digital Tools and Modeling vs. Minimal Tool Use**
    - Utilizing advanced tools would allow for easier and more efficient ways to detect vulnerabilities, as well as optimize plant layouts against intrusion.
    - Tools used would have to comply with policies at the given time.
  - **Aligning with Regulatory Security Frameworks vs. Prioritizing Speed and Market-Driven Security**
    - To prevent unnecessary additional costs along with project rejection, it is best that reactor vendors follows SbD with appropriate guidance from IAEA and NRC.

Conclusion (cont'd)

- SWOT Options and Solutions:
  - **Unified Security Frameworks (option #1) vs. Decentralized or Custom-Built Systems (option #2)**
    - This varies depending on the reactor system and the project at hand. Sometimes custom systems are necessary to hit mission goals.
  - **Adapting Mature IT Cybersecurity Tools for OT/Nuclear vs. Developing Custom OT-Specific Solutions**
    - This varies depending on the situation. Readily available technology such as IDS or SIEM drastically saves time, allowing for rapid deployment. Not optimal for legacy OT systems (poor compatibility) and not specifically tailored to any specific environment.
  - **Converting Existing Safety Test Facilities to Cyber-Physical Environments vs. Building New Cyber-Integrated Facilities from Scratch**
    - Leveraging existing infrastructure might be the best case because there are already plans to use decommissioned reactor facilities as test beds through NRIC. Although I&C might need retrofitting, this is currently the best course of action both finance-wise as well as time-wise.

Conclusion (cont'd)

- SWOT Options and Solutions:
  - **Building a Modular Cyber-Physical Testbed for OT/Nuclear vs. Retaining Traditional Safety-Only Facilities**
    - Building a modular, cyber-physical testbed is the most optimal option overall
    - It is easy to implement new technology while also not having to cover costs of rebuilding
    - ARDP, DOME and LOTUS, will be leveraged by several reactor vendors, supporting organization, and stakeholders, which are mostly focused for safety; however, could be extended to cyber-physical security as well.

- By using a SWOT analysis, the study emphasizes the advantages of early implementation over retroactive fixes and explores technologies such as reactor simulators, AI, and digital twins for threat detection. Aligned with U.S. NRC and IAEA guidance and frameworks, the study proposes transforming NRIC and INL into a phased, secure-by-design cyber-physical testbed to ensure resilient, next-generation reactor operations that support safety, sustainability, and energy sector viability.

References

- Kim, Y., & Han, J. (2023). Cyber hardening of nuclear power plants with real-time nuclear reactor operation: Preliminary operational testing. ScienceDirect. https://doi.org/10.1016/j.anucene.2023.109359
- USNRC, U.S. Nuclear Regulatory Commission. (2025a). Cybersecurity. https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cybersecurity.html
- Center for Strategic and International Studies. (2021). Strengthening cybersecurity in U.S. and U.K. nuclear facilities. https://www.csis.org
- New Jersey Cybersecurity & Communications Integration Cell. (2020). Nuclear reactors, materials, and waste sector threat analysis report. https://www.cyber.nj.gov
- IAEA, International Atomic Energy Agency. (2025a). Cyber security for nuclear power plants. Retrieved July 21, 2025, from https://ww.iaea.org/
- Kevin Dunne. (2025). How to perform a SWOT analysis. Retrieved July 21, 2025, from https://www.mindtools.com/pages/article/newTMC_05.htm
- Cisco. (2025). What is OT vs. IT?. Retrieved July 21, 2025, from https://www.cisco.com/site/us/en/learn/topics/industrial-iot/what-is-ot-vs-it.html
- Silva, R. B., Piqueira, J. R. C., Cruz, J. J., & Marques, R. P. (2021). Cybersecurity assessment framework for digital interface between safety and security at nuclear power plants. *International Journal of Critical Infrastructure Protection*, *34*, 100453.
- Sklyar, V. (2012). Cyber security of safety-critical infrastructures: a case study for nuclear facilities. Information & Security, 28(1), 98.
- NRIC, National Reactor Innovation Center. (2025). Welcome to NRIC. https://nric.inl.gov/
- INL, Idaho National Laboratory. (2025). Critical infrastructure security. https://inl.gov/cybercore/critical-infrastructure-security
- Western Services Corporation. (2025). All news. Retrieved July 21, 2025, from https://www.ws-corp.com/default.asp?PageID=79&PageNavigation=All-News
- Bhowmik, P. K. (2025). *SECURED: Simulator-Enhanced Control and Understanding of Reactor systems for cyber-Event Defense* (No. INL/MIS-25-82966-Rev000). Idaho National Laboratory (INL), Idaho Falls, ID (United States). https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_155997.pdf
- Bhowmik, P.K., S. Alam, S. Talukder, and P. Sabharwall. 2023. “Nuclear-Integrated Energy Units: Advancing Cybersecurity for Resilient Energy Systems.” *IEEE International Conference on Systems, Man, and Cybernetics (SMC 2023),* 1–4 October 2023, Maui, HI, USA. INL/CON-23-72960, October 2023. Available at: https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_66413.pdf (accessed 14 November 2024).

References (cont'd)

- Bhowmik, P.K., S. Talukder, S. Alam, and P. Sabharwall. 2023. "Cybersecurity Challenges and Solutions for Distributed Energy Resources." *IEEE International Conference on Systems, Man, and Cybernetics (SMC 2023),* 1–4 October 2023, Maui, HI, USA. INL/CON-23-72954, October 2023.
- Glenn, C., Sterbentz, D., & Wright, A. (2016). *Cyber threat and vulnerability analysis of the US electric sector* (No. INL/EXT-16-40692). Idaho National Lab.(INL), Idaho Falls, ID (United States).
- Möller, D. P. (2023). Cybersecurity Maturity Models and SWOT Analysis. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 305-346). Cham: Springer Nature Switzerland.
- USNRC, U.S. Nuclear Regulatory Commission. (2025b). Home page. https://www.nrc.gov/
- USNRC, U.S. Nuclear Regulatory Commission. (2025c). 10 CFR Part 73.54—Protection of digital computer and communication systems and networks. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html
- USNRC, U.S. Nuclear Regulatory Commission. (2025d). Regulatory Guide 5.71: Cybersecurity programs for nuclear facilities. https://www.nrc.gov/reading-rm/doc-collections/reg-guides/protection/rg/05-071/
- INPO, Institute of Nuclear Power Operations. (2025). About INPO. https://www.inpo.info/
- NEI, Nuclear Energy Institute. (2025). Home page. https://www.nei.org/
- IAEA, International Atomic Energy Agency. (2025b). Home page. https://www.iaea.org/
- AEC, International Electrotechnical Commission. (2025). Home page. https://www.iec.ch/
- INL, Idaho National Laboratory. (2025b). Cybercore Integration Center. https://inl.gov/cybercore
- Sandia National Laboratories. (2025). Nuclear energy cybersecurity by design. Retrieved July 21, 2025, from https://energy.sandia.gov/programs/nuclear-energy/nuclear-energy-security/nuclear-energy-cyberSbD/
- Mozilla. (2025). Session hijacking. MDN Web Docs. Retrieved July 21, 2025, from https://developer.mozilla.org/en-US/docs/Glossary/Session_Hijacking

References (cont'd)

- DHS, U.S. Department of Homeland Security. (2025). Cybersecurity and critical infrastructure. Retrieved July 21, 2025, from https://www.dhs.gov/archive/coronavirus/cybersecurity-and-critical-infrastructure
- Secure by Design: What Does It Mean & How to Reasonably Implement It. (2025). Retrieved August 1, 2025, from Secure by Design: What Does It Mean & How to Reasonably Implement It
- IAEA, International Atomic Energy Agency. (2025). Instrumentation and control systems for nuclear power plants. Retrieved August 1, 2025, from Instrumentation and Control Systems for Nuclear Power Plants | IAEA
- Digital twin. Retrieved July 21, 2025, from https://www.ansys.com/en-in/products/digital-twin
- Fruhlinger, J. (2022). Defense in depth explained: Layering tools and processes for better security. *CSO. Available online: https://www. csoonline. com/article/573221/defense-in-depth-explained-layering-tools-and-processes-for-better-security. html (accessed on 28 July 2022)*.
- SNL, Sandia National Laboratories. (2025). Safety, security, and safeguards for advanced nuclear power. Retrieved August 1, 2025, from https://energy.sandia.gov/programs/nuclear-energy/safety-security-and-safeguards-for-advanced-nuclear-power/
- Snell, M. K., Jaeger, C. D., Scharmer, C., Jordan, S. E., Tanuma, K., Ochiai, K., & Iida, T. (2013). *Security-by-design handbook* (No. SAND2013-0038). Japan Atomic Energy Agency, Ibaraki, Japan; Sandia National Lab.(SNL-NM), Albuquerque, NM (United States). https://www.osti.gov/servlets/purl/1088049
- NIST, National Institute of Standards and Technology. (2025). Home page. https://www.nist.gov/Ansys. (2025).
- AC08970266, A. (Ed.). (2011). Core knowledge on instrumentation and control systems in nuclear power plants. IAEA.
- Adams, S. S., Bruneau, R. J., Jacobs, N. L., Murchison, N., Sandoval, D. R., & Seng, B. E. (2018). Enhancing power plant safety through coupling plant simulators to cyber digital architecture. https://www.osti.gov/servlets/purl/1484584
- Root, S. J., Throckmorton, P., Tacke, J., Benjamin, J., Haney, M., & Borrelli, R. A. (2023). Cyber hardening of Nuclear Power Plants with real-time nuclear reactor operation, 1. Preliminary operational testing. Progress in nuclear energy, 162, 104742. https://doi.org/10.1016/j.pnucene.2023.104742.

References (cont'd)

- Allgood, B. and A. Fels, P.K. Bhowmik, P. Sabharwall, "Reactor Simulation Using CrowPi," High School Internship Research Report, June 21, 2023 – July 21, 2023, INL/RPT-23-73744.
- Bhowmik, P.B., Dhar, S.K., Chakraborty, S. 2013. "Operation and Control of TRIGA Nuclear Research Reactor with PLC," *Int. J. of Info. and Electronics Eng.* 3 (6). https://ijiee.org/papers/377-C025.pdf.
- Pohlmann, M. L., P.K. Bhowmik, C. Wang, and P. Sabharwall. 2024. "Development of a Simplified AI Model for Effective Sensor Anomaly Detection in Nuclear Reactor Systems." *ES 2024 18th International Conference on Energy Sustainability*, 15–17 July 2024, Anaheim, CA, USA. https://doi.org/10.1115/1.4064123.
- Abdellatif, H. H., P.K. Bhowmik, D. Arcilesi, and P. Sabharwall. (2024). "Accident event progression, gaps, and key performance indicators for steam generator tube rupture events in water-cooled SMRs: A Review," *Prog. Nucl. Energy*, 168, 105021. https://doi.org/10.1016/j.pnucene.2023.105021.
- Abdellatif, H. H., P.K. Bhowmik, D. Arcilesi, and P. Sabharwall. (2024). "Analysis of AP1000 small-break loss-of-coolant accident using reactor transient simulator." *Nucl. Technol.*, 10 June 2024, 1–17. https://doi.org/10.1080/00295450.2024.2342168.
- Marsh, K., P.K. Bhowmik, P. Sabharwall, "Integrating PCTRAN with AI-Driven Host-Intrusion Detection and Secured Container Systems for Advanced Malware Analysis," Internship Report, 2024, INL/RPT-24-80484-Rev000. https://www.osti.gov/servlets/purl/2448404/.
- Purser, K., M. Clegg, Q. Kester, D. Tucker, P.K. Bhowmik, K.L. Fossum, P. Sabharwall, "Reactor System Demonstration with Cyber-Attack Scenarios Using CrowPis and Arduino Microcontrollers," High School Internship Report, 2024, INL/RPT-24-80481-Rev000. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_129240.pdf.
- Aanonsen, A., G. Chen, P.K. Bhowmik, P. Sabharwall, "Advanced Data Science Model for Detecting Intelligent Malware," Internship Report, 2024, INL/RPT-24-80512-Rev000. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_129750.pdf.

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.