Advanced Reactor Safeguards & Security

2024 Program Roadmap

Prepared for
US Department of Energy

Benjamin B. Cipiti[1], Dan Warner[2], Katya Le Blanc[3], Alan Evans[1], John R. Russell[1], Nathan Shoman[1], Anna Taconi[1], Mike Rowland[1], Chris Lamb[1], Lee Maccarone[1], Ben Karch[1], Andrew Hahn[1], Patrick Moosir[1], Shannon Eggers[3], Robert Youngblood[3], Claudio Gariazzo[4], Nathaniel Hoyt[4], Benjamin Blakely[4], Rick Vilim[4], Lap Cheng[5], Yonggang Cui[5], Mark Croce[6], Azaree Lintereur[6], Philip Gibbs[7], Maggie Arno[7], Sunil S Chirayath[7], Karen K Hogue[7], Shirmir Branch[8], Glenn Fink[9]

[1]Sandia National Laboratories
[2]U.S. Department of Energy
[3]Idaho National Laboratory
[4]Argonne National Laboratory
[5]Brookhaven National Laboratory
[6]Los Alamos National Laboratory
[7]Oak Ridge National Laboratory
[8]Pacific Northwest National Laboratory
[9]Savannah River National Laboratory

July 2024
SAND2024-09669R

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Prepared by Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

Sandia National Laboratories

ABSTRACT

The Advanced Reactor Safeguards and Security (ARSS) program was established to provide research support addressing near term challenges that advanced nuclear reactor vendors face in meeting domestic Material Control and Accounting (MC&A), Physical Protection System (PPS), and Cybersecurity requirements for U.S. construction. The technical work in the program is meant to (1) support nuclear reactor vendors with advanced MC&A, PPS, and Cybersecurity designs for next generation reactors, (2) provide technical bases for the regulator, and (3) promote the integration of Safeguards and Security by Design early in the design process. Existing domestic regulations for safeguards and security, as outlined in the Code of Federal Regulations, were written for large light water reactors, and rule-making efforts are underway to develop regulations more suited to different reactor designs. The ARSS program seeks to remove roadblocks in the deployment of new and advanced reactors by solving regulatory challenges, reducing safeguards and security costs, and utilizing the latest technologies and approaches for robust plant monitoring and protection. This roadmap discusses the goals of the ARSS program, current research, and program plan for the next five years.

ACKNOWLEDGEMENTS

The Advanced Reactor Safeguards and Security Program is funded through the Office of Nuclear Energy within the United States Department of Energy.

CONTENTS

LIST OF FIGURES

This page left blank

EXECUTIVE SUMMARY

The Advanced Reactor Safeguards and Security (ARSS) program seeks to remove roadblocks in the deployment of new and advanced reactors in the United States by solving regulatory challenges, reducing domestic safeguards and security costs, and utilizing the latest technologies and approaches for robust plant monitoring and protection. Safeguards and Security by Design (SSBD), or the consideration of safeguards and security requirements early in the design process, is an over-arching principle that guides this program. The following summarizes five key goals of the ARSS program.

1. **Develop Next Generation Physical Protection Systems and Approaches:** The need for large numbers of on-site responders is a significant economical roadblock for deployment of small modular reactors and microreactors which need to compete with other sources of power. Existing regulations written for large Light Water Reactors (LWRs) may not apply to these new designs. The ARSS program is evaluating Physical Protection System (PPS) approaches that provide robust protection with a drastically reduced response force, provide protection against the insider threat, and utilize the latest in detection, delay, and response technologies. The research is evaluating how enhanced safety (longer timelines in accident/sabotage scenarios) can be utilized in developing optimized and appropriate physical protection approaches. This area of work is evaluating unique sabotage targets since the advanced reactors will have new sabotage pathways to consider. The ARSS program is also considering the interfaces with Material Control and Accounting (MC&A) as well as cybersecurity including evaluating cyber-physical attacks.
2. **Develop MC&A Approaches for Pebble Bed and Liquid-Fueled Molten Salt Reactors:** Pebble Bed Reactors (PBRs) utilize fuel pebbles instead of fuel assemblies, and liquid fueled Molten Salt Reactors (MSRs) contain fuel in a molten salt form. Both present MC&A challenges since they move away from the traditional item accountancy approach typical of existing reactors. The ARSS program is developing MC&A approaches for PBRs and MSRs as well as solving key gaps in the accountancy strategy through new measurement technologies and approaches. The interfaces between safeguards and security in the overall plant design and protection of these systems are also being examined.
3. **Provide R&D Support for Unique Deployment of SMRs and Microreactors:** A variety of new uses for SMRs and microreactors are being considering in the U.S. including use of microreactors for university research reactors, use of advanced reactors for floating nuclear plants or civilian maritime propulsion, and use of advanced reactors for industrial applications like process heat. The ARSS program is providing research support to better understand safeguards and security challenges for these deployment options.
4. **Develop Cyber Informed Engineering Approaches and Apply Cybersecurity Technologies to Advanced Nuclear Systems:** A rapidly evolving cyber threat space coupled with increased reliance on digital systems presents multiple challenges in developing reactor designs that are protected against cybersecurity attacks. The ARSS program supports research to develop systems-level approaches including Defensive Cyber Security Architectures for the different classes of advanced reactors. This work is linked with technology development and red-teaming to provide evidence that nuclear control systems will be secure. While cybersecurity research in general is a very broad and growing field, the ARSS program focuses on challenges and technology solutions as they would apply specifically to nuclear energy systems. The research examines where technologies may be used, provides testing and evaluation, and develops recommendations for vendors on the appropriate use of cyber technologies in nuclear control systems.

5. **Examine International Interfaces:** The vast majority of vendors are ultimately interested in international deployment. From a SSBD perspective, the vendors should design MC&A and PPS systems in a way that also helps to meet international requirements (which can vary depending on the country). The DOE NE ARSS program works in partnership with National Nuclear Security Administration (NNSA) programs that focus on international safeguards and security for advanced reactors. The ARSS program also supports U.S. involvement in the Generation-IV International Forum's Proliferation Resistance and Physical Protection working group.

As part of the five major thrust areas defined above, there are two crosscutting topics that cover all of these spaces: vendor engagements and the application of SSBD. While most of the work in ARSS is designed to be broadly applicable to all vendors or classes of reactors, design-specific challenges need to be solved as the vendor designs mature and move closer to deployment. The ARSS program provides support to the DOE laboratories for vendor engagements to help validate the protection and accountancy approaches being considered. These vendor engagements are highly useful to understand the current challenges the vendors are navigating and promote SSBD within their organizations. In addition to design-specific work tailored to the particular vendor, these projects generate a generic lessons-learned report that provide value to other nuclear reactor vendors.

The work in the ARSS program to date has shown that advanced reactor vendors will benefit greatly from taking a Safeguards, Security, and Safety by Design (3SBD) approach to develop cost-effective protection strategies. 3SBD means that all requirements for safety, MC&A, PPS, cybersecurity, and international safeguards are taken into account very early and throughout the full design process. 3SBD also means understanding the interfaces between the S's and tradeoffs that must be made in the design space. The ARSS program will increasingly move toward full 3S design approaches for each class of advanced reactor.

The ARSS program area has several stakeholders. The vendors are key stakeholders, and their needs are driving the research and direction of the program. Nuclear utilities are also a key stakeholder since the burden of operational costs of the MC&A, PPS, and Cybersecurity falls on the operator of the plant. The Nuclear Energy Institute (NEI) provides an interface between vendors and has explored several of these challenge areas in the past. The Nuclear Regulatory Commission (NRC) is also a key stakeholder, and much of the research is being performed with their input—it is hoped that the work will also be useful to help inform regulatory needs in the future. There are several other program areas within DOE NE that require coordination including those focusing on the specific classes of advanced reactors and cross-cutting program areas that support advanced reactors vendors in other ways. Stakeholder engagement is a key aspect of the program to prioritize research.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
3SBD	Safety, Security, and Safeguards by Design
AI	Artificial Intelligence
ARCADE	Advanced Reactor Cybersecurity Analysis and Development Environment
ARSS	Advanced Reactor Safeguards and Security
ARDP	Advanced Reactor Demonstration Program
BBRE	Bullet and Blast Resistance Enclosure
CAS	Central Alarm Station
CFR	Code of Federal Regulations
COTS	Commercial Off the Shelf
DA	Destructive Analysis
DCSA	Defensive Cybersecurity Architecture
DMA	Deliberate Motion Analytics
DOE	Department of Energy
FKMP	Flow Key Measurement Point
GIF	Generation-IV International Forum
HALEU	High Assay Low Enriched Uranium
HPGe	High Purity Germanium
IAEA	International Atomic Energy Agency
ID	Inventory Difference
IKMP	Inventory Key Measurement Point
iPWR	Integral Pressurized Water Reactor
LWR	Light Water Reactor
MBA	Material Balance Area
MC&A	Material Control and Accountability
MFIT	Modular Flow Instrumentation Testbed
ML	Machine Learning
MSR	Molten Salt Reactor
MW	Megawatt
NDA	Nondestructive Analysis
NE	Office of Nuclear Energy
NEI	Nuclear Energy Institute
NNSA	National Nuclear Security Agency
NRC	Nuclear Regulatory Commission
PBR	Pebble Bed Reactor

Abbreviation	Definition
PIDAS	Perimeter Intrusion Detection and Assessment System
PIDS	Perimeter Intrusion Detection System
PIRT	Phenomenon Identification Ranking Table
PPS	Physical Protection System
PRA	Probabilistic Risk Analysis
PR&PP	Proliferation Resistance and Physical Protection
ROWS	Remote Operated Weapons System
RPM	Radar Bi-Spectral Pan Tilt Zoom Module
RTR	Research and Test Reactor
SE	Secure Element
SEID	Standard Error of the Inventory Difference
SFR	Sodium Fast Reactor
SMR	Small Modular Reactor
SNM	Special Nuclear Material
SSBD	Safeguards and Security by Design
TRISO	Tri-Isotropic
UAV	Unmanned Aerial Vehicle
VAI	Vital Area Identification

1. INTRODUCTION

New nuclear energy deployment has had a challenging path over the past several decades. Although public support for nuclear can be a factor, economics plays a more important role. The existing fleet of large, light water reactors (LWRs) has seen plant shutdowns due to difficulties competing in the current electricity market. New large reactor construction is particularly challenging in the United States due to the very high up-front capital costs required, which many utilities either cannot afford or view as too much of a risk. In addition, increasing energy demand has not grown as fast as once predicted, and 1000 MW_e installations are too large for many regions.

As a result, interest in new nuclear energy generation has moved toward smaller, more modular installation. This renewal of interest is also being driven by several vendor startups over the past decade and venture capital money going into small modular and advanced reactor designs. However, small and advanced reactors continue to face challenging market economics. There are several hurdles that must be overcome for new nuclear deployment to be successful. Past work has identified these roadblocks for Small Modular Reactors (SMRs),[1,2] but there are new challenges as designs have evolved toward different reactor classes and sizes. One of the current goals of the overall Nuclear Energy program area within the Department of Energy (DOE) is to help alleviate these roadblocks to deployment.

The Advanced Reactor Safeguards and Security (ARSS) program provides research support for Material Control and Accounting (MC&A), Physical Protection System (PPS), and Cybersecurity to help enable advanced nuclear energy systems (see Figure 1). Each pathway provides R&D support at the systems level, to provide overall system design approaches, and at the technology level to examine new technologies or applications to meet regulatory requirements. All areas must consider the interface with safety, although safety is not part of the R&D portfolio in the ARSS program. Over the next several years, the ARSS program will increasingly look at integrated design approaches and move more toward Safeguards, Security, and Safety by Design (3SBD).

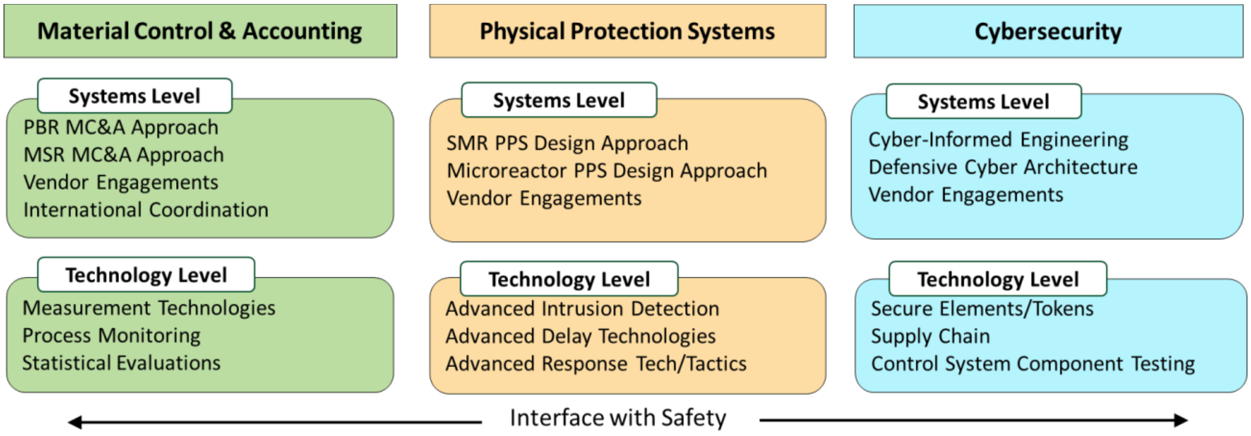

Figure 1: ARSS Research Areas

Existing regulations for safeguards and security, as outlined in the Code of Federal Regulations (CFR), were written for large LWRs, and some of the requirements are not suited to smaller advanced reactor designs. The Nuclear Regulatory Commission (NRC) is currently going through a rulemaking process

[1] T. Grenci et al., "Interim Report of the American Nuclear Society President's Special Committee on Small and Medium Sized Reactor (SMR) Generic Licensing Issues," American Nuclear Society (July 2010).

[2] R.J. Bell et al., "Position Paper: Physical Security for Small Modular Reactors," Nuclear Energy Institute (July 2012).

to help address these issues.[3,4] The ARSS program seeks to remove roadblocks in the deployment of new and advanced reactors by solving regulatory challenges, reducing safeguards and security costs, and utilizing the latest technologies and approaches for robust plant monitoring and protection.

This document represents a roadmap for the ARSS program over the next five years. Most of the research in the program is targeted on near-term deliverables to provide guidance to vendors as soon as possible. These near-term deliverables focus on approaches that will meet regulatory requirements and can inform both vendors and the regulator. The ARSS program is designed to cover a range of issues that will be applicable to all vendors, but the work will be guided by those vendors that have more near-term needs. The research portfolio is expected to change over the next five years as existing challenges are solved and new gaps are identified.

[3] "Rulemaking for Physical Security for Advanced Reactors," NRC Docket ID: NRC-2017-0227, Nuclear Regulatory Commission (2019).

[4] "Preliminary Proposed Rule Language: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors," NRC Docket ID: NRC-2019-0062 (2020).

2. PROGRAM DRIVERS

The research areas in the ARSS program are informed primarily by vendor and utility needs. Input from the Nuclear Energy Institute (NEI) and the NRC is also considered. The majority of the research is designed to be applicable across different reactor classes and not focused on any one design. The Advanced Reactor Demonstration Program (ARDP) award winners, announced by DOE NE in late 2020, play a role in prioritization. The following lists the award winners from the ARDP program as well as those vendors in licensing or pre-licensing activities with the NRC.

Demonstration Projects:

- Terrapower and GE-Hitachi Natrium Reactor (sodium cooled fast reactor, 345 MWe, coupled with molten salt thermal energy storage, metallic fuel assemblies using high assay low enriched uranium (HALEU)).
- X-Energy Xe-100 Reactor (high temperature gas cooled pebble bed reactor with fuel fabrication facility, 80 MWe, pebble fuel using HALEU).

Risk Reduction Award Winners:

- Kairos Hermes Reduced-Scale Test Reactor (supports fluoride salt cooled high temperature pebble bed reactor, HALEU fuel).
- Westinghouse eVinci Microreactor (1.6 MWe, solid fueled, heat pipe cooled, HALEU fuel).
- BWXT Advanced Nuclear Reactor (transportable microreactor, TRISO fuel in SiC matrix, HALEU fuel).
- Holtec SMR-160 Reactor (light water cooled SMR, 160 MWe, low enriched uranium (LEU) fuel).
- Southern Company & Terrapower Molten Chloride Reactor Experiment (fast spectrum precursor to the Molten Chloride Fast Reactor design, HALEU fuel).

Advanced Reactor Concepts-20 Program Award Winners:

- Advanced Reactor Concepts Inherently Safe Advanced SMR (100 MWe sodium cooled reactor).
- General Atomics Fast Modular Reactor Conceptual Design (50 MWe, fast spectrum, helium cooled, 9 year fuel life).
- Massachusetts Institute of Technology Horizontal Compact High Temperature Gas Reactor.

Advanced Reactor Vendors in Licensing or Pre-licensing activities with NRC:

- NuScale Integral Pressurized Water Reactor (NRC design certification in 2022).
- Holtec SMR-160 Pressurized Water Reactor
- GE-Hitachi BWRX-300 Boiling Water Reactor
- General Atomics EM^2 Helium Cooled Fast Reactor
- Kairos Power Fluoride High Temperature Reactor
- Terrapower Natrium Sodium Fast Reactor
- Westinghouse eVinci Microreactor
- Terrestrial Energy Integral Molten Salt Reactor
- X-Energy Xe-100 Pebble Bed Reactor
- Terrapower Molten Chloride Fast Reactor
- General Atomics Helium Cooled Fast Modular Reactor

- ARC Clean Technology Sodium Fast Reactor
- Oklo Aurora Powerhouse
- Ultra Safe Nuclear Corporation and University of Illinois High Temperature Gas Test Reactor
- University of Illinois & Ultrasafe Micro Modular Reactor Helium Fast Reactor
- Radiant Industries Kaleidos Microreactor
- Abilene Christian University Molten Salt Research Reactor

The following sections describe the five key thrust areas of the ARSS program, which are listed below. The existing research is outlined with a focus on expected benefit and key outcomes. The path forward over the next five years is also discussed.

1. Develop Next Generation Physical Protection Systems and Approaches
2. Develop MC&A Approaches for Pebble Bed and Liquid-Fueled Molten Salt Reactors
3. Provide R&D Support for Unique Deployment of SMRs and Microreactors
4. Develop Cyber Informed Engineering Approaches and Apply Cybersecurity Technologies to Advanced Nuclear Systems
5. Examine International Interfaces

3. DEVELOP NEXT GENERATION PHYSICAL PROTECTION SYSTEMS AND APPROACHES

The existing regulatory structure pertaining to physical protection for licensing of new nuclear reactors is outlined in the U.S. Code of Federal Regulations (CFR), 10 CFR Part 73. These regulations were originally written to support large LWRs and so were not designed for advanced reactors and smaller designs. NRC has spent much effort re-evaluating the applicability of the regulations over the past decade given the increasing interest in small modular, advanced, and microreactor designs.

In particular, the traditional requirement for large numbers of on-site responders may not be appropriate for smaller designs. While maintaining a larger protective force on-site can be absorbed in the cost for large power producers, equivalent on-site responders may be both inappropriate and cost-prohibitive for smaller reactors. Insider threat mitigation must also be considered in PPS design, and potential impacts due to smaller protective forces should be assessed.

PPS technologies are constantly improving. New technologies, increased automation, and improvements in machine learning and artificial intelligence allow for new or modified protection strategies compared to the current fleet. This is balanced by the fact that new technologies also change the threat landscape and advanced reactors may be part of new deployment strategies possibly coupled with fuel cycle facilities. PPS designs need to be robust, yet flexible to anticipate changing future threats. Security by Design is a key goal in the development of PPSs—security needs to be considered early in the design process so that costly facility retrofits or operational contingencies are not needed later, and the initial security system design can be as cost-efficient as possible. Further, the cyber threat continues to expand with time, so PPS approaches must also consider cyber-physical attacks and develop more integrated approaches for cybersecurity and PPS.

The ARSS program is providing guidance to vendors to help develop a robust and cost-effective PPS. This goal spans all vendors, but specific implementation will vary based on reactor size and design. There are three focus areas within this goal:

- Reduce total security staffing size while demonstrating high PPS system effectiveness.
- Evaluate new detection, delay, and response technologies.
- Develop PPS designs as part of a 3SBD approach.

3.1. Reduce Staffing Size while Demonstrating High PPS System Effectiveness

Cost-effective security systems are a key need for advanced reactor vendors. The ARSS program has and continues to evaluate reductions in overall security staffing since it may be a significant contributor to long-term operational costs. Reductions in staffing could require exemptions using the current licensing process (if meeting 10 CFR part 73.55). The goal of this work is to present new approaches and performance metrics to validate the PPS designs for vendors to consider when designing their security plan. This R&D can also help inform regulatory decision makers about PPS designs more tailored for small and advanced reactor designs.

Program work to date has developed hypothetical physical security models for an integral Pressurized Water Reactor (iPWR), Pebble Bed Reactor (PBR), Sodium Fast Reactor (SFR), microreactor, and Molten Salt Reactor (MSR). 2D and 3D models of the facilities were developed to explore different PPS approaches with next-generation protection systems and response force strategies. Path analysis, force-on-force adversary modeling, and tabletop exercises have been used to explore new approaches that consider changes to the building and layout early in the design process to develop a much more efficient and effective PPS. Other related R&D in the program is being integrated into the modeling efforts including advanced detection, delay, and response technologies as well as attention to where integration with safety, MC&A, and cybersecurity will provide advantages.

Figures 2, 3, 4, 5, and 6 show the generic models that cover a range of advanced reactor designs. Lessons learned from previous iterations are being incorporated into all designs to provide security by design recommendations for vendors.

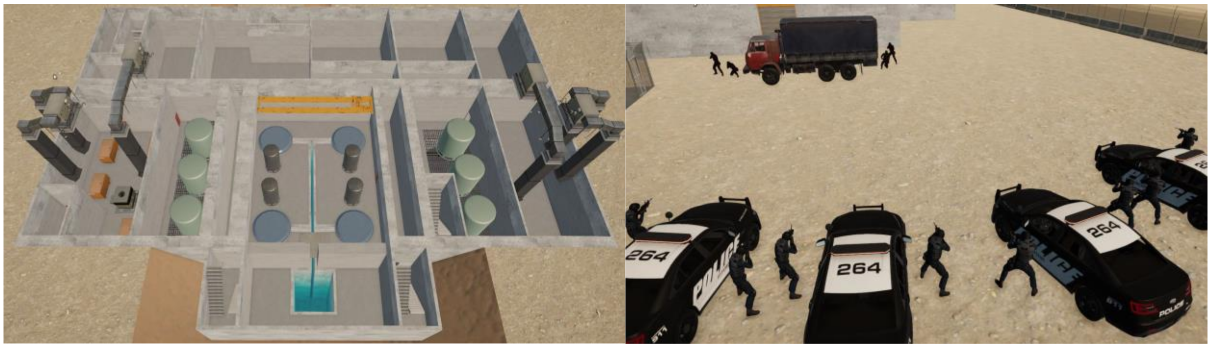

Figure 2: Pressurized Water SMR PPS Model[5]

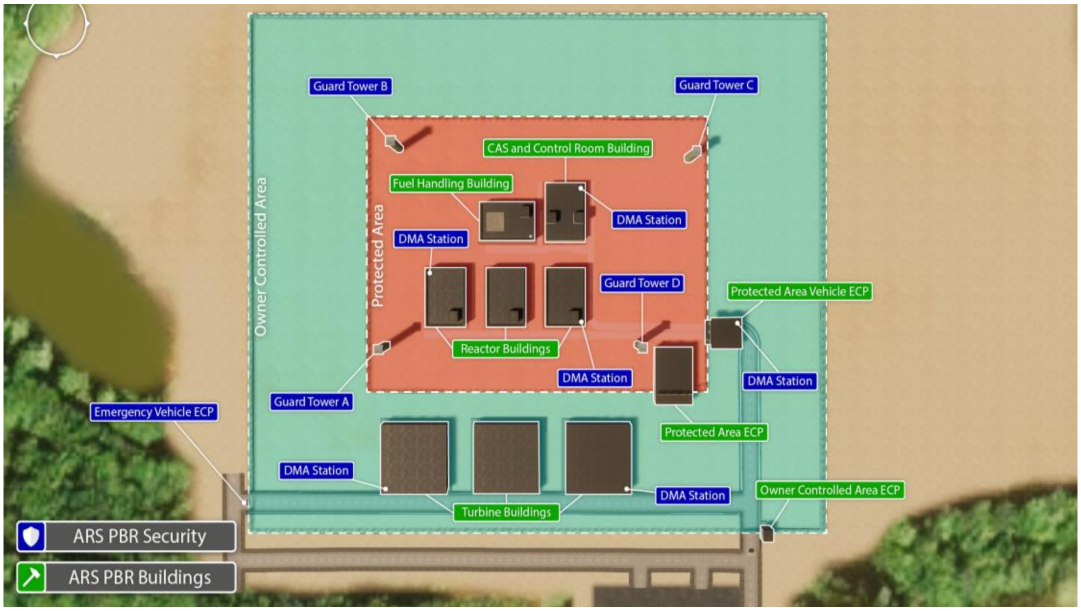

Figure 3: Pebble Bed Reactor PPS Model[6]

[5] A.S. Evans et al., "U.S. Domestic Small Modular Reactor Security by Design," Sandia National Laboratories SAND2021-0768 (January 2021).

[6] A. Evans et al., "U.S. Domestic Pebble Bed Reactor Security-by-Design," Sandia National Laboratories SAND2021-13122R (October 2021).

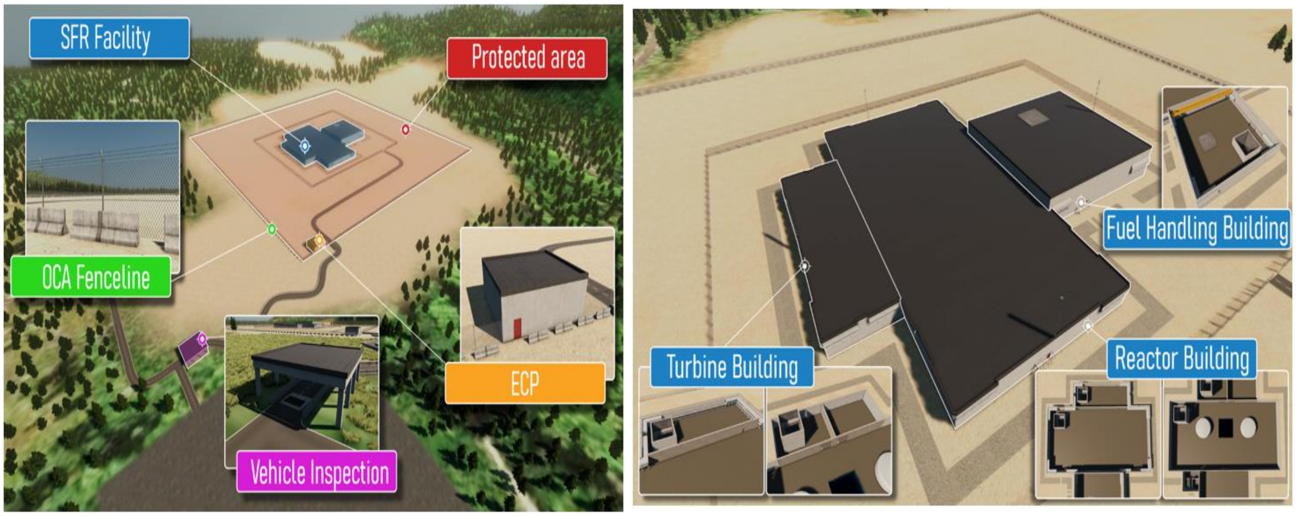

Figure 4: Sodium Fast Reactor PPS Model[7]

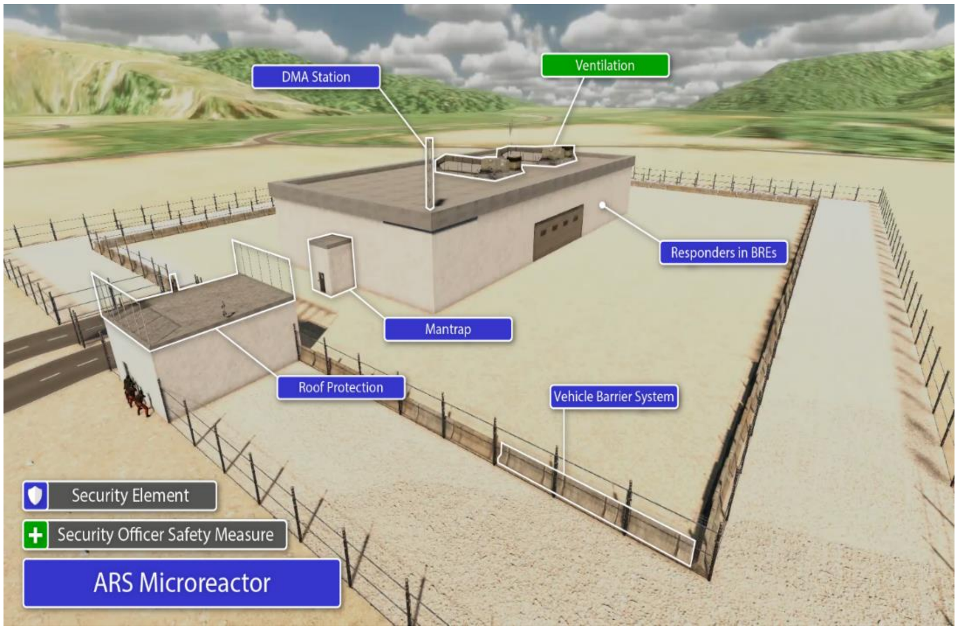

Figure 5: Microreactor PPS Model[8]

[7] A. Evans et al., "U.S. Domestic Sodium Fast Reactor: Security by Design," Sandia National Laboratories SAND2023-09146R (September 2023).

[8] A. Evans et al., "U.S. Domestic Microreactor Security-by-Design," Sandia National Laboratories SAND2021-13779R (October 2021).

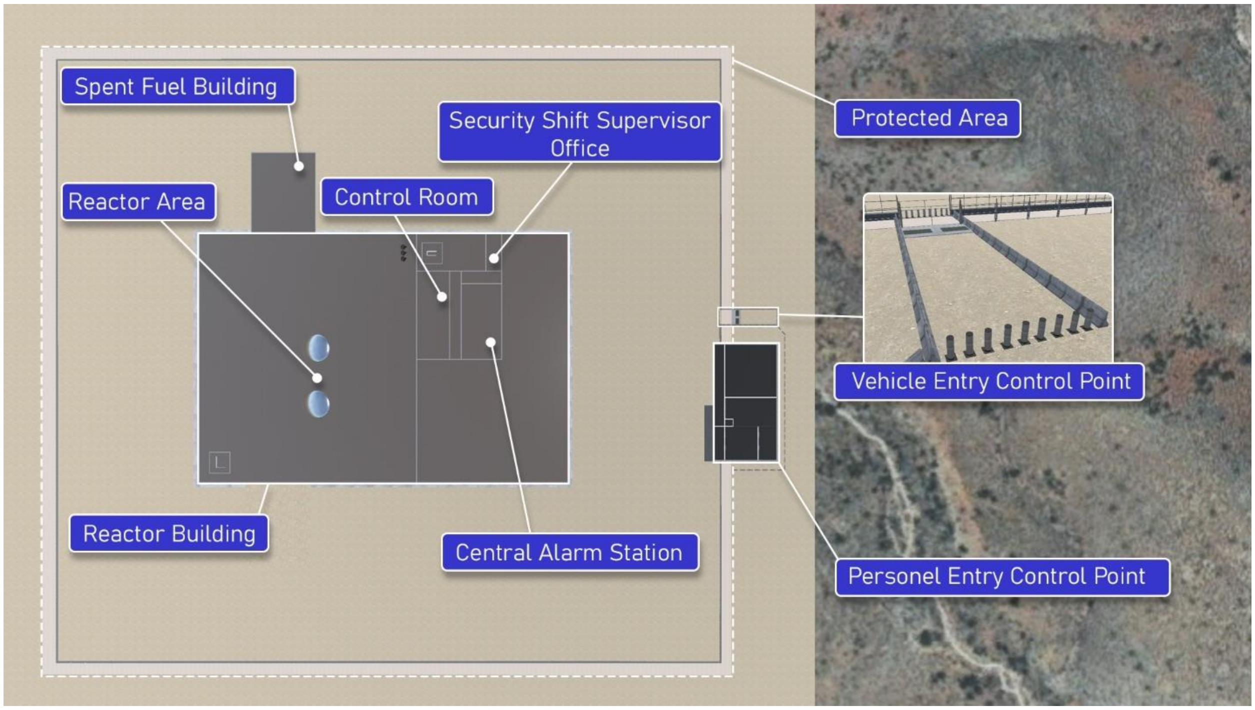

Figure 6: Molten Salt Reactor PPS Model[9]

It is important to note that the modeling work supported through the ARSS program is meant to be used for R&D to provide new options for the vendor community. The results generated would only be used to inform designs submitted to NRC for licensing, and nuclear reactor vendors will need to perform analysis independently unique to their reactor and site designs. Vendors may develop these capabilities internally or utilize contractors who specialize in PPS analysis for the license application.

Vendor engagements help to validate the work in the ARSS program. These engagements are carried out under non-disclosure agreements to protect any proprietary or sensitive information. In the PPS space, vendor engagements to date have focused on reviewing PPS designs and providing recommendations to reduce staffing and improve security by design. All vendor engagement work provides a document on generic lessons learned for the full community along with work specific to that vendor design. In some cases, the vendor engagements are being carried out in partnership with National Nuclear Security Administration (NNSA) programs to develop a more complete SSBD approach.

The R&D on PPS design to date has already generated a number of security by design recommendations which will be summarized here:

1) Use of off-site response by local law enforcement is not recommended since it likely will not provide cost savings and leads to the need for extensive delay technologies.
2) Below grade reactors are slightly more expensive but allow responders in the building ground floor. Above grade reactors may require guard towers. Additionally, below-grade reactors may provide more resilience to large vehicle-borne explosive devices or other explosive devices used by an adversary.

[9] A. Evans et al., "U.S. Domestic Molten Salt Reactor: Security by Design," Sandia National Laboratories SAND2024-07607R (June 2024).

3) Optimal building design should include one square or rectangular building with all facilities and critical targets contained within for ease of protection. Multiple modules on site should consider avoiding multiple buildings.
4) Blast and bullet resistant enclosures (BBREs) in the corners of the buildings (hardened fighting positions that allow fighting externally and internally) are preferred over guard towers since they give responders more flexibility.
5) Shark cages or man traps should be utilized on all entrances/exits to the building to provide more delay time for adversaries trying to enter the building.
6) The turbine halls should be included in the protected area to protect the plant investment.
7) A hatch or roof plug is preferred for moving equipment in and out as opposed to large high-bay doors.
8) Ankle breaking rocks should be utilized in strategic locations around the building (i.e. after fence lines or at the edge of buildings) to provide additional delay time.

Path Forward

Future work will continuously refine the different reactor models considering lessons learned from previous work. In the near term, definitive design recommendations for on-site security staffing will be described for different types of sites considering differences between first-of-a-kind and nth-of-a-kind deployment. This work will also include a security plan that describes the needs for compensatory measures and more fully describes the numbers of security staffing required when considering the number of shifts, time off, workers calling in sick, etc.

Future work will also tie in related program R&D on sabotage targets for advanced reactors, integrated MC&A and physical protection analyses, and integrated cyber-physical analyses. Within five years, the program envisions an overall plant protection system design and best practices document for each reactor class that provides a 3SBD approach. These documents will cover MC&A, PPS, and cybersecurity design for each reactor class.

Vendor engagements will continue to be used to validate the program work. Existing engagements will likely wrap up as PPS designs near completion, but the ARSS program maintains additional budget to work with new vendors as requested.

3.2. Evaluate New Detection, Delay, and Response Technologies

PPS analysis considers state-of-the-art technologies for detection, delay, and response. Many of these technologies have been developed in other programs and so may not require additional R&D but are being considered as options in the PPS design. Detection technologies include Perimeter Intrusion Detection and Assessment Systems (PIDAS—a combination of microwave sensors and cameras), radar, lidar, infrared systems, and advanced sensor fusion algorithms. Delay technologies include additional barriers, man-traps, hardened doors, dispensable barriers, etc. Response technologies may include proper placement of hardened fighting positions and remote operated weapons systems (ROWS).

The ARSS program is helping to develop Deliberate Motion Analytics (DMA) as a detection technology that can potentially save a nuclear facility considerable cost.[10] DMA is a sensor fusion

[10] J.R. Russell et al., "Deliberate Motion Analytics Fused Radar and Video Test Results," Sandia National Laboratories, SAND2021-5413 (April 2021)

algorithm designed for high security applications that uses deliberate target motion to differentiate alarms caused by an intruder from those caused by other natural sources. It is capable of fusing multiple sensors, such as radar, lidar, and video, to provide superior detection with low false positive rates. DMA naturally leverages the power of complementary sensors in its algorithm. Since a PIDAS can lead to very high upfront security costs, the potential replacement with a technology like DMA can save costs while increasing detection radius. Figure 7 demonstrates the simplicity of DMA as compared to traditional approaches which require many sensors and more fencing.

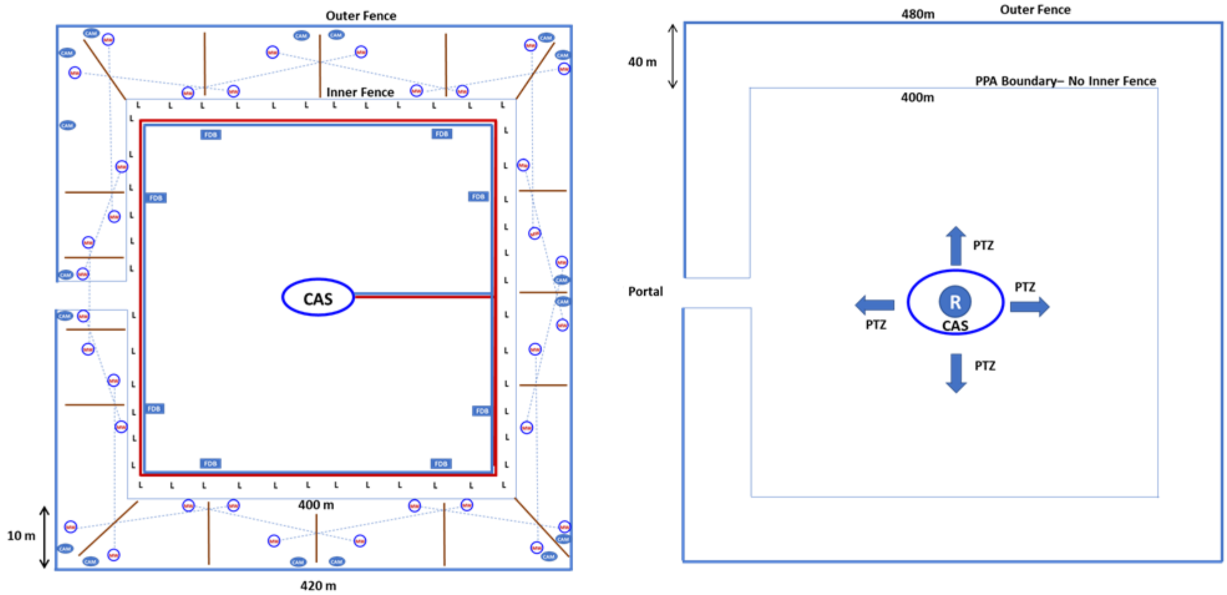

Figure 7: Traditional PIDAS Design (Left) Compared to DMA System (Right)

Current work on DMA is evaluating a DMA enabled PIDAS design, simulating an SMR site that is 180m by 180 meters. Figure 8 shows an aerial view of the test site. The centrally located radar and imager system (Radar Bi-Spectral Pan Tilt Zoom Module – RPM) shown in Figure 8 has demonstrated that it can provide reliable detection with a low nuisance alarm rate.[11] Significant cost saving from this architecture are due to elements of the simplistic architecture such as, no power or comms are needed at the perimeter, no trenching is required, and no lights are required to image an intruder because of the use of thermal imagery.

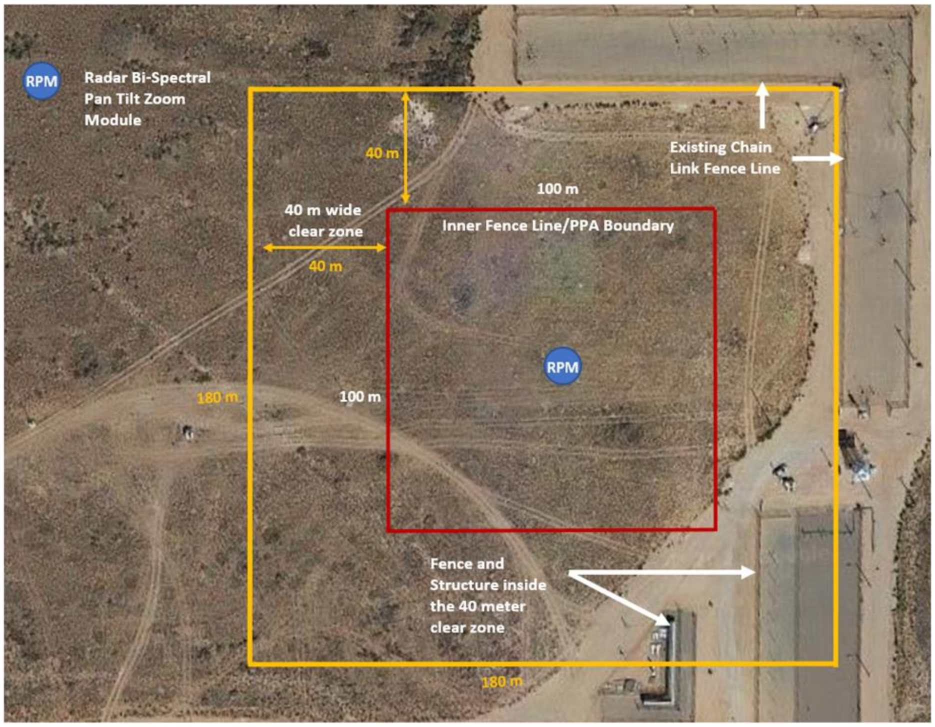

Figure 8: Test Bed Simulating an SMR Site Employing a DMA Design

SMR and microreactor sites are going to be much smaller than what has been typical of large LWR sites. As such, the distance between the site boundary and key buildings is smaller. Delay technologies may be more important for these sites to give responders more time to muster in the event of an adversary attack. Current work is providing data to vendors on delay technologies and performance for consideration in their PPS designs. These technologies are also being incorporated into path analysis and force-on-force adversary modeling to increase overall system effectiveness or help optimize the overall PPS design.

Remote Operated Weapons Systems (ROWS) can provide a force multiplier to protect critical targets. Industry and related R&D efforts have supported development of ROWS, and it's use is being considered as part of the modeling and simulation work. Current work is continuing to evaluate the use of ROWS for advanced reactors and generate a better understanding of its potential use cases for different designs. The use of ROWS for advanced reactors may be unique—small sites might preclude

[11] J.R. Russell et al., "Multi-Sector, Multi-Intruder Test Results for a DMA enabled PIDS (DPIDS)", Sandia National Laboratories, SAND2024-01437R (January 2024).

its use in external systems but might provide value internally to protect key pathways to targets as a final denial system.

Path Forward

In future work, DMA is showing a great deal of promise as a new PPS detection technology. In the near term, DMA will continue to be tested in configurations more typical of an SMR or microreactor and in different terrains. Near term work is also extending the use of DMA to detection of Unmanned Aerial Vehicles (UAVs) to provide 2π detection for intrusion onto any nuclear site via land or air. Future work will move toward piloting studies on a demonstration facility or with vendor partners. Future work also must consider how DMA can fit into the current NRC licensing process.

Future work on delay technologies will focus on technology recommendations for vendors and those technologies that provide the most value. ROWS and related concepts will continue to be explored in the modeling space to determine impact on advanced reactor PPS designs.

3.3. Develop PPS Designs that Integrate Safety, MC&A, and Cybersecurity

Advanced and small reactors have a unique opportunity to take an integrated approach to 3SBD. Enhanced safety systems may provide a benefit to physical security. Reactors that move away from large fuel assemblies may have nuclear material accountancy challenges that can be mitigated through better integration with physical protection. The cyber threat is constantly evolving, so cyber-physical attacks need to be considered.

The NRC is currently in a rule-making effort that may allow advanced reactors to take credit for enhanced safety systems.[12] The proposed rule-making allows the vendor to develop an alternative approach if radiological consequence results in low-enough off-site dose, the design prevents an adversary from compromising mitigating features, or if inherent reactor characteristics and engineered safety and security features maintain radiological consequences below a threshold given a potential attack. The approach may include alternatives to physical barriers, allowance of an off-site secondary alarm station, and relief from the prescriptive requirement for the minimum number of armed responders.

Sabotage analysis is being carried out to determine if the use of new coolants and fuels presents new attack pathways for the adversary. Recent work has examined sabotage pathways for microreactors, PBRs, SFRs, and MSRs. This work is helping to inform the PPS design to ensure that additional adversary targets are protected at an appropriate level.

There may be attack scenarios where the timeline for damage to the fuel or core may become important from a physical security perspective. While in general the PPS approach will be to prevent an adversary from reaching the reactor, spent fuel, control systems, and other vital systems, there may be attack pathways that can remove decay heat cooling. Long timelines before accidents occur can allow reliance on off-site response in these unique scenarios. Advanced reactors also need to consider unique sabotage targets through the use of different coolants, fuels, and safety systems. These are areas where an integrated safety-security approach is needed.

Current R&D is beginning to evaluate nuclear material diversion pathway analysis for different classes of advanced reactors including the pebble bed reactor (PBR) and liquid fueled MSR designs. These reactors will have more challenges in how MC&A is accomplished and will likely rely more on physical

[12] NRC Preliminary Proposed Rule Language Part 73 of Title 10 of the Code of Federal Regulations [NRC-2017-0227], available at https://www.nrc.gov/docs/ML2018/ML20182A157.pdf (2021).

protection and containment/surveillance as part of an overall protection approach. Diversion pathway analysis may be utilized to evaluate the integration of MC&A with physical protection.

The cyber threat continues to evolve at a rapid pace. The impact of cyber security attacks can hinder the ability of the reactor control systems and the PPS. As advanced reactors look to remote monitoring and remote operation, the impact of a cyberattack needs to be evaluated. Current research is evaluating cyber-physical attacks to cover the likely threat space more adequately in the future.

Path Forward

Over the next five years, safety and security will be coupled more tightly to better inform the design of a reactor's PPS. Accident sequence timelines will be used to inform sabotage scenarios, both to determine the consequence of a particular sequence of actions and how long the plant operators would have to recover after neutralization of the attack. These insights will then be used to enhance design trade-offs between economics and security. Consideration of unique sabotage targets will be factored into the overall analysis. The integrated safety and security approach should move toward industry and NRC feedback and adoption, starting with the more near-term advanced reactor vendors. In future work, the sabotage targets and vulnerabilities for specific reactor classes will be developed in more detail. As noted above, this work will feed into the design and analysis of the PPS.

Over the next five years, the integration of security and MC&A will also be evaluated when needed. Challenges in this space do not occur for all advanced reactors, but diversion pathway analysis maybe needed in some cases. Future work will also see a higher degree of coordination with the cyber security work in ARSS to develop protection systems robust to physical and cyber-attacks.

4. DEVELOP MC&A APPROACHES FOR PEBBLE BED AND LIQUID-FUELED MOLTEN SALT REACTORS

The existing regulatory structure pertaining to MC&A for licensing of nuclear reactors is outlined in the U.S. Code of Federal Regulations (CFR), 10 CFR Part 50, while MC&A for fuel cycle facilities is outlined in 10 CFR Part 74. Aspects of Part 74 may be utilized in the licensing of advanced reactors that do not have solid fuel assemblies, but in general the regulations were not developed for advanced reactors.

Pebble bed reactors (PBRs), which use Tri-structural Isotropic (TRISO) fuel embedded in graphite pebbles, are one class of advanced reactors. The operation of PBRs, with proposed constant refueling of pebbles and a TRISO fuel form, present accounting challenges as compared to traditional LWRs and their fixed fuel assemblies. These challenges stem from a much smaller fuel form that cannot be tracked individually.

Liquid-fueled molten salt reactors (MSRs) have unique features that result in additional MC&A challenges. Some aspects of MSRs are similar to bulk processing facilities since the SNM is not contained in discrete fuel assemblies and instead contained in a molten salt. Existing NRC MC&A approaches for bulk processing facilities like enrichment, fuel fabrication, and reprocessing are not directly applicable to liquid-fueled MSRs but may be used to inform an MC&A approach.

The ARSS program is addressing both the MC&A approach and new technologies that may help with accounting for both PBRs and MSRs.

4.1. Pebble Bed Reactors

Recent work in the ARSS program completed a major milestone report that outlines the full MC&A approach for PBRs, but there are still several areas that need additional R&D.[13] Figure 9 shows an overview of the MC&A approach which assumes one overall Material Balance Area (MBA) that will likely be subdivided into sub-MBAs or item control areas. Flow Key Measurement Points (FKMPs) and Inventory Key Measurement Points (IKMPs) are shown in Figure 9.

Reasonable progress has been made on packaging and handling for both fresh and spent fuel. Some of the reactor vendors have current design efforts underway to increase the capacity of spent fuel containers. For pebble counting and indexing systems, which will be critical to accurate physical inventories of the reactor vessel, vendors are still designing and testing these systems. For the reactor inventory approach, a much more detailed discussion is needed to integrate operations, safeguards, and security requirements. The pebble handling system also includes burnup measurements, pebble counting systems, a pebble integrity check, and possibly a batch identification measurement (but this could be combined with other measurements).

[13] D. Kovacic et al., "Nuclear Material Control & Accounting for Pebble Bed Reactors," Oak Ridge National Laboratory, ORNL/SPR-2023/2988 (December 2023).

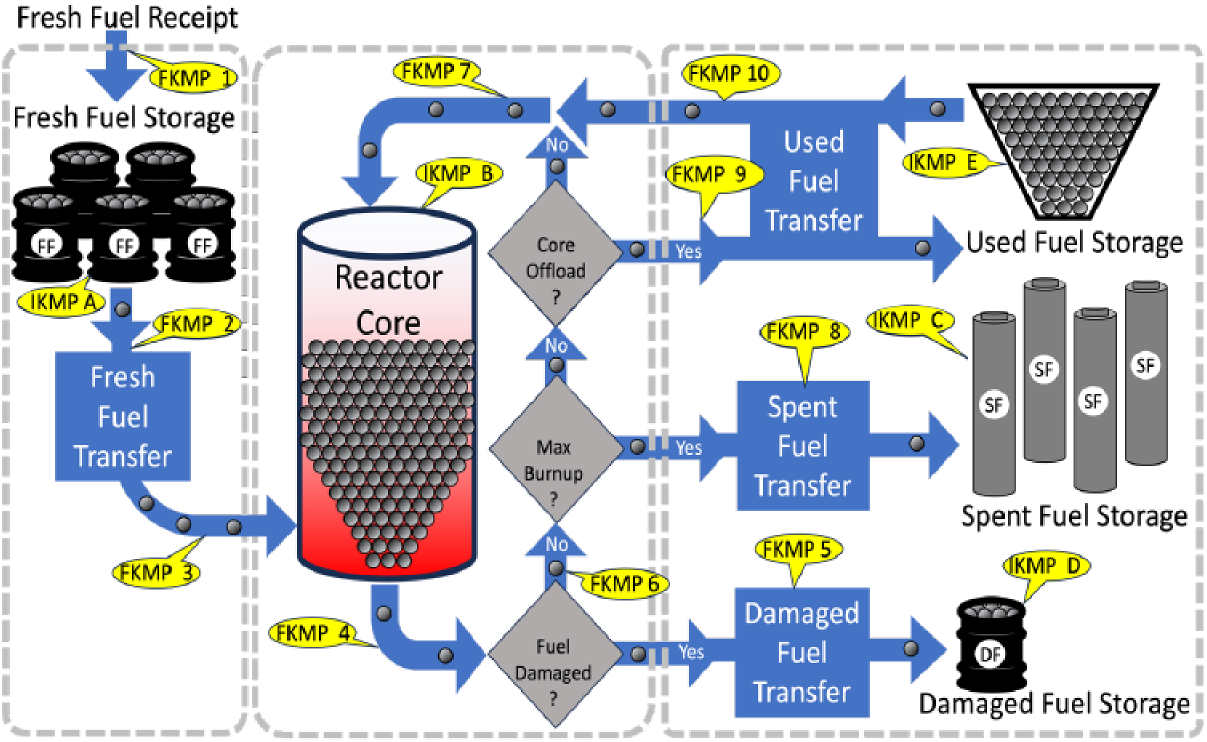

Figure 9: Material Balance Area (MBA) Structure for PBRs

PBRs will not track the nuclear material in each pebble since the quantity of nuclear material per pebble is very small. MC&A will be performed on a canister basis since many pebbles are required to accumulate a NRC formula quantity. Reactor codes, as with LWRs, are traditionally acceptable for estimating fissile content. However, the operator needs to measure burnup in order to better utilize the fuel. They have a strong economic incentive to recycle the pebbles until their burnup limit is reached, and the burnup (and corresponding nuclear material content) will vary depending on the path the pebble takes in the core. There also may be interest in batch identification for pebbles of different enrichments and/or to help keep track of the number of passes better.

ARSS research is supporting pebble burnup measurements. This measurement is important for operations since it determines if a pebble can be recycled or if it has surpassed a burnup limit, but it can also be used for MC&A declarations and to validate reactor codes which will be the primary source of information on fissile content. Current work is focused on understanding the fundamental capabilities of nondestructive gamma spectroscopy with high-resolution (HPGe) and ultra-high resolution (microcalorimeter) detectors through measurements of irradiated TRISO materials. Results confirm that the Cs-134/137 ratio measured with HPGe detectors can be used to estimate burnup as with LWR fuels. A new capability that has been demonstrated is direct quantification of the U/Pu element ratio using fluoresced U/Pu K X-rays measured with a microcalorimeter spectrometer (Figure 10).[14] This ratio is an important safeguards signature and is strongly correlated with burnup. While this method has been proposed for LWR fuels, TRISO fuels have favorable properties that make fluoresced U/Pu X-rays a more quantitative metric of burnup and average pebble composition. This

[14] M. Croce et al., "NDA of TRISO Fuels," Los Alamos National Laboratory LA-UR-23-32266 (October 2023).

is primarily due to the fact that uranium in a fuel pebble is distributed in small particles throughout a graphite matrix with much less attenuation within the particles than in larger conventional fuel pellets. Additional signatures of burnup and irradiation timeline may be visible as well in fuel pebbles shortly after removal from the reactor core from fission product gamma rays.

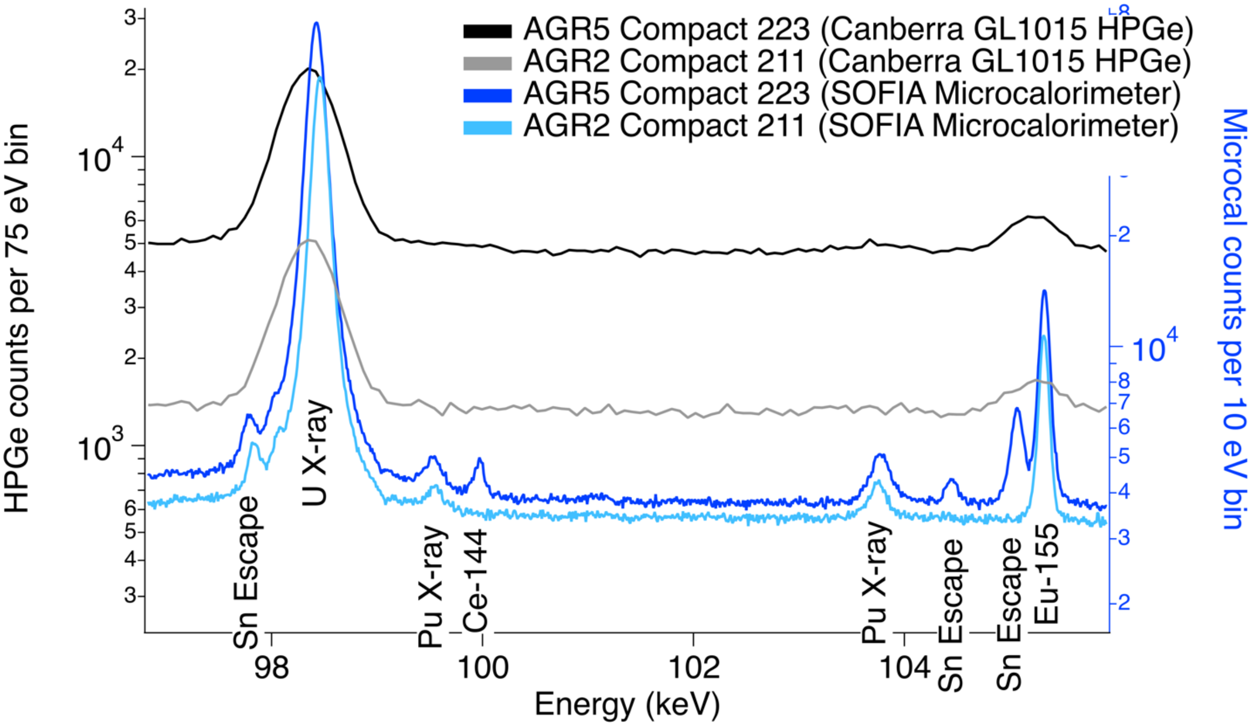

Figure 10: Fluoresced U and Pu X-rays Visible in Ultra-High Resolution Gamma Spectra of High-Burnup TRISO Compacts

Machine Learning (ML) approaches are being evaluated to improve the burnup measurement results for reduced uncertainty. Previous work[15] has shown that the ML algorithm learns based on the full gamma spectra and can determine burnup to lower uncertainty than peak ratio correlations alone. Figure 11 shows an example of a simulated gamma spectra—simulations of a variety of burnups, cooling times, and acquisition times have been generated to determine how ML approaches can help.

[15] Y. Cui et al., "Use Machine Learning to Improve Burnup Measurement in Pebble Bed Reactors," Brookhaven National Laboratory, BNL-222200-2021-FORE (September 2021).

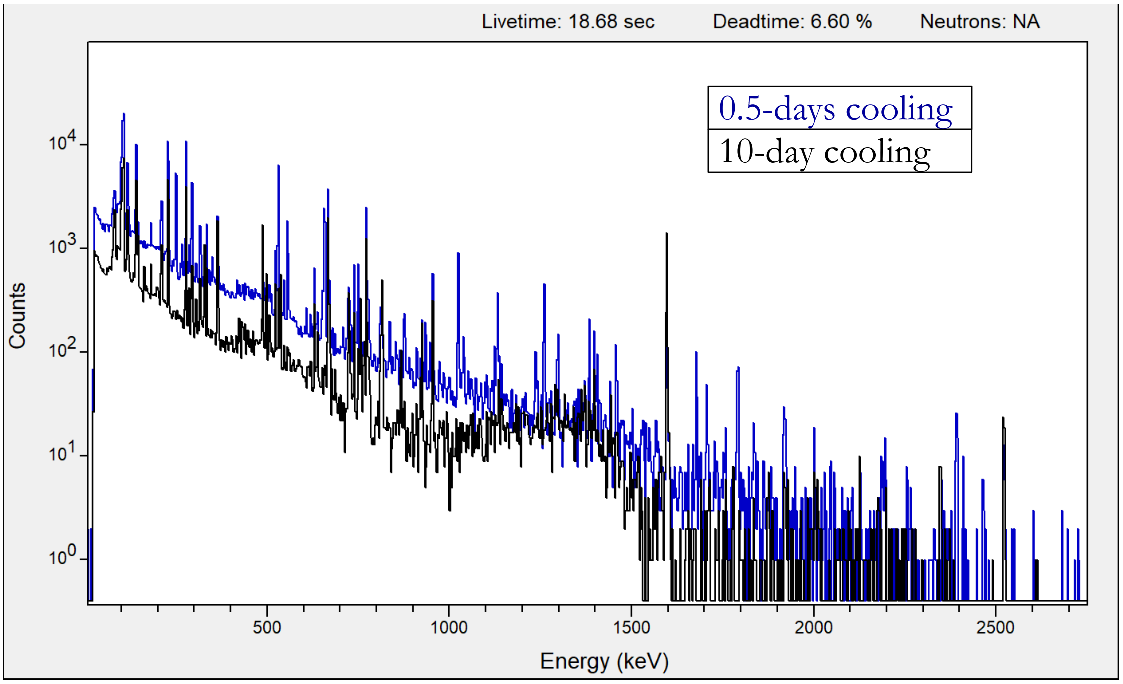

Figure 11: Simulated Gamma Spectra from a Pebble with a 20 Second Acquisition Time

The initial estimations of fissile content in the discharged pebbles by both the neutronics code and fuel burnup measurements are expected to be reasonable. However, these estimations will have opportunities for improvement if there is a better understanding of the parameters and assumptions, which are most sensitive to the variabilities of fuel burnup and residual fissile content in the discharged pebbles. Sensitivity studies were conducted to investigate how minor perturbation of parameters, such as fuel temperature, neutron flux (or specific power), initial ^{235}U enrichment, and residence time, will affect the parameters of interest for MC&A aspects of nuclear security and safeguards of PBRs. The parameters of interest are fuel burnup and residual masses of ^{235}U, ^{239}Pu, and total Pu in the discharged fuel pebbles. Such an understanding of parametric uncertainties and their effects can inform PBR modelers and designers as to where to target improvements for more accurate values for the parameters of interest in the discharged pebbles. Sensitivity studies targeting uncertainty estimation can support MC&A of discharged pebbles stored in used fuel canisters.

Past work has examined different options for batch identification of pebbles. Current work is evaluating eddy current and infrared scanning, respectively, to develop a dry pebble identification and integrity assessment method. The eddy current method utilizes the surface features (engineered or due to damage) to identify a pebble's batch. Infrared scanning is being evaluated for identifying features within the outer 5mm layer of graphite using the inherent heat signature sourced from the pebble's interior.

Path Forward

In future work, integration of PBR modeling and simulation features into current reactor codes and validation of spent fuel measurements is likely to be an on-going effort. As models of the PBR cores are developed, they will inform measurement system selection and design. Gamma measurements are preferred, but uncertainty quantification needs to be determined for very short-cooled fuel. While burnup of each pebble is the key measurement, estimation of U and Pu is also important for accounting. Over the next five years, the ARSS program will team with related programs in DOE NE to validate burnup measurements through experimental measurements of short-cooled irradiated

TRISO fuel. Once the observable burnup signatures are sufficiently understood, a plan for implementation of nondestructive assay technologies will be developed.

ML approaches will continue to be evaluated focusing on the realism of the data and generating realistic spreads. More work is required to understand if there are specific peaks or areas of the spectra that are dominant in the algorithm. In the next 3-5 years, application to real spectra on irradiated TRISO fuel or pebbles will be evaluated.

For the eddy current and infrared scanning technologies for pebble defect measurements, researchers are working collaboratively with vendors to determine needs and fit into the planned pebble handling systems. Successful technology demonstration will be needed before vendors can consider incorporating into their systems.

4.2. Liquid-Fueled Molten Salt Reactors

MC&A approaches for existing LWRs and bulk processing facilities are not directly applicable to liquid-fueled MSRs due to the flowing nature of the fuel. Research is required to determine (1) appropriate MC&A approaches, (2) how MC&A might be met using different measurement methods, and (3) evaluating the potential applications and limitations of existing measurement technology on materials and process streams within MSRs.

Similar to all reactors, actinide content in MSRs are changing when operating since plutonium (or, in a limited number of designs uranium-233) quantities build up over time and uranium-235 quantities decrease over time due to burnup. The difference is the use of liquid molten salt fuel which is more difficult to track than discreet fuel assemblies. The liquid fuel is inaccessible due to very high radiation levels, high temperatures, and biological shielding around the nuclear reactor system. MSR systems may also include online fuel reconditioning, which can complicate MC&A approaches due to the combination of two traditional facility types into one (i.e. reprocessing and reactor). The technical work supporting this focus area is divided into development of the MC&A approach and measurement technologies that may be used as part of the approach.

Recent work has developed an overall MC&A approach for liquid-fueled MSRs.[16] Figure 12 outlines the Material Balance Area (MBA) structure at a high level for MSRs, which includes performing periodic inventories at the front end (MBA 1) and back end (MBA 3) and relying on monitoring to detect diversion in MBA 2. Periodic inventories will likely be worked into the MC&A plan, but there will be limits as to how well accounting can work given the large quantities of actinides and complex reactor loop geometry.

[16] K.K. Hogue et al., "Planning for Material Control and Accounting at Liquid-Fueled Molten Salt Reactors," ORNL/SPR-2023/3181, Oak Ridge National Laboratory (January 2024).

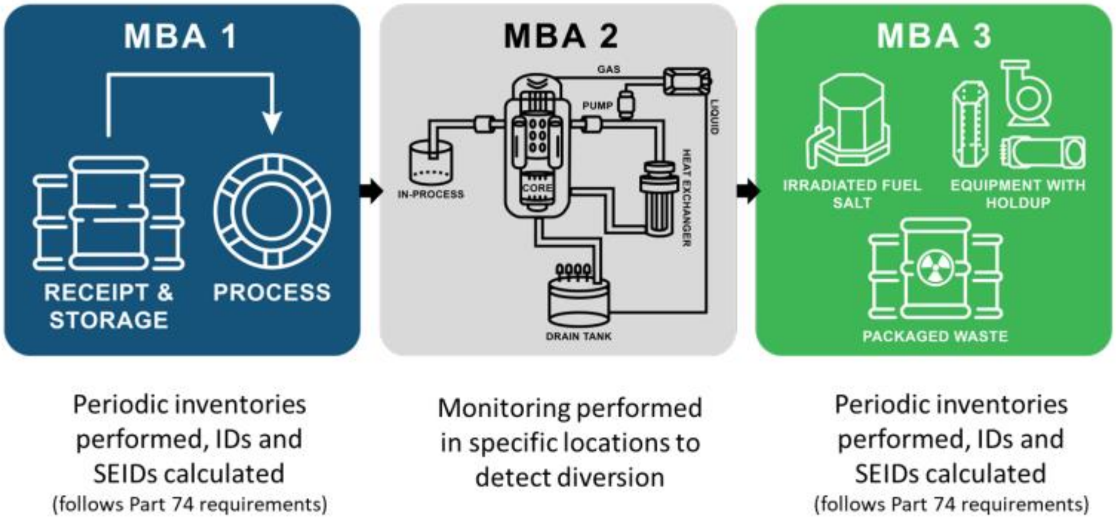
MBA 1
RECEIPT & STORAGE
PROCESS
MBA 2
GAS
PUMP
LIQUID
IN-PROCESS
CORE
HEAT EXCHANGER
DRAIN TANK
MBA 3
IRRADIATED FUEL SALT
EQUIPMENT WITH HOLDUP
PACKAGED WASTE
Periodic inventories performed, IDs and SEIDs calculated
(follows Part 74 requirements)
Monitoring performed in specific locations to detect diversion
Periodic inventories performed, IDs and SEIDs calculated
(follows Part 74 requirements)

Figure 12: MBA Structure for MSRs

Safeguards performance modeling has shown how proposed measurement systems can track nuclear material and detect material loss. Traditional inventory difference calculations, which are required for bulk handling facilities, show that even measurements using destructive analysis with uncertainties below 0.5% will still lead to overall absolute error much greater than one formula quantity (as defined by the U.S. NRC) or one significant quantity (as defined by the International Atomic Energy Agency). However, destructive, or non-destructive measurements could support validating reactor modeling and simulation codes. Hence, reliance on containment and surveillance, additional process monitoring measurements, and/or physical security will be needed to augment the material accounting measurements.

Vendor engagements help to validate the overall MC&A approach for MSRs. These engagements provide useful insight into the challenges being faced with new designs and with the current regulatory framework. As noted earlier, the vendor engagements are designed to produce a document describing generic lessons learned in addition to work more specific to the particular vendor design.

The ARSS program is also supporting research on measurement technologies that will be required for the MC&A approach. Initial guidance from the regulator has suggested that some type of actinide quantification in the molten salt will be needed. This type of measurement will have a dual use in that the operator also will need it for monitoring inventories for reactor control.

Optical spectroscopy-based monitoring tools are being developed to characterize the complex chemical systems anticipated in molten salt processes (see Figure 13).[17,18] The technology is mature and commercially available but has been adapted to the harsh molten salt environments. Current work is evaluating measurements with more complex systems and high actinide concentrations to be more representative of MSR systems.

[17] A. Lines et al., "On-line Monitoring for Molten Salt Reactor MC&A: Optical Spectroscopy-Based Approaches," Pacific Northwest National Laboratories, PNNL-31955 (September 2021).

[18] S. Branch, et al., "Exploring the Complex Chemistry of Uranium within Molten Chloride Salts" *Ind Eng Chem Res* **2023**, *62* (37), 14901–14909. DOI:10.1021/acs.iecr.3c02005.

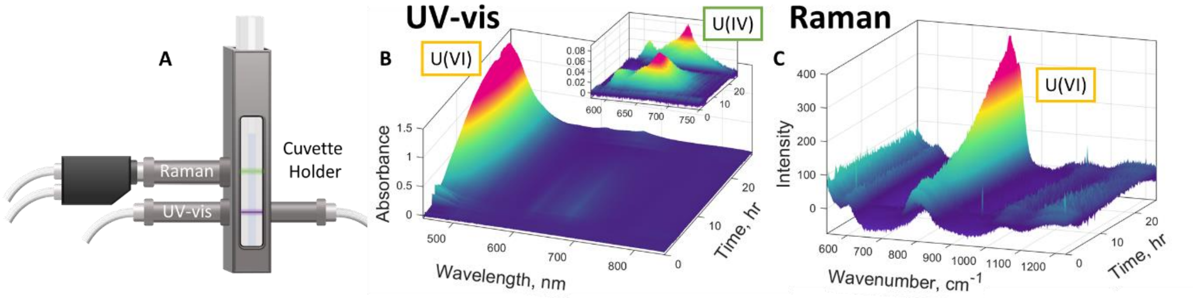

Figure 13: Optical Spectroscopy Setup Allowing Both UV-Vis Absorbance and Raman Spectral Interrogation

Expanding the understanding of analyte behavior within molten salts through chemometric analysis offers the opportunity to better understand the chemical behavior of molten salt reactors for the purpose of reactor operations as well as MC&A. Uranium disproportionation and chemical interactions are explored through optical techniques. First and foremost, this provides new and powerful insight into uranium sensitivity to oxidants present in salt melts while also expanding the understanding of uranium redox patterns within the chloride eutectics. This knowledge is highly valuable in the design and demonstration of MSR technology, providing engineers and vendors with insight in to needed levels of salt purification and redox control. Additionally, the optical monitoring techniques developed here can be leveraged to control molten salt processes and complete material accounting.

Flow tolerant electrochemical sensors to provide mass accountancy, corrosion, and salt health monitoring for MSRs are also being developed.[19] This flow tolerant electroanalytical approach makes use of hydrodynamic electrochemistry to provide the necessary salt composition and salt redox state measurements. The sensors will also measure the salt flow rate, which is essential to account for in-flows, outflows, and hold-up in MSR systems. This instrument is being tested on the Modular Flow Instrumentation Testbed (MFIT) at Argonne National Laboratory (shown in Figure 14), which was developed under the ARSS program. At present, the MFIT is the only forced-flow radiological molten salt system within the U.S. national laboratory complex.

[19] N. Hoyt, E. Stricker, and C. Moore, "Design and Construction Progress for the Modular Flow Instrumentation Testbed and Associated Sensors," Argonne National Laboratory, M3RS-20AN0401112 (September 2020).

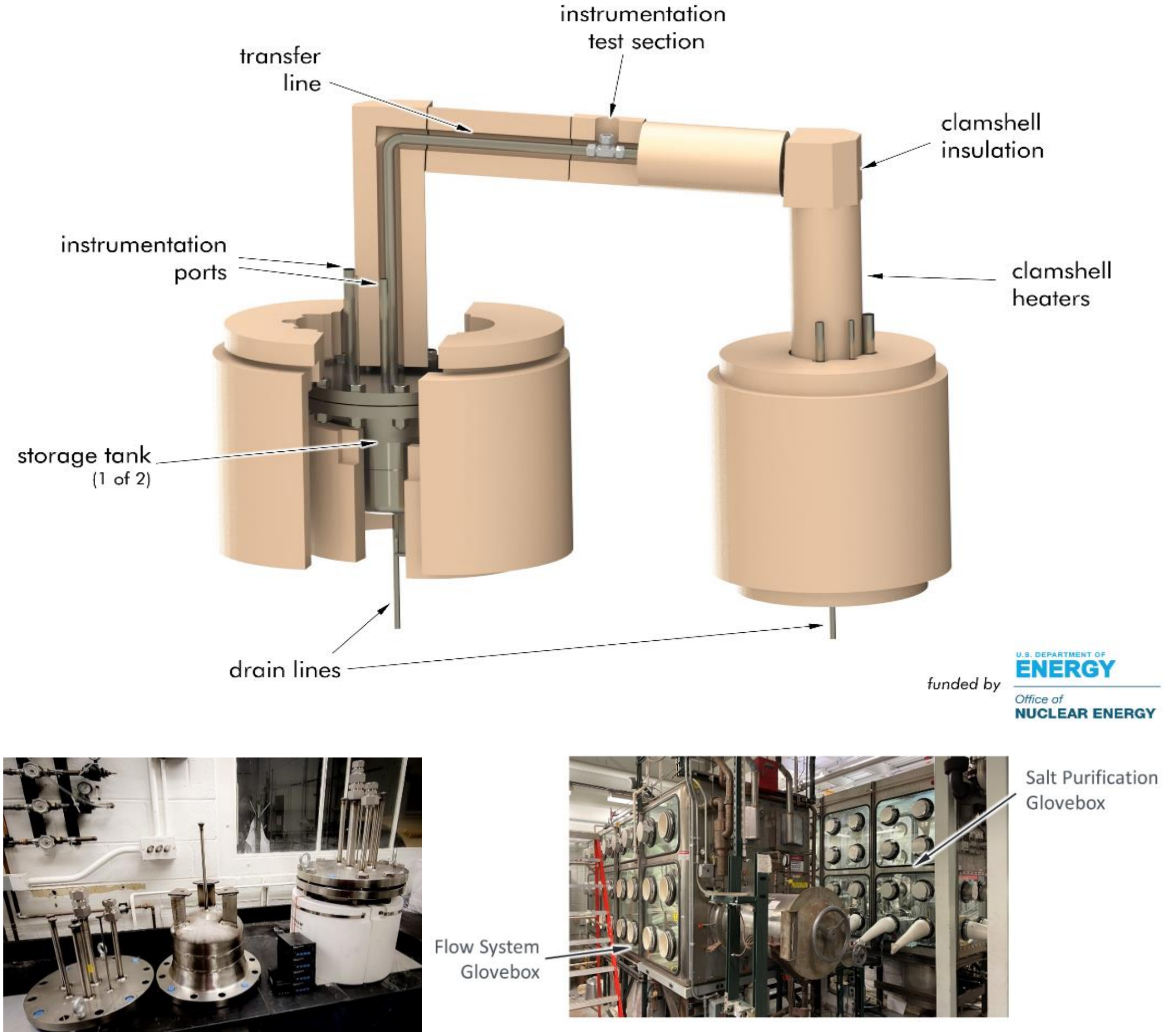

Figure 14: Modular Flow Instrumentation Testbed (MFIT) at Argonne National Laboratory. Rendering of the Platform (top), Storage Tanks and Associated Parts (Bottom Left), and Salt Purification and Flow System Glovebox (Bottom Right).

Apertures in the storage tanks and along the transfer line present many opportunities for testing of varied on-line, at-line, and off-line salt monitoring approaches, including salt samplers and particle monitoring sensors. The combined use and synthesis of data from multiple types of sensors will be important to resolve the material accounting challenges facing MSR-relevant systems. Beyond safeguards, the modularity of the MFIT design permits installation of complete test sections for examination of subsystems including chemistry control systems.

Industry is interested in both monitoring technologies and incorporating these technologies into their testing plans. Other technology solutions will be needed to quantify total salt mass/volume in an MSR for accounting.

Path Forward

Although the overall MC&A approach for MSRs has been defined, additional work is required on front-end and back-end operations including re-fueling and processing of off-gases, noble metals, and irradiated fuel salt and wastes, as well as further defining the overall MC&A approach by applying it to different case studies. Integrated solutions for MC&A, physical protection, and cyber should be considered. Due to limited data on expected material inventories and applicability of different measurement technologies, the MC&A declarations will depend on depletion tools to accurately model inventories in the system. These tools will need to be validated against real systems once they become available.

Vendor engagements will continue to be used to validate the MC&A approach and identify gaps where additional research may be required. One key benefit of the vendor engagements is to provide test beds for measurements technologies and MC&A approaches in the future. Vendor interest in new technologies and approaches plays a key role in the direction of the ARSS program.

The research on measurement technologies is increasingly moving into the demonstration phase with planned collaborations with nuclear reactor vendors. Future development of the optical spectroscopy approach will focus on testing in more realistic environments with the ultimate goal of piloting on a reactor test bed. In the next 1-2 years the team will work with an industry partner to test the spectroscopy system on non-rad test loops. Future work will explore testing on irradiated molten salts or a molten salt reactor loop.

The long-term goal of the flow-tolerant electroanalytical sensor development work is to assess and confirm the performance of these electrochemical sensors over long-durations in a variety of representative coolant and fuel salts. The testing will include a long-duration assessment of the stability, accuracy, uncertainty, and longevity that can be expected from these sensor designs. Multimodal assessments and safeguards scenario testing leveraging the MFIT will also be performed for a variety of complementary sensors used in combination with the electrochemical probes. The economical, multifunctional nature of the flow-tolerant electroanalytical sensors will ultimately help to promote their widespread installation at multiple areas within an MSR.

For the system to monitor total salt mass/volume in an MSR, future work is needed. Similarly, technology solutions for non-destructive methods to quantify SNM in irradiated salt leaving the reactor system must be considered in order to account for material being containerized or entering a waste stabilization process. This becomes more relevant as MSR designs that envision on-site irradiated salt processing come closer to market.

5. PROVIDE R&D SUPPORT FOR UNIQUE DEPLOYMENT OF SMRS AND MICROREACTORS

SMRs and microreactors are being evaluated for use in numerous different deployment scenarios, which may expand in the future. The size and form factor of SMRs and microreactors make them candidates for non-traditional use cases. Examples include floating power stations, marine propulsion, satellite power, off-planet bases, diesel generator replacement, and community power generation (including college campuses). These deployment scenarios, and use cases, will lead to unique security and safeguards considerations. The ARSS program is evaluating these considerations to support non-traditional deployments.

The security challenges associated with unique deployment scenarios of SMRs and microreactors which will need to be addressed include identifying security requirements, assessing sabotage pathways, and considering the impacts of increased automation and/or remote operation. Current security planning and site analysis does not account for all potential sabotage pathways for these deployments. There are likely to be a variety of facility designs associated with these deployment scenarios, and these designs could present different security scenarios. For example, deployment in a remote location, versus near population centers or college campuses, versus marine locations will all have unique security considerations. The ARSS program is identifying the targets, and pathways, for these scenarios and assessing them to determine the appropriate security by design features. These situations should be assessed in modeling and simulation space to ensure that the appropriate analysis tools exist, and to provide general recommendations for different scenarios.

Current security requirements, as detailed in 10 CFR 73, are based on LWRs and may not be applicable to all SMR and microreactor deployment scenarios. There are different licensing pathways for a research or test reactor.

Another consideration which will need to be addressed for some of the unique deployment scenarios is an increased reliance on autonomous or remote operation. Understanding the cyber security risks and requirements, and how they may vary for different situations, will be critical for supporting deployment. The ARSS program is incorporating cyber security to address this growing need.

In addition to the security measures which will be required for unique SMR and microreactor deployments, there will also be safeguards considerations that will need to be addressed. The need for new MC&A approaches for advanced reactors was discussed in the earlier sections of this report. Many of the same issues will need to be addressed for the SMRs and microreactors that are operated in non-traditional environments.

It should also be noted that the security and safeguards considerations for unique SMR deployments could have interfaces with safety. These interfaces, for example, related to location, reliance on off-site responders for designs that have specific considerations (e.g. fuel form, coolant, etc.) will need to be addressed as strategies for security and safeguards are developed.

Marine propulsion is being examined to reduce the carbon footprint of overseas shipping. There are a number of safeguards and security challenges with both floating power stations and civilian marine propulsion. Reactors on any sort of boat or floating platform will have unique sabotage pathways not typically explored in a more traditional PPS analysis for a reactor on land. Current work is starting to explore path analysis to support PPS analysis for floating power stations and marine propulsion.

Another unique potential deployment scenario for advanced reactors is on college campuses. Universities are considering deployment of microreactors as research facilities, or even eventual power production, for campuses. Vendor partnerships are being utilized to examine building research or test reactors to attract students, demonstrate carbon-free energy production, and serve as a model for different areas of the country.

University research and test reactors can apply for a license through the NRC under a different set of requirements. These requirements are generally lighter for physical security, although the NRC can impose additional requirements for reactors producing more than 2 MW. Current research is looking into the variety of reactors being considered and determining where additional support may be needed with respect to MC&A, physical protection, or cybersecurity. Some of the deployment specific factors which will require additional consideration include the reactor design/technology, use case, and applicability of traditional RTR regulations. Specific security requirements for the different reactor types if they are deployed as RTRs, and the application of advanced reactor specific regulations for RTRs, also need to be established. These potential deployments are progressing quickly, and identification of the necessary support should be prioritized.

Path Forward

Nontraditional siting and use scenarios for SMRs and microreactors present a unique set of challenges which will need to be addressed to support these deployments. The specific security and safeguards requirements for these deployments need to be established, and the support that will be needed to meet the requirements needs to be determined. The security support should include PPS analysis, including target and path analysis, and cyber security considerations. Future work should provide research support for PPS modeling and analysis, including for both RTRs and maritime use of nuclear. This work will be in partnership with NNSA due to the potential international implications of maritime nuclear.

MC&A support will also be needed; this will include determining how accountancy will be performed, and ensuring the required measurement technology exists. Identifying the regulatory requirements, and the processes that will be required, will also need to be addressed. Future work will need to consider both specific deployment scenarios, and general requirements which can be addressed for broader deployment categorizations (e.g. all university deployments).

These novel deployment scenarios will create an opportunity to explore 3S interfaces, and 3S by design considerations; the ARSS program will support 3S by design and the 3S interfaces. In addition to the scenarios highlighted, future work may also expand into other non-electric applications of nuclear including process heat, energy for industrial complexes, or energy for critical infrastructure. The ARSS program can provide support for safeguards and security in these modalities if requested.

Future R&D in this space may expand into (1) delay and response factors for remotely located facilities, (2) PPS for maritime applications of advanced reactors, (3) challenges associated with cybersecurity for facilities in areas that may preclude constant remote data transmission and/or remotely operated facilities that require increased data transmission, (4) MC&A challenges of floating nuclear power plants or nuclear propelled cargo ships, and (5) U.S. reporting requirements for nuclear facilities still owned by the U.S. but operated in another state, as can be the case for maritime use of nuclear.

6. CYBERSECURITY RESEARCH

Advanced reactor technologies differ from existing commercial nuclear plants in a variety of ways that will change the emphasis on cybersecurity and will challenge existing regulatory approaches to cybersecurity. Greater use of digital technology and automation, smaller and simpler reactor designs, passive and inherent safety features, and new concepts of operation all change the landscape of how designers and regulators approach cybersecurity. Additionally, the sheer number of new design concepts and the uncertainty in the regulatory framework for licensing advanced reactors makes it challenging for stakeholders to address unique technical challenges associated with cybersecurity of advanced reactors.

New designs will rely more on digital technology for their control systems and will employ automation for more functions than existing designs. Concepts for advanced reactors range from fully digital control systems with limited analog or electromechanical backups to fully digital and fully autonomous operation. This reliance on digital equipment increases the burden to ensure the security of systems that rely on computers and communications including sensors, controllers, actuators, and any other capabilities that are employed in future control systems. The existing regulatory approach, which relies on characterizing digital equipment based on their proximity to or influence on safety functions, and managing these critical digital assets by evaluating hundreds of cyber security controls for each asset will not scale to the increased use of digital equipment in future plants.

Specifics of the system design will also interact with the control technology in ways that may actually decrease the burden for designers to address cybersecurity. Smaller and simpler reactor designs such as microreactors may reduce the safety consequences to a degree where fewer systems and digital components have a safety impact. This issue is twofold. First, smaller reactors have smaller source terms and smaller power, which influences the degrees of consequences that need to be considered. Second, simpler designs may have fewer actions taken by the control system, which reduces the complexity of the systems and the number of components that are required to achieve operational and safety functions.

The current regulatory framework for cybersecurity is governed by Title 10 of the Code of Federal Regulations (CFR) 73.54, “Protection of digital computer and communication systems and networks”. This approach requires protection of digital equipment based on its proximity to or interaction with safety and emergency preparedness functions. There is draft regulation 10 CFR Part 53 under development for Advanced Reactors which focuses on a risk informed performance-based approach. This framework provides a flexible, technology agnostic and graded approach to cybersecurity, which may help to mitigate the challenges with previous prescriptive approaches. But it also increases the need for flexible and rigorous tools for evaluating risk, consequence, and effectiveness of security controls.

U.S. NRC draft regulatory guidance DG-5075[20] proposes Tiered Cybersecurity Analysis (TCA) to improve the efficiency of Cyber Informed Engineering (see Figure 15). Tier 1 design analysis begins by eliminating any scenarios for which compromise of control systems will not lead to unacceptable consequences. Tier 2 focuses on identifying digital systems for which compromise will lead to an unacceptable consequence and develops a defensive cybersecurity architecture (DCSA) to prevent access to key control systems. However, even with a DCSA established there will be some susceptible

[20] NRC Draft Regulatory Guide DG-5075, “Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53,” available at https://www.nrc.gov/docs/ML2328/ML23286A278.pdf (June 2024).

cyber-attack pathways—Tier 3 then focuses on denial of task to add active controls to either stop or detect intrusion.

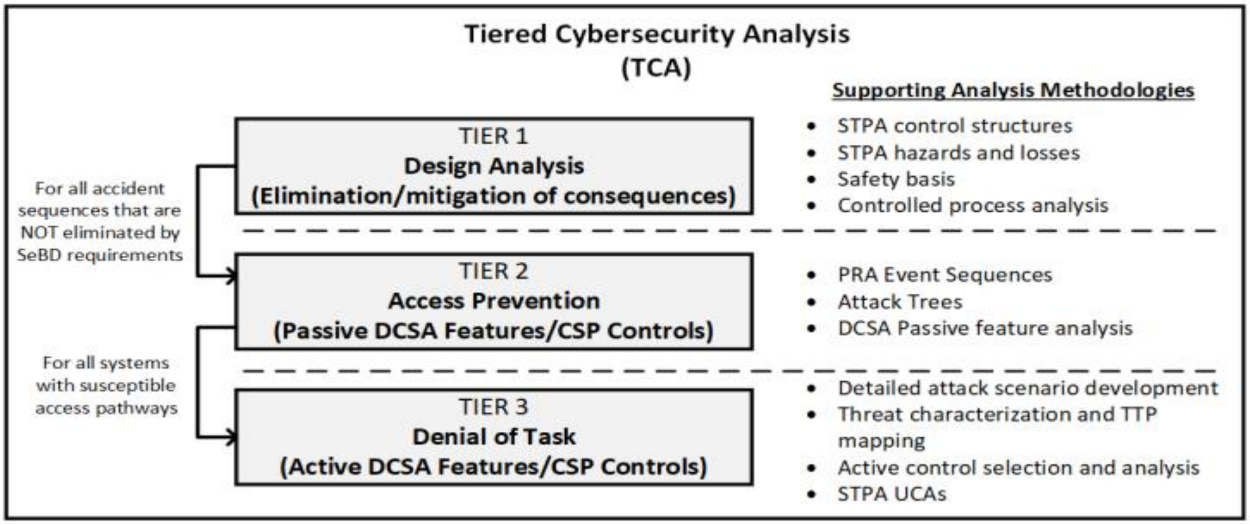
Tiered Cybersecurity Analysis
(TCA)
Supporting Analysis Methodologies
For all accident sequences that are NOT eliminated by SeBD requirements
TIER 1
Design Analysis
(Elimination/mitigation of consequences)
STPA control structures
STPA hazards and losses
Safety basis
Controlled process analysis
TIER 2
Access Prevention
(Passive DCSA Features/CSP Controls)
PRA Event Sequences
Attack Trees
DCSA Passive feature analysis
For all systems with susceptible access pathways
TIER 3
Denial of Task
(Active DCSA Features/CSP Controls)
Detailed attack scenario development
Threat characterization and TTP mapping
Active control selection and analysis
STPA UCAs

Figure 15: Proposed Tiered Cybersecurity Analysis[20]

6.1. Develop Cyber Informed Engineering Approaches

The ARSS program supports research to develop approaches that address cybersecurity in the design stage and throughout the entire engineering lifecycle. Cyber informed engineering incorporates both security by design features and other capabilities to engineer *out* cyber-enabled consequences or the ability to engineer *in* security features during the design phase, following the TCA approach. Projects in the ARSS program address the various stages of TCA.

6.1.1. Develop Tools to Support the Identification and Validation of Consequences of Cyber-Enabled Accident Scenarios

The ARSS program is developing tools and analysis techniques that correlate physical consequences to cybersecurity scenarios to characterize how cyberattacks on control systems equipment could have a physical impact on reactor systems. Ideally these tools would combine realistic understanding of cybersecurity threats and adversary tactics and techniques with high fidelity models of control systems and reactor physics. This work forms the basis for Tier 1 of TCA to first identify and eliminate scenarios that will not lead to an unacceptable consequence.

Currently the ARSS program is supporting the development of Advanced Reactor Cyber Analysis and Development Environment (ARCADE). This modeling and simulation environment connects a control system emulation platform with simulation tools already in use by the nuclear industry and will eventually connect to a cyber-attack simulation environment. Analysis performed with ARCADE is used to assess the consequence and inform the risk of cyber-attack on control system functions and network architectures. Figure 16 shows an overview of how ARCADE will be utilized.

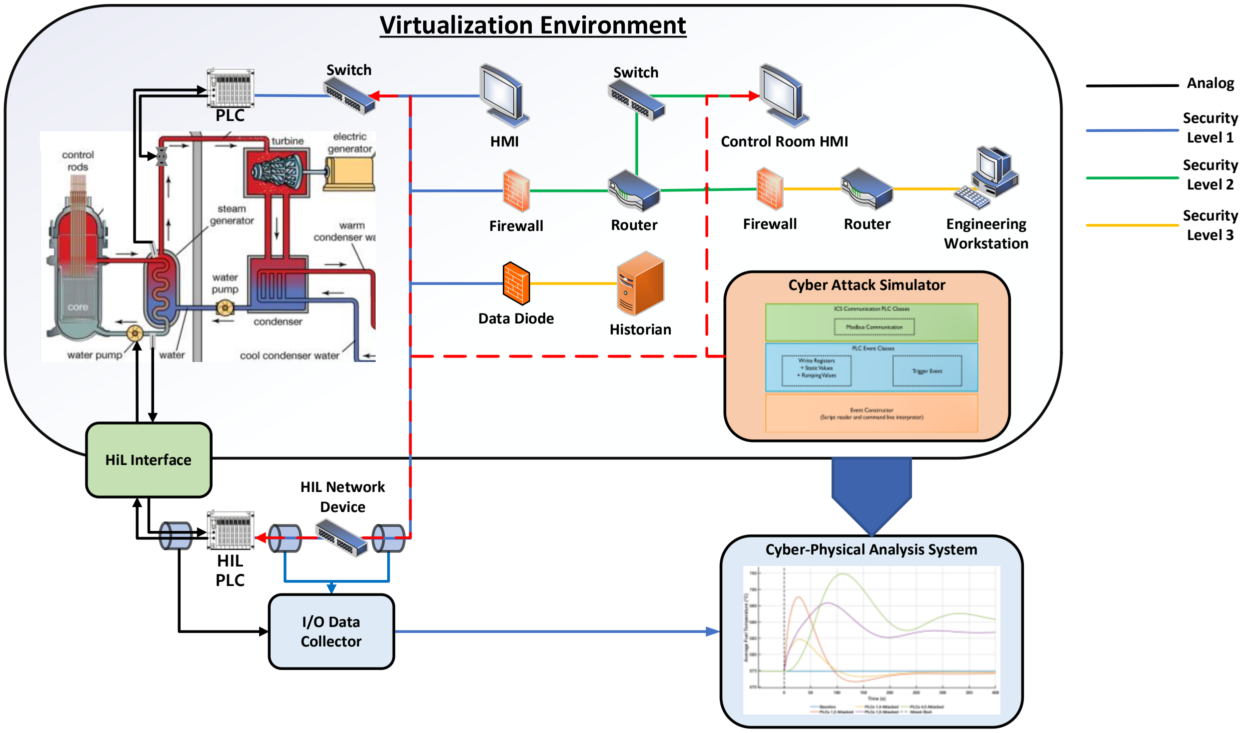

Figure 16: ARCADE Environment

ARCADE has a larger impact on Tier 1 initially as a blue team tool to help identify the defensive strategy for advanced reactors. Eventually, it will have more impact on Tiers 2 and 3 and may be used more for red teaming systems.

As the development of ARCADE matures, the ARSS program will assess the quality of the evidence ARCADE provides against alternative tools for assessing physical consequences of system design and evaluate whether alternated techniques need to be developed to assess how cybersecurity of controls systems can lead to physical consequences.

Path Forward

The ARCADE tool will be demonstrated with its first open-source release at the end of FY24. Future work will refine the tool and see more use as its use is more integrated into other cybersecurity R&D in the ARSS program. Efforts are currently underway to use ARCADE to examine cyber-physical attacks. Future work will more deeply explore the potential connections between ARCADE and the PPS modeling tools. Future work will also include development of tools that asses the economic tradeoff of cybersecurity aspects of the design, both in terms of consequence and in terms of the security technologies and controls implemented in the design.

6.1.2. Develop DCSAs for the Different Classes of Advanced Reactors

A defensive cyber security architecture (DCSA) is a method of architecting a system of systems based on the functions executed by each system. The implementation of a DCSA is a key element of the U.S. NRC draft regulatory guidance DG-5075[21] and is a strong part of Tier 2 and 3 of TCA. A

[21] NRC Draft Regulatory Guide DG-5075, "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53," available at https://www.nrc.gov/docs/ML2328/ML23286A278.pdf (June 2024).

conceptual DCSA model is shown in Figure 17. A DCSA consists of two primary features: security levels and security zones. Security levels provide a graded approach for defending plant functions. Security levels are assigned to functions based on their importance to plant safety, with the most important functions receiving the most stringent cybersecurity controls. Security zones define logical connections between systems where communication is trusted and provide defense-in-depth by forcing the adversary to breach multiple zones to compromise the functions needed to cause an accident sequence. Security zones also provide opportunities for detection of adversarial activity as the adversary attempts to penetrate individual zones or move laterally from one zone to another.

The ARSS program is developing a DCSA for each class of advanced reactors that is informed by security by design features common to that reactor class across vendors. These efforts will serve two purposes. The first purpose is to provide a technical starting point for industry to leverage in their plant-specific DCSA designs. The second purpose is to demonstrate the DCSA design process that is essential to implementation of DG-5075. This purpose is critical to enable the DCSAs to be leveraged by industry. Advanced reactor designers will have DCSA considerations unique to their plants, and a thorough demonstration of the DCSA design process will enable them to make the modifications necessary for their plants.

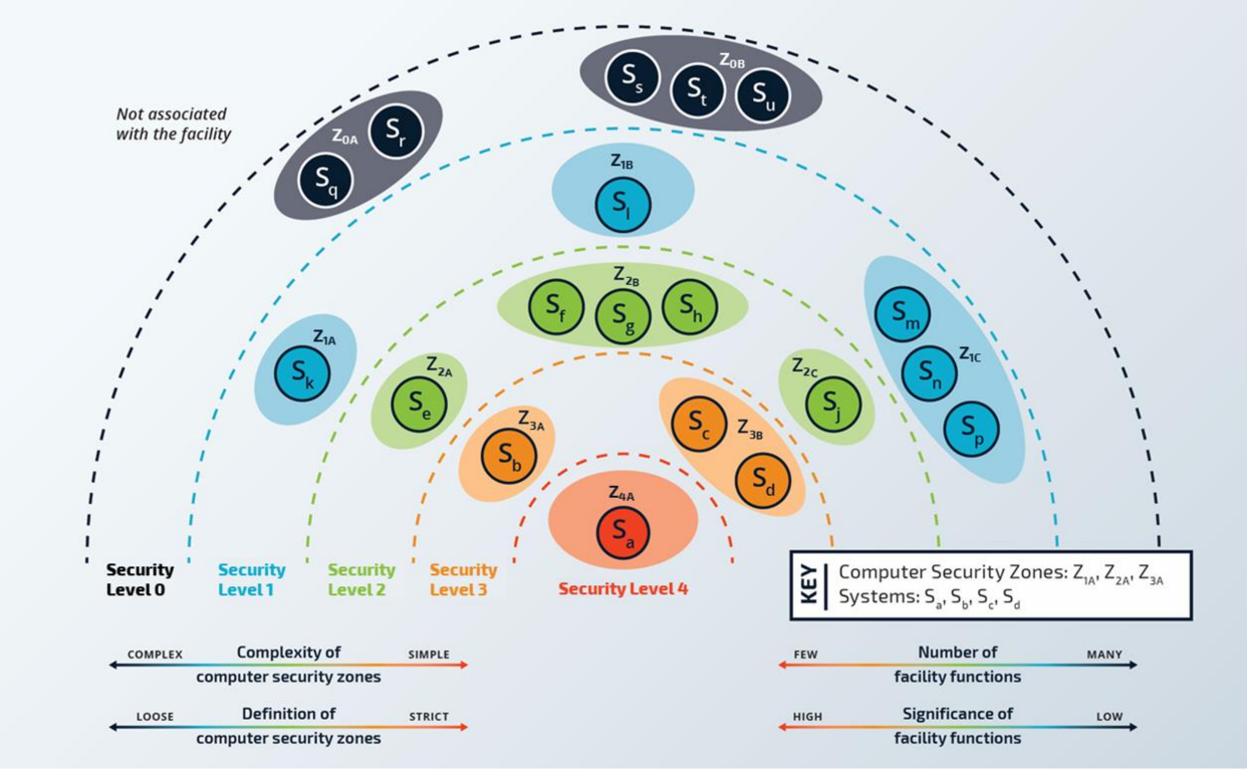

Figure 17: Defensive Cyber Security Architecture (DCSA) Model

Path Forward

In the near term, a DCSA will be developed for each advanced reactor class. The DCSA efforts will be integrated with other ARSS projects, and will provide the contextual basis for future cybersecurity technology R&D. For example, integration of the DCSA design process with ARCADE will enable rapid modeling and analysis of DCSA design candidates to select designs that satisfy specific safety and operational criteria. Further integration with physical security analysis will enable analysis of blended cyber-physical attacks. The DCSA templates can also be used as application context for cybersecurity technologies such as secure elements.

Over the next five years, the DCSA for each reactor class will be combined with the PPS and MC&A work on the different reactor classes to develop a complete reference for MC&A, PPS, and cybersecurity design recommendations by reactor class.

6.1.3. Develop Techniques and Tools that Simplify Implementation and Tracking of Security Requirements Controls

While developers who are closer to licensing and deployment are focused on operational concepts that minimize the risk to licensing, there is consensus that economic operation of both the future fleet and the existing fleet will require a much more integrated and connected control system than is feasible using today's methods and regulatory approach. While there are several technical challenges to be solved, these are mainly in system integration and careful design of processes to support secure integration. There are several areas related to tracking cybersecurity requirements in design and tracking cyber security relevant details where technology needs to be developed, matured, or evaluated to support the needs.

ARSS is supporting the development of integrated digital model-based systems engineering (MBSE) and cyber informed engineering (CIE) approach and implement in a software tool. The objectives of CIE design and operational principles are to ensure an engineering team considers and mitigates the potential for cyber compromise throughout the systems engineering lifecycle. The adoption of a risk-informed MBSE approach to nuclear digital engineering projects will provide a formal methodology to support the integrated requirements, design, analysis, verification, and validation necessary to incorporate safety, security, and resilience from unintentional digital incidents into the overall functional design

Path Forward

Future work will address supply chain and digital asset management by developing or adapting tools to support effective generation, tracking, and updating a software bill of materials and relating them to plant functions and integration with vulnerability management.

6.1.4. Assess the Interplay between Physical Security and Cybersecurity

Cybersecurity is intertwined with physical security. Some important context in any cybersecurity assessment is a clear understanding of what the physical boundaries are and what barriers are in place to achieve physical access to computers, networks, and control systems components. Further, physical security monitoring and control systems often rely on computers and networks, and the cybersecurity of those systems must be considered when assessing the overall security posture of the system.

As described in Section 3.3, the ARSS program is supporting analysis of cyber-physical attacks that cover the full range of ways that either cyber-attacks could take out elements of a PPS or that physical attacks could be used to gain access to control systems. The ARSS program is examining how the tools used for physical and cybersecurity may be used together to develop more robust plant protection approaches. This work plays a strong role in the Tier 2 analysis by also considering where physical protection elements and systems fall on a plant's DCSA.

Path Forward

In the near term, the PPS elements will be added to the DCSA. Blended cyber-physical tabletop exercises will help inform the overall approach for different classes of advanced reactors. Over the next five years, blended cyber-physical attacks will be examined in more detail with increasing reliance on both the PPS and cybersecurity analysis codes and tools. This work will feed into the five-year plan of developing guidance documents for each reactor class that cover PPS, MC&A, and cybersecurity design recommendations.

6.1.5. Develop Techniques to Support Assessing Cybersecurity Risk and Cybersecurity Performance

A risk-informed, performance-based regulatory approach requires rigorous methodologies for characterizing cyber risk and measuring cybersecurity performance. Though there has been significant investment and ongoing research on creating or adapting traditional risk analysis methods to include cybersecurity, there is still not a widely accepted and easily implemented method to evaluate cybersecurity risk in nuclear facilities. Further, there are no accepted methods for evaluating non-safety consequences and hybrid scenarios to support decision making or design for advanced reactors.

The ARSS program is investing in the development of techniques to assess risk based on multiple attributes rather than just one (for example, prevention of core damage, prevention of radiological release, and high plant availability, rather than focusing on core damage prevention alone). The tradition risk equation, which includes probability of attack as one variable, has historically been difficult to estimate. Previous work in the physical protection space has examined shifting this variable to level of difficulty[22] to more appropriately determine the likelihood of an attack vector given resources and competencies required following the Risk-Informed Management of Enterprise Security (RIMES) methodology. Current R&D in the ARSS program is evaluating applying a RIMES-type approach to cybersecurity threat analysis.

Path Forward

This work in general is at an early stage and will mature significantly over the next five years as the work on DCSA design moves more toward performance testing. Because the cyber threat landscape is constantly evolving, the design of cybersecurity systems will need to continuously evolve in an efficient manner.

Future work will partner with existing test beds to investigate methods to characterize cybersecurity risk and performance with more rigor. These partnerships may be within the national laboratory system, at universities, or with industry.

Future work will address critical gaps in characterizing cybersecurity risk and prioritizing cyber-attack scenarios and consequences, including exploring the RIMES methodology in more detail to determine its effectiveness and use in threat analysis. A key focus of RIMES will be to optimize cybersecurity design by focusing limited resources on the most plausible attacks that have the greatest consequence.

6.2. Apply Cybersecurity Technologies to Advanced Nuclear Systems

While cybersecurity research in general is a very broad and growing field, the ARSS program focuses on challenges and technology solutions as they would apply specifically to nuclear energy systems. The

[22] G. Wyss et al., “A Method for Risk-Informed Management of Enterprise Security (RIMES),” Sandia National Laboratories, SAND2013-9218P (October 2013).

research examines where technologies may be used, provides testing and evaluation, and develops recommendations for vendors on the appropriate use of cyber technologies in nuclear control systems.

6.2.1. Evaluate Existing Cybersecurity Technologies and Approaches for Nuclear Control Systems

Existing cyber security technologies and techniques are employed in critical infrastructure. Financial institutions use encryption and authentication to protect our financial information. Safety critical industries have employed existing techniques to support remote monitoring and control of critical functions. Though many mature technologies exist, they are not yet widely applied in nuclear control systems. The ARSS program performs research to identify these technologies and evaluate their applicability in control system contexts. This work is informed by the system functions identified in the DCSA and by the factors identified in the characterization of advanced nuclear reactor control systems.

One example of these technologies is secure elements (SE). SE is an integrated circuit providing tamper resistance, cryptographic security, and secure offline storage. SE are widely adopted for increasing confidence and confidentiality in computing systems across multiple industries. Work in the ARSS program has extended the proposed use cases for SE to control systems (see Figure 18). This work will also provide AR vendors with guidance on where SEs can be most efficiently included within DCSAs to improve network security posture. Current work is considering Field Programmable Gate Array (FPGA) based safety systems for architectures including SE.

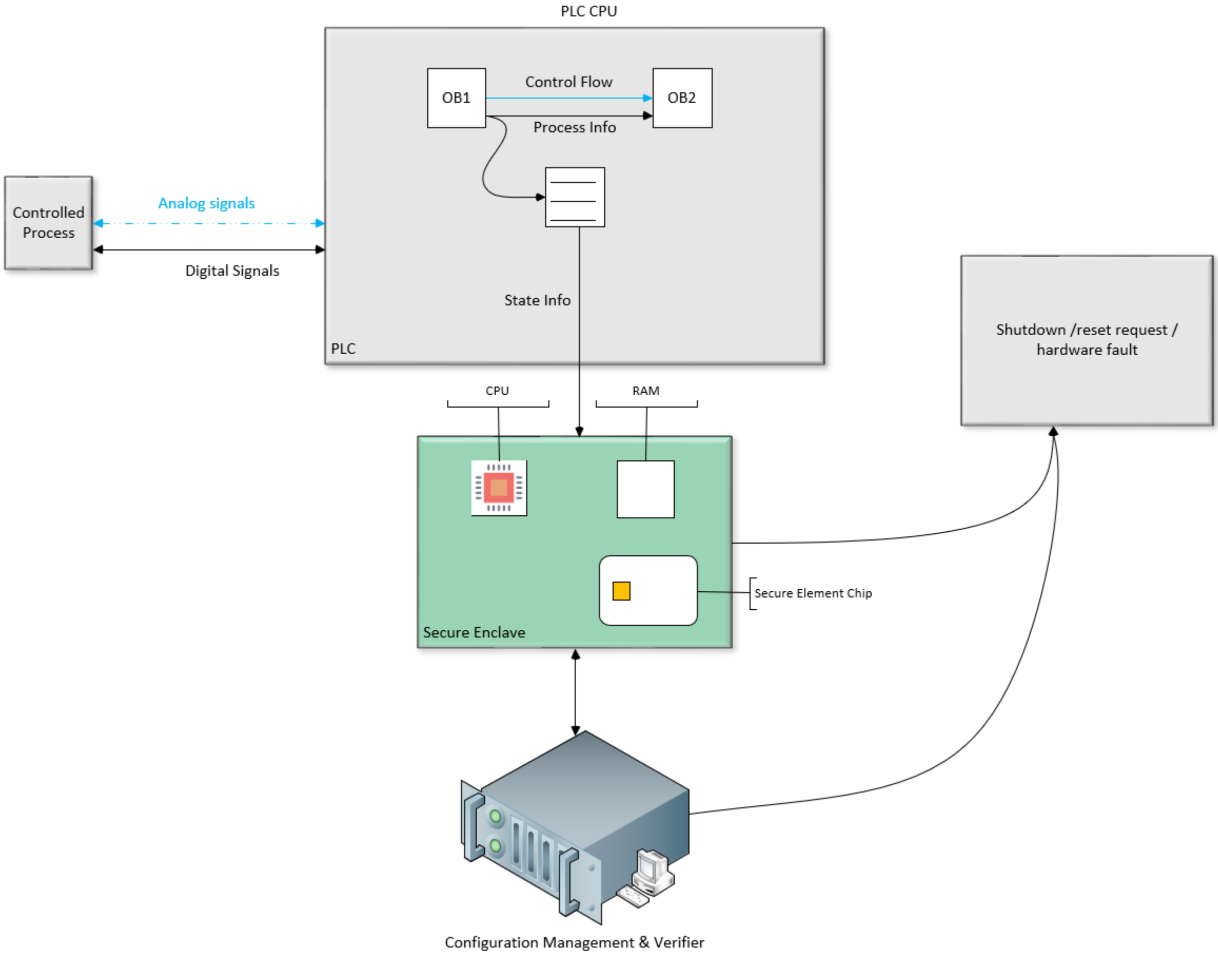

Figure 18: Use of Secure Elements in Nuclear Control Systems

ARSS is also performing research to evaluate the tradeoffs, regulatory considerations, and overall performance of network protocols that provide integrity support in lieu of techniques that provide integrity and confidentiality (such as encryption) which may not be appropriate for all control systems contexts.

Path Forward

Future work will satisfy industry requests for implementation guidance on using SE or other hardware root of trust technology for use in advanced reactors. The program will work with industrial partners to provide this guidance. Many implementation details rely on the specific performance requirements of the process, and the performance capabilities of the SE that are available to the vendor. Important to note here is that following the cybersecurity analysis that vendors may soon rely on (based on NRC DG-5075), the secure element would be a Tier 3 consideration. This means that some cybersecurity control is required to be implemented within the process' DCSA zone(s) to avoid potential design basis events. This work aims to provide vendors with a sense for what implementation details are available to them that conform to the previous design phases' results. Future work will identify additional cyber security technologies that should be employed in advanced reactor control systems and identify the barrier or constraints that may hinder or limit their use.

6.2.2. Provide Evidence to Support the Use of Wireless

The use of wireless in nuclear is a strong industry request due to potential cost savings for the operator, but its use in nuclear for safety related and important to safety functions currently is not allowed under NRC guidance. The key challenge with adoption of wireless technologies for safety functions within advanced reactors is associated with reducing or in some cases eliminating the physical boundaries where a system or device can be accessed, leading to exposures of the function(s) of the device or system to adversaries not authorized to access the physical locations where the devices or systems are located.

The use of wireless technologies demand prioritization of logical boundaries. Logical boundaries are "areas" from where data communications (over wireless) can be accessed, denied, or interacted with. Figure 19 shows an example of how the logical boundary area (area with wireless signal propagation) may extend beyond the physical boundary of a protected area. Attackers may access the resource from outside, inside the limited area, or inside the protected area. Current work is examining defensive strategies including: fortification (multiple successive and independent barriers, like a castle's moat, outer walls, inner walls, and keep), chokepoint (gate, drawbridge, doorways), access control (e.g., verification/authentication and authorization/entry), and deception. Deception is not currently used within nuclear reactor approaches but could have value to wireless especially to inform active defense.

As part of the Tier 2 analysis in TCA, the main goal of the wireless R&D in the ARSS program is to develop a series of test plans to provide the evidence needed to support use of wireless (given recommendations for appropriate implementation) or determine limitations or areas/systems for which wireless should continue to not be allowed. The test plans are divided into six groups:

i. [Architectural] Groups 1 & 2: Requirements that are associated with multiple layers and zones having strategic impacts to the entire cybersecurity of a DCSA.

ii. [Single Boundary] Groups 3 through 6: Requirements associated with a single system, wireless technology, or one or two logical boundary layers, with impacts limited to the single system, wireless technology, or logical boundary layer.

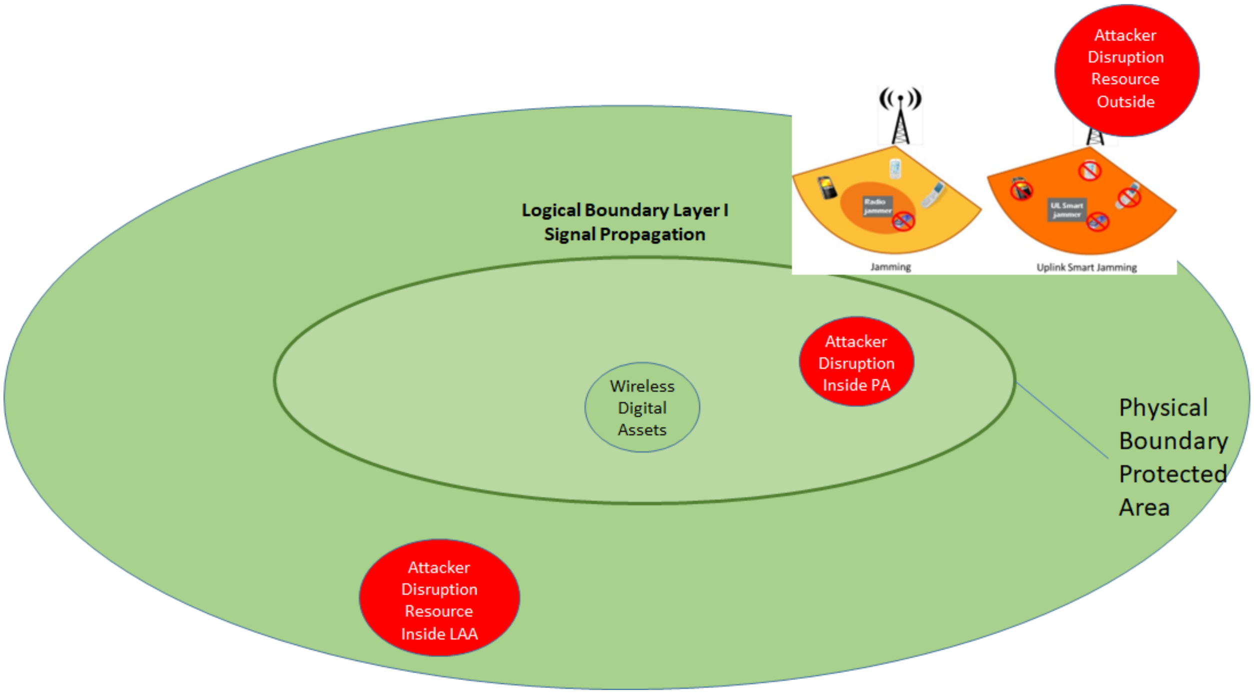

Figure 19: Comparison of Logical Boundary Layers and Physical Boundaries

Path Forward

Future work will explore the best approach for carrying out the test plans to support the use of wireless in nuclear. Testing may include teaming with industry with the ultimate goal of providing evidence for the regulator that may allow the use of wireless within certain constraints.

6.2.3. Evaluate Use Cases for Leveraging Artificial Intelligence and Machine Learning to Provide Cybersecurity Vulnerability and Threat Management in Advanced Reactors

Artificial Intelligence (AI) technology is being developed for potential use in aspects of reactor operations such as predictive maintenance, fault identification, and cyber vulnerability and threat management. However, AI and machine learning (ML) introduce new challenges related to explainability, use of proprietary or private data, potential spoofing of sensor readings or control inputs, or tampering with models. Using AI/ML technologies to develop automated or autonomous processes in advanced reactors can potentially minimize the labor costs of scaling up fleets of SMRs without multiplying the manpower costs related to monitoring and security. Guidance is required regarding which use cases are appropriate for AI/ML, incorporating cyber-informed principles into the design and deployment of AI/ML systems, and introducing appropriate compensating administrative/technical preventive/detective/corrective controls such as vulnerability management of AI/ML systems, secondary/independent monitoring of their activity, review of deployed algorithms and/or their outputs, appropriate levels of "human-in-the-loop" integration, or ensuring systems are designed with appropriate protections against inappropriate control inputs.

Work in the ARSS program will explore how ML algorithms can be trained on historical data to recognize patterns of normal behavior, allowing them to flag suspicious activity and alert security teams to potential threats. By combining AI and ML with traditional cybersecurity measures, advanced reactors can create a robust and adaptive defense against the increasingly sophisticated cyber threats they face, ensuring the safe and reliable operation of these critical infrastructure assets.

The ARSS program is developing a data-driven SMR threat hunting representations for embedded-system anomaly tracking (SMR-THREAT) to assist security personnel to hunt for threats to identify malicious activity in fused cyber and operational data from SMR control systems. The tools ingest data from diverse system logs as well as process and performance metrics. Natural language processing learns normal behavior patterns. Interactive visualizations allow threat hunters to explore relationships and detect anomalies in this multidimensional data.

SMR-THREAT will fuse timestamped cyber flows and physical transactions from various systems by aligning timescales and entity behaviors. The resulting multidimensional representation, encoded via natural language processing, will characterize normal relationships between digital and physical systems. Interactive visual interfaces of the changes in normal state over time will then help threat hunters identify anomalies, signaling potential 3S issues. By integrating cyber and physical data, SMR-THREAT will enhance monitoring and protection to provide a unified 3S perspective on the health and operational security of the plant in a way not possible with current monitoring tools.

The integration of AL/ML into cybersecurity systems for advanced reactors also introduces new risks and challenges. These include the potential for biased decision-making, over-reliance on AI, and AI-generated attacks. Additionally, poor data quality, lack of transparency, and vulnerabilities in AI systems themselves can compromise their effectiveness. Furthermore, regulatory challenges, difficulties in human-AI collaboration, and a cybersecurity skills gap may arise. It is crucial to carefully consider these risks and develop strategies to mitigate them to ensure the safe and reliable operation of advanced reactors. Cybersecurity experts will need to work with advanced reactor developers to ensure that the reactor data stream supports effective threat identification and diagnosis.

Path Forward

The research objectives and priorities for developing cyber-informed best practices for the application of AI/ML to advanced reactor operations aim to ensure the safe, secure, and efficient integration of these technologies into nuclear power plants. The primary objectives include: (1) identifying and mitigating potential cyber vulnerabilities in AI/ML systems to prevent unauthorized access or manipulation of reactor operations; (2) developing guidelines for the secure integration of AI/ML algorithms with existing reactor control systems and instrumentation; (3) creating standards for the validation and verification of AI/ML models used in reactor operations to ensure accuracy and reliability; and (4) establishing a framework for continuous monitoring and updating of AI/ML systems to address emerging cyber threats and ensure compliance with regulatory requirements. By achieving these objectives, the research aims to facilitate the adoption of AI/ML technologies in advanced reactor operations while minimizing the risk of cyber-attacks and ensuring the highest levels of safety and reliability.

7. CONSIDER INTERNATIONAL REQUIREMENTS

While the focus of the ARSS program is to help vendors meet domestic MC&A, PPS, and cybersecurity requirements, the vast majority of vendors are also interested in international deployment. From a SSBD perspective, it is useful for vendors to consider both domestic and international requirements in the design of their facilities. The ARSS program is coordinating research with related NNSA program areas that fund research on international safeguards and security.

Experience, techniques, and research from the International Atomic Energy Agency (IAEA) international safeguards domain are being evaluated to aid in (1) developing domestic MC&A approaches for advanced reactors and (2) preparing U.S. reactors for potential safeguards verification by the IAEA. The IAEA conducts international safeguards verification in over 180 countries. The purpose of IAEA safeguards is to account for nuclear material and verify that nuclear materials are not diverted or manufactured by state actors for non-peaceful purposes, in contrast with domestic MC&A which focuses on subnational threats.

The ARSS program is working with NNSA programs that support research in international safeguards and international security for advanced reactors. The ARSS program can both leverage work in the international space for potential use to meet regulatory requirements and at the same time provide ARSS program results to NNSA programs to help inform the linkages between domestic and international requirements.

The Office of Nuclear Energy has been a long-time supporter of the Generation-IV International Forum (GIF). The Proliferation Resistance and Physical Protection (PR&PP) working group examines safeguards and security aspects of the various advanced reactor designs, facilitates the practice of SSBD for advanced reactor designs, and assures that analyses are an aid to informing decisions by different stakeholders, including regulators, designers, and policy makers. The PR&PP working group has recently updated six advanced nuclear reactor system white papers which analyze the six GIF systems from a PR&PP viewpoint. New initiatives include updating the PR&PP methodology, investigating the 3S interface (the congruence of safety, security, and safeguards) for a pebble bed reactor design, and evaluating various siting options for SMRs and microreactors from a PR&PP viewpoint. The insights gained from the PR&PP working group are being pulled into the ARSS program.

Path Forward

Future work on international interfaces will answer the following key questions:

- Where are the technical intersections between IAEA safeguards and U.S. domestic material control and accounting (MC&A), and what key distinctions or caveats must be accounted for when translating findings from one domain to the other?
- How can we better provide guidance to vendors and operators to help meet both U.S. and international requirements for MC&A, international safeguards, PPS, and cybersecurity?

The goal of this work is to develop guidance for U.S. advanced reactor vendors that wish to capture synergies between domestic and international safeguards. The research will help to harmonize vendor outreach efforts being conducted by NNSA on this topic and could serve as a basis for selected SSBD recommendations for industry.

In the future, there are several ways the approaches and lessons learned from the PR&PP working group can assist the vendor community. The PR&PP methodology should be better socialized with the U.S. nuclear industry along with its applications to implement safeguards and security by design.

Areas of design novelty related to the interface between safety, security, and safeguards should be identified. GIF maintains a periodic industry forum which has been used to identify current directions for the PR&PP working group. The work will continue to be presented to the GIF industry forum for feedback and to solicit areas of interest for future work.

8. CONCLUSION

The ARSS program provides laboratory R&D to help remove roadblocks to advanced reactor deployment. The five key program goals are based on current needs of the vendors to help develop efficient, appropriate, and effective MC&A, PPS, and cybersecurity designs to help vendors streamline licensing. The goals of the program will change as progress is made in the various reactor designs. The ARSS program is emphasizing near-term results, so as problems are solved, the work will naturally move on to other priorities. Advanced reactors designs also continue to develop and gain fidelity, so future challenges may be identified.

Stakeholder feedback is critically important to maintain relevancy for the work. Vendor and NRC feedback is most important, but there are several other stakeholders that work in the safeguards and security areas who can provide unique perspectives. As part of the program plan, stakeholder meetings and individual meetings with vendors, advanced reactor groups, and the NRC will be a routine part of the technical work.

A key metric of the ARSS program is to prevent safeguards and security challenges from impeding licensing and commercialization of new designs. The R&D portfolio presented here will provide regulatory approaches, new technologies, and analysis that proves how reactors will meet the underlying goals of developing safe and secure nuclear energy systems.

REFERENCES

1. T. Grenci et al., "Interim Report of the American Nuclear Society President's Special Committee on Small and Medium Sized Reactor (SMR) Generic Licensing Issues," American Nuclear Society (July 2010).
2. R.J. Bell et al., "Position Paper: Physical Security for Small Modular Reactors," Nuclear Energy Institute (July 2012).
3. Rulemaking for Physical Security for Advanced Reactors, Nuclear Regulatory Commission, NRC Docket ID: NRC-2017-0227, available at https://www.nrc.gov/docs/ML1909/ML19099A017.pdf.
4. "Preliminary Proposed Rule Language: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors," NRC Docket ID: NRC-2019-0062 (2020).
5. A.S. Evans et al., "U.S. Domestic Small Modular Reactor Security by Design," Sandia National Laboratories SAND2021-0768 (January 2021).
6. A. Evans et al., "U.S. Domestic Pebble Bed Reactor Security-by-Design," Sandia National Laboratories SAND2021-13122R (October 2021).
7. A. Evans et al., "U.S. Domestic Sodium Fast Reactor: Security by Design," Sandia National Laboratories SAND2023-09146R (September 2023).
8. A. Evans et al., "U.S. Domestic Microreactor Security-by-Design," Sandia National Laboratories SAND2021-13779R (October 2021).
9. A. Evans et al., "U.S. Domestic Molten Salt Reactor: Security by Design," Sandia National Laboratories SAND2024-07607R (June 2024).
10. J.R. Russell et al., "Deliberate Motion Analysis Fused Radar and Video Test Results," Sandia National Laboratories, SAND2021-5413 (April 2021).
11. J.R. Russell et al., "Multi-Sector, Multi-Intruder Test Results for a DMA enabled PIDS (DPIDS)", Sandia National Laboratories, SAND2024-01437R (January 2024).
12. NRC Preliminary Proposed Rule Language Part 73 of Title 10 of the Code of Federal Regulations [NRC-2017-0227], available at https://www.nrc.gov/docs/ML2018/ML20182A157.pdf (2021).
13. D. Kovacic et al., "Nuclear Material Control & Accounting for Pebble Bed Reactors," Oak Ridge National Laboratory, ORNL/SPR-2023/2988 (December 2023).
14. M. Croce et al., "NDA of TRISO Fuels," Los Alamos National Laboratory LA-UR-23-32266 (October 2023).
15. Y. Cui et al., "Use Machine Learning to Improve Burnup Measurement in Pebble Bed Reactors," Brookhaven National Laboratory, BNL-222200-2021-FORE (September 2021).
16. K.K. Hogue et al., "Planning for Material Control and Accounting at Liquid-Fueled Molten Salt Reactors," ORNL/SPR-2023/3181, Oak Ridge National Laboratory (January 2024).
17. A. Lines et al., "On-line Monitoring for Molten Salt Reactor MC&A: Optical Spectroscopy-Based Approaches," Pacific Northwest National Laboratories, PNNL-31955 (September 2021).
18. S. Branch, et al., "Exploring the Complex Chemistry of Uranium within Molten Chloride Salts" *Ind Eng Chem Res* **2023**, *62* (37), 14901–14909. DOI:10.1021/acs.iecr.3c02005.
19. N. Hoyt, E. Stricker, and C. Moore, "Design and Construction Progress for the Modular Flow Instrumentation Testbed and Associated Sensors," Argonne National Laboratory, M3RS-20AN0401112 (September 2020).
20. NRC Draft Regulatory Guide DG-5075, "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53," available at https://www.nrc.gov/docs/ML2328/ML23286A278.pdf (June 2024).

21. NRC Draft Regulatory Guide DG-5075, "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53," available at https://www.nrc.gov/docs/ML2328/ML23286A278.pdf (June 2024).
22. G. Wyss et al., "A Method for Risk-Informed Management of Enterprise Security (RIMES)," Sandia National Laboratories, SAND2013-9218P (October 2013).