SANDIA REPORT
SAND2021-12084
Printed September 2021

Sandia National Laboratories

Advanced Reactor Operational Technology Architecture Categorization

Prepared for the
US Department of Energy
Office of Nuclear Energy
Milestone No. M2CT-21SN1104024

Ray Fasano, Andrew Hahn, Alexandria Haddad, Christopher Lamb

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

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DoE and DoE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

Seven generation III+ and generation IV nuclear reactor types, based on twelve reactor concepts surveyed, are examined using functional decomposition to extract relevant operational technology (OT) architecture information. This information is compared to existing nuclear power plants (NPPs) OT architectures to highlight novel and emergent cyber risks associated with next generation NPPs. These insights can help inform operational technology architecture requirements that will be unique to a given reactor type. Next generation NPPs have streamlined OT architectures relative to the current generation II commercial NPP fleet. Overall, without compensatory measures that provide sufficient and efficient cybersecurity controls, next generation NPPs will have increased cyber risk. Verification and validation of cyber-physical testbeds and cyber risk assessment methodologies may be an important next step to reduce cyber risk in the OT architecture design and testing phase. Coordination with safety requirements can result in OT architecture design being an iterative process.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the hard work and commitment of all contributors to the project. In particular, we would like to acknowledge the strong support and leadership of Rebecca Onuschak at the Department of Energy. Chris Spirito, Katya Le Blanc (INL) and Lon Dawson, Michael Rowland, David Luxat (SNL) are to be commended for their programmatic and technical guidance.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

EXECUTIVE SUMMARY

Advanced reactor[1] (AR) designs are projected to have an increased reliance on streamlined architectures, diverse control systems specific to reactor type, and operate in remote locations. This report seeks to categorize the current operational technology (OT) architectures of leading designs. With dozens of reactor concepts being vigorously developed worldwide, the scope of this report was limited to reactor designs targeted for the U.S market with small modular reactor (SMR) or micro reactor (MR) characteristics, significant financial/technical support, and are positioned for the United States (U.S.) energy market. These new architectures are developed based on the following demanding design constraints: (1) economic, minimizing staffing requirements, (2) novel safety and operational systems, prioritizing passive systems, and (3) coupling to diverse energy outlets. Table I lists the twelve reactor concepts surveyed in this report.

Table I. Surveyed AR concepts

Design Name	Designer	Reactor Type	Thermal Power (MW)	Refueling Cycle (months)	Neutron Spectrum	Fuel Arrangement
Aurora	OKLO	Heat Pipe Cooled Micro Reactor	4	240	Fast	Hexagonal Blocks
eVinci	Westinghouse	Heat Pipe Cooled Micro Reactor	12	36	Thermal	Monolithic Block
Modular Micro Reactor	Ultra-Safe Nuclear Corporation	Gas Cooled Reactor	15	240	Thermal	Pellets in graphite blocks
Xe-100	X-Energy	Gas Cooled Reactor	200	Continuous	Thermal	Pebble Bed
BWXT Advanced Nuclear Reactor	BWX Technologies	Gas Cooled Reactor	50	Unknown	Thermal	Unknown
BWRX-300	GEH	Boiling Water Reactor	870	24	Thermal	Fuel Bundles
ARC-100	ARC with GEH	Sodium Fast Reactor	260	240	Fast	Fuel Bundles
Natrium	TerraPower with GEH	Sodium Fast Reactor	~931	Unknown	Fast	Unknown
MCFR	TerraPower	Molten Chloride	600	Continuous	Fast	Liquid Fuel

[1] Generation III+ & IV reactors

Design Name	Designer	Reactor Type	Thermal Power (MW)	Refueling Cycle (months)	Neutron Spectrum	Fuel Arrangement
		Fast Reactor				
NuScale SMR	NuScale	IPWR	200	24	Thermal	Fuel Bundles
SMR-160	Holtec	PWR	525	24	Thermal	Fuel Bundles
Hermes Reduced-Scale Test Reactor	Kairos Power	Liquid Fluoride Salt Cooled	~320	Continuous	Thermal	Pebble Bed

Only three reactors Aurora, modular micro reactor (MMR), and ARC-100 have 20 year refueling cycles and use different techniques to achieve this design goal. The Aurora reactor uses high density U-Zr fuel with 19.75% enrichment. The MMR uses a large volume of fuel, high burnup TRIstructural-ISOtropic (TRISO) fuel in silicon carbide pellets, and 19.75% enrichment. Finally, the ARC-100 reactor utilizes breeding with U-Zr fuel with a slightly lower enrichment of 13.10%.

To understand the future OT architectures proposed by these AR concepts past and current context is helpful. Historically, when generation II nuclear power plants (NPPs) began to modernize their instrumentation and control (I&C) systems, cybersecurity related complexity increased considerably. However, these NPPs were not originally obligated to have a cybersecurity program. After the 9/11 terrorist attacks there was a renewed focus on nuclear security and the U.S. Nuclear Regulatory Commission (U.S. NRC) begin implementing cybersecurity into regulatory requirements. In 2009, the U.S. NRC finalized Title 10 of the Code of Federal Regulations part 73.54 (NRC 10 CFR 73.54), "Protection of Digital Computer and Communication Systems and Networks". Part 73.54 established that NPPs are required to protect digital computer and communication systems and networks, up to and including the plants' design basis threat (DBT). National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and NIST SP 800-82 provided technical guidance for U.S. NRC Regulatory Guide (RG) 5.71, which assisted licensees in the development of acceptable cybersecurity plans. Now cybersecurity plans exist in conjunction with physical security and safety requirements.

As reactor design and technological complexity continues to increase a unified OT architecture is needed. These methods will support the coordination of safety, physical security, and cybersecurity requirements, as well as, the use of enabling technologies. Current research is exploring how to implement a risk informed approach and the required analysis tools needed to move away from the current compliance-based approach. Cyber-physical experiments are important to investigate how safety and security requirements interact and the efficacy of proposed risk assessment methodologies. Established experiments investigate cyber-attack prevention, detection, response, and OT architecture requirements [1, 2]. Previous analyses primarily focus on generation II and III reactor designs without considering novel control systems and capabilities unique to next generation reactors. The International Atomic Energy Agency's (IAEA) NP-T-3.19 covers a range of next generation reactor OT architectures in comprehensive detail [3]. Information in this report is an extension of NP-T-3.19 with updated information focusing on specific reactor concepts.

ACRONYMS

BOP	Balance of Plant
BWR	Boiling Water Reactor
CDA	critical digital assets
CFR	Code of Federal Regulations
CIA	Confidentiality, Integrity, and Availability
CRDM	Control Rod Drive Mechanism
DBT	Design Basis Threat
DCSA	Defensive Computer Security Architecture
DiD	Defense-in-Depth
DoD	Department of Defense
DoE	Department of Energy
DRAC	Direct Reactor Auxiliary Cooling
ECCS	Emergency Core Cooling System
EP	Emergency Preparedness
EPRI	Electric Power Research Institute
ES	Electrical System
FLiBe	Fluoride-Lithium-Beryllium
FPGA	Field Programmable Gate Array
FSAR	Final Safety Analysis Report
GCR	Gas Cooled Reactor
GEH	GE Hitachi Nuclear Energy
HAZCADS	Hazard and Consequence Analysis for Digital Systems
HPCI	High Pressure Coolant Injection
HTGR	High Temperature Gas Reactors
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
KSAs	Knowledge, Skills, and Abilities
LWR	Light Water Reactor
MACCS	MELCOR Accident Consequence Code System
MMR	Modular Micro Reactor
MR	Micro Reactor
MSR	Molten Salt Reactor
MSRE	Molten-Salt Reactor Experiment
NASA	National Aeronautics and Space Administration
NE	Nuclear Energy
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant

NRC	Nuclear Regulatory Commission
ORNL	Oak Ridge National Laboratory
OT	Operational Technology
OTSG	Straight-Tubed Once Through Steam Generator
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
QL	Quality Level
RG	Regulatory Guide
SFR	Sodium Fast Reactor
SMR	Small Modular Reactor
SNL	Sandia National Laboratory
SP	Special Publication
SSCs	Systems, Structures, and Components
SSEP	Safety, Security, or Emergency Preparedness
STPA	systems theoretic process analysis
TRISO	TRIstructural-ISOtropic
U.S.	United States

1. INTRODUCTION

This report fulfills milestone report Advanced Reactor Operational Technology Architecture Categorization (M2CT-21SN1104024) under work package M3CT-21SN110402. This work was sponsored by the Department of Energy's Office of Nuclear Energy (DoE-NE).

Seven generation III+ and generation IV nuclear reactor types, based on twelve reactor concepts were surveyed to extract relevant OT architecture information. Table 1-1 lists the twelve reactor concepts surveyed in this report.

Table 1-1. Surveyed AR concepts

Design Name	Designer	Reactor Type	Thermal Power (MW)	Refueling Cycle (months)	Neutron Spectrum	Fuel Arrangement
Aurora	OKLO	Heat Pipe Cooled Micro Reactor	4	240	Fast	Hexagonal Blocks
eVinci	Westinghouse	Heat Pipe Cooled Micro Reactor	12	36	Thermal	Monolithic Block
Modular Micro Reactor	Ultra-Safe Nuclear Corporation	Gas Cooled Reactor	15	240	Thermal	Pellets in graphite blocks
Xe-100	X-Energy	Gas Cooled Reactor	200	Continuous	Thermal	Pebble Bed
BWXT Advanced Nuclear Reactor	BWX Technologies	Gas Cooled Reactor	50	Unknown	Thermal	Unknown
BWRX-300	GEH	Boiling Water Reactor	870	24	Thermal	Fuel Bundles
ARC-100	ARC with GEH	Sodium Fast Reactor	260	240	Fast	Fuel Bundles
Natrium	TerraPower with GEH	Sodium Fast Reactor	~931	Unknown	Fast	Unknown
MCFR	TerraPower	Molten Chloride Fast Reactor	600	Continuous	Fast	Liquid Fuel
NuScale SMR	NuScale	IPWR	200	24	Thermal	Fuel Bundles

Design Name	Designer	Reactor Type	Thermal Power (MW)	Refueling Cycle (months)	Neutron Spectrum	Fuel Arrangement
SMR-160	Holtec	PWR	525	24	Thermal	Fuel Bundles
Hermes Reduced-Scale Test Reactor	Kairos Power	Liquid Fluoride Salt Cooled	~320	Continuous	Thermal	Pebble Bed

This information is contrasted with existing generation II NPPs and corresponding challenges. This comparison highlights unique design considerations, as well as, future standards, regulatory, and research areas of improvement. To limit the scope of this report the reactors assessed were limited to designs that have SMR or MR design characteristics, significant financial/technical support, and are positioned for the U.S. energy market.

These insights help inform unique OT architecture characteristics for a given reactor type. Next generation NPPs have streamlined OT architectures, relative to the current generation II NPP fleet, and increased reliance on passive safety systems. These measures have the potential to reduce the independence and diversity between systems. Furthermore, a reduction in operations and maintenance personnel, increased automation, increased digital instrumentation and control (I&C) component complexity, multi-unit operation, diverse energy outlets, and potential remote operation increase the cyber-attack surface. Taken in totality, without addressing OT architecture in the design phase, next generation NPPs will have similar challenges faced by generation II reactors coupled with potentially increased security risk. Verification and validation and uncertainty quantification of cyber-physical risk assessment methodologies and tools are an important next step to enhance the OT architecture of advanced reactors (ARs) [4].

2. CONCEPTS AND DEFINITIONS

The following sections introduce fundamental concepts and definitions used throughout this report.

2.1. OT Architecture

Architecture is defined as "the complex or carefully designed structure of something,"[2] and is used heavily in the design and construction of buildings. The term architecture, however, is gaining adoption in cloud computing infrastructure, software, and network design. A security architect is now a key position within an organization's cybersecurity team. The hardware and software used to monitor or control nuclear power plant (NPP) system functions, is the definition of OT. For the purposes of this report the term OT architecture is defined as outlined in Figure 2-1. Visual representation of OT architecture definitionFigure 2-1. Safety and security architectures can be categorized as subcategories under OT architecture. These architectures have unique design considerations but also share critical dependencies that affect overall system design and operation. Shared dependencies between safety and security must be coordinated to prevent safety considerations from degrading security considerations and vice versa.

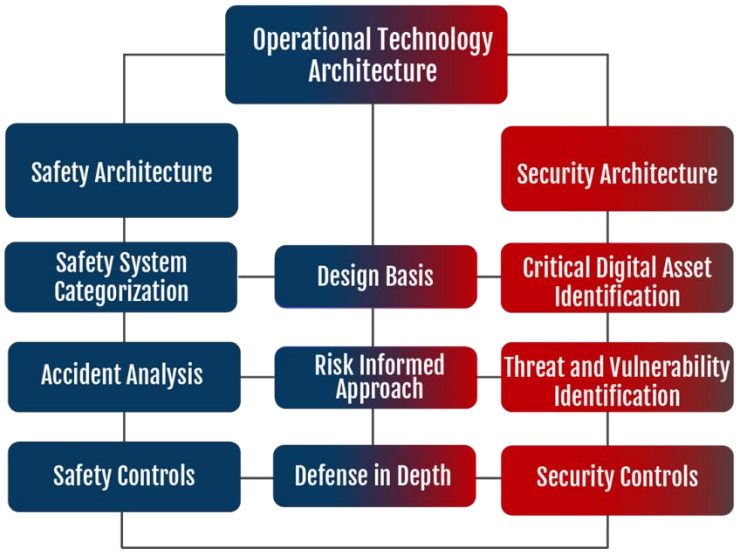

Figure 2-1. Visual representation of OT architecture definition

The Purdue Architecture is the first, best known, application of an architecture-based approach for OT infrastructure, as seen in Figure 2-2. This architecture provided designers with a framework to design an OT network by dividing system functions into five distinct levels. This concept was expanded to a security architecture that assigns unique security and assurance requirements to each level. The use of firewalls or data diodes between levels or sensitive parts of the network were used to control access and the flow of information. However, as the complexity of systems scale a unified OT architecture is needed to properly coordinated safety and security requirements. It is important to note that the digital systems used within a PPS are included within the definition of OT architecture.

[2] https://www.google.com/search?q=architecture+definition&rlz=1C5GCEM_enUS946US953&oq=architecture+definition&aqs=chrome.0.0i433i512j0i512l4j0i10i512j0i512l4.5619j0j15&sourceid=chrome&ie=UTF-8 .

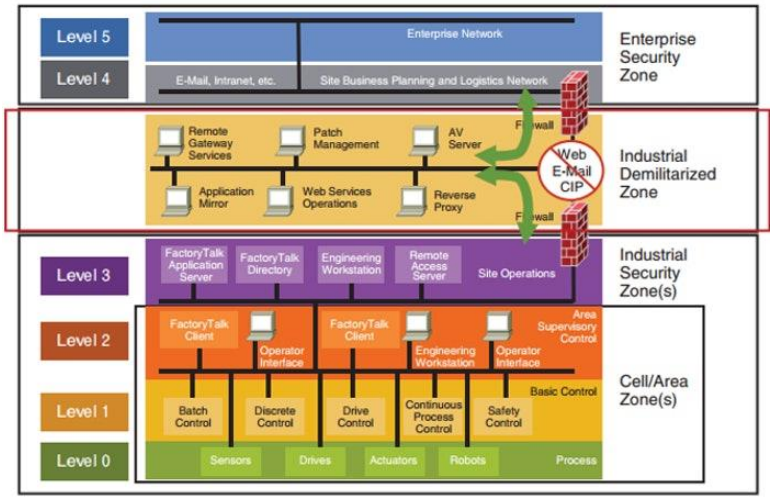

Figure 2-2. Five levels of the Purdue Architecture [5]

2.2. Defense in Depth

An emerging central design requirement for OT architectures is Defense-in-Depth (DiD), which is specifically called out in U.S. NRC 10 CFR Part 73.54(c)(2). Section C.3.2 of U.S. NRC RG 5.71 further specifies that "the failure of a single protective strategy or security control should not result in the compromise of a safety, security, or emergency preparedness function." By establishing multiple independent and diverse security controls the complexity of compromising a safety, security, or emergency preparedness (SSEP) function greatly increases. Security controls for the application of DiD are called out in U.S. NRC RG 5.71 C.3.3, and are further separated into technical, operational and management controls. These controls were derived from NIST SP 800-53 and NIST SP 800-82. The concept of safety DiD is also applied to mitigate common cause failures, ensuring that the failure of a single safety system does not compromise overall safety. Similar to security, safety controls are applied to reduce safety risk to a desired level.

2.3. Safety Architecture

A critical focus of safety is to account for random, early, and normal wear out failures of OT systems, or individual components, that will cause damage, injury, or increase risk. The bathtub curve approximates the failure rate of such systems as a function of time (Figure 2-3). Establishment of an overall safety architecture is needed to provide assurance that safety system functions are available, and integrity of these functions is maintained. Safety architectures range from component level to system level analysis. For NPPs safety systems are categorized based on their overall importance to safety using a graded approach. NPP safety systems are designed to ensure that the plants design basis is maintained during anticipated and unanticipated system transients. To meet this requirement safety DiD is employed by using multiple safety controls and the concept of independence and diversity. Some examples of these safety controls are mitigations against common cause failures, the use of fault tolerant hardware and software, or various administrative controls.

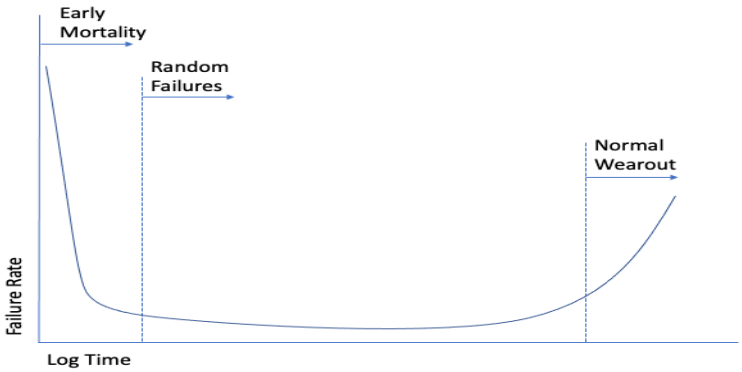

Figure 2-3. Bathtub curve of component failure

Using Figure 2-4, developed by Preschern C. et al, a subset of possible safety architectures for both software and hardware have been enumerated. Regarding NPPs, these architectures are used throughout a plant I&C system. A well-known example is the Triple Modular Redundancy architecture for the Reactor Protection System (RPS). This architecture uses three identical and independent calculations to determine whether a RPS trip signal should be generated. If one of the processes fails, the other two can veto the failure. However, if two out of the three controller processes fail (vote to trip), the RPS signal will be sent.

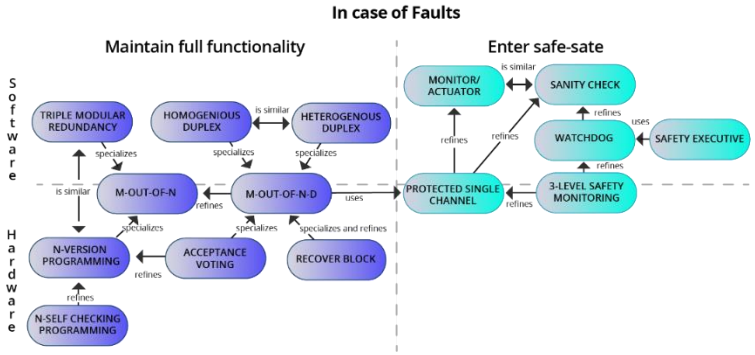

Figure 2-4. Subset of possible safety architectures for hardware and software

Zooming out from the hardware and software to the broader system of systems, safety architecture is applied so that no single safety system failure would lead to an accident scenario.

Quality Levels (QL), from A – D, are typically used to rank the importance of safety or safety-related systems. The lowest QL is a D. An A is the highest QL carrying the most stringent assurance requirements. Quality levels have been conflated with a system's trustworthiness and although there is a correlation between QL ranking and security levels, these systems, regardless of level, cannot be assumed trustworthy. The next section discusses trust models that describe how information security has requirements that do not directly overlap with safety considerations.

Generally, the safety architect prioritizes the availability of a system and the security architect prioritizes the integrity of the system. These goals are not mutually exclusive but do require additional coordination, as exemplified in IEC 62859:2016. Due to the complex nature of systems of systems, safety engineers typically assume a worst-case initiating event and then reverse engineer

compensating safety measures until an acceptable level of risk is achieved. Risk is defined in this report as the likelihood of an event multiplied by the consequence. Engineering codes such as MELCOR and the MELCOR Accident Consequence Code System (MACCS) can be used to calculate risk metrics important in the nuclear industry such as core damage frequency and large early release frequency.

2.4. Security Architecture

Although aspects of safety and security overlap, security is unique in that systems are targeted with malicious intent by an intelligent adversary. The intelligence of an adversary depends on their level of Knowledge, Skills, and Abilities (KSAs), allowing for different classes of adversaries to be identified. The six-tier approach, Figure 2-5, is one way to view the KSAs of different levels of adversary. Tier VI and V adversaries are more likely to directly target critical infrastructure, as well as have the resources to map out the safety and security architectures of a system to identify vulnerabilities. Furthermore, these adversaries may implant vulnerabilities in the design phase of a project to leverage in the future. Due to the high degree of penetration of a multilayered, long lead time attack the security architect must assume that single security controls are insufficient. Tier IV and III adversaries are also problematic in that they are more than capable of successfully completing high profile, highly disruptive attacks. However, these adversaries are less likely to target safety systems. This implies that a security architect cannot ignore any asset under protection due the diverse KSAs and intent of adversaries.

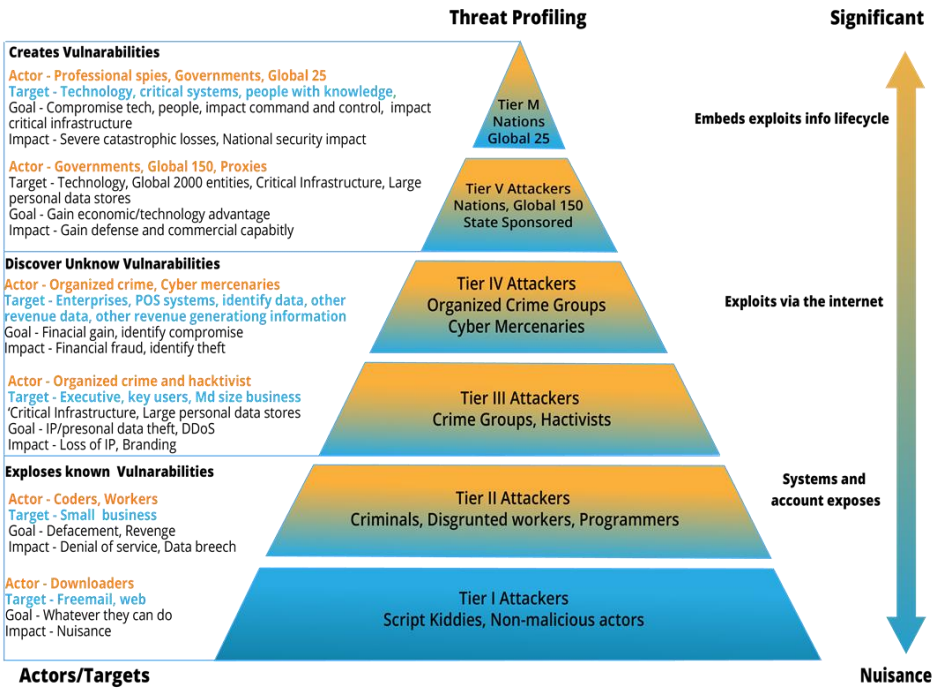

Figure 2-5. Threat profiling of cyber threat actors into tiers

Ultimately, a security architecture needs a risk informed approach to efficiently utilize the security budget for all assets. Safety systems that are risk significant will receive the most analysis and security measures. Non-safety systems with less risk will receive the least amount of security controls.

Security architects recursively use threat modeling and, like safety architects, reverse engineer from the worst-case scenarios to apply security controls. Licensees, per NRC 10 CRF Part 73.54, are required to protect a NPP from cyber and physical attacks up to and including the DBT. Security Architects should be familiar with cyber and physical security design considerations since physical security systems rely heavily on OT.

Cybersecurity controls seek to protect the Confidentiality, Integrity, and Availability (CIA) of data encapsulated by information systems. When sharing information, systems use trust models to inform data flow requirements within a security architecture. For example, the Bell-Lapadula Model used for U.S. government sensitive information (Top Secret to Unclassified) focuses primarily on confidentiality of the information. The Biba Integrity Model, as the name implies, focuses primarily on the integrity of the information. Since integrity for control systems is the overriding security design requirement, it is prioritized. Less important is confidentiality of information flow, hence ICS protocols generally do not use encryption. An assumption that trust models make, that is problematic for real systems, is that the initial system is secure. As seen in supply chain attacks there is a non-zero probability of compromise. A robust supply chain program is necessary to reduce the probability of initial compromise of an OT device.

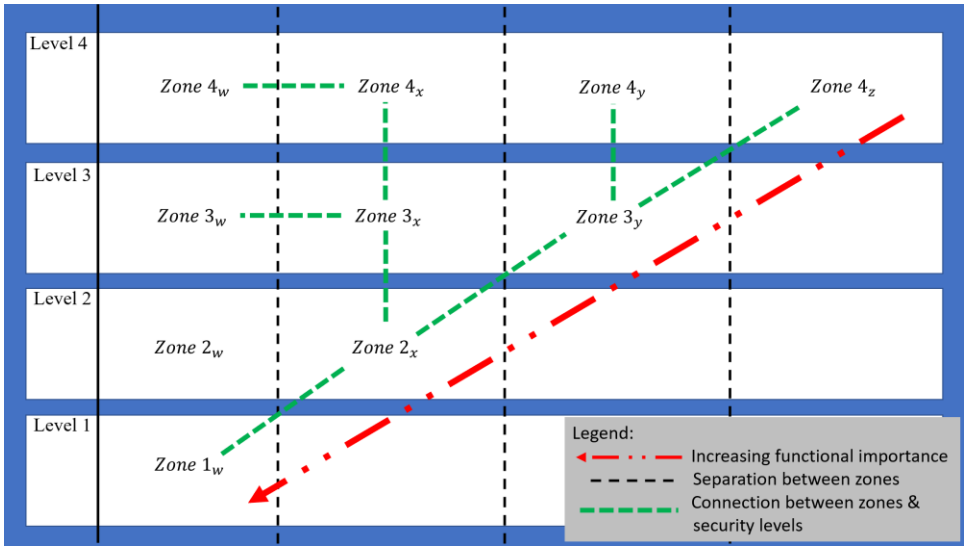

Figure 2-6. Abstraction of security zones and levels used in an OT architecture

The concept of security levels and zones, Figure 2-6, as part of a Defensive Computer Security Architecture (DCSA), is a new addition to security architectures [6, 7]. Current DCSA requirements address some architectural challenges in the current fleet of NPPs overviewed in Section 4.3, (i.e. large monolithic zones).

3. CURRENT APPROACHES

This section reviews U.S. NRC regulatory history as it is the primary reference for U.S. licensees. Additionally, it is important to understand NIST SP 800-53 and NIST SP 800-82. The NIST documents provide a significant amount of the technical basis for U.S. NRC's cyber regulation and guidance. The NIST documents outline cybersecurity requirements for federal information systems and critical infrastructure. NIST SP 800-53 is primarily for IT systems and NIST SP 800-82 covers cybersecurity nuances presented by OT systems [8, 9]. Both documents are not specific for NPPs.

The standard IEEE 692-2013: Criteria for Security Systems for Nuclear Power Generating Stations does not cover cybersecurity in significant detail and is primarily focused on physical security. Therefore, one must look to the international IEC standards for NPP specific recommendations. In this case IEC 62859:2016, IEC 62645:2019, and IEC 63096:2020 are the relevant standards [10-12]. In both the NIST and IEC standards high level architecture, safety and security development is encouraged early in the system lifecycle. IEC 62859:2016 specifically states that when trying to balance safety and security requirements architecture development may lead to an iterative process.

3.1. U.S. NRC Regulatory Approach to OT Architecture

Published in 2014, NUREG/CR-7141 provided a comprehensive mapping of controls to the current NRC regulations at that time [13]. This document also has a good history of the regulatory approach to security controls, the historical list is provided here for reference. The historical list has been expanded to include more information, current revisions, and the proposed new rule NRC 10 CFR 53, which is being written specifically for ARs.

2002 – U.S. NRC includes first cybersecurity requirements in physical security and design basis threat orders.

2004 – Publication of NUREG/CR-6847, "Cybersecurity Self-Assessment Method for U.S. Nuclear Power Plants," October 2004, providing guidance on methods for conducting cybersecurity self-assessments

2005 – U.S. NRC endorsement of the Nuclear Energy Institute (NEI) 04-04, "Cybersecurity Program for Power Reactors," providing guidance for developing and maintaining a cybersecurity program at licensed nuclear utilities

2006 – Publication of U.S. NRC RG 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," January 2006, providing guidance for the secure design, development, and implementation of safety related digital instrumentation and control systems

2007 – Publication of Branch Technical Position 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," March 2007, stating that system cybersecurity features be maintained under a configuration management program, tested, and that safety analysis includes consideration of cybersecurity risks

2009 – U.S. NRC finalized its rulemaking effort and issued new cybersecurity regulation (i.e., NRC 10 CFR 73.54) for nuclear power reactors, hereafter referred to as the cybersecurity regulation. The cybersecurity regulation requires that a licensee's cybersecurity program be incorporated as a component of the on-site physical protection program. As such, the cybersecurity plan is one of four security plans described in NRC 10 CFR Part 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage."

2010 - Publication of U.S. NRC RG 5.71, Revision 1, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," January 201. This regulatory guide provides an approach that the U.S. NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber-attack as defined by 10 CFR 73.1. Security controls outlined in RG 5.71 were based on security controls outlined in NIST SP 800-53

2010 – U.S. NRC endorsement of the NEI 08-09, "Cybersecurity Plan for Nuclear Power Reactors," which was developed by NEI to assist licensees in complying with the requirements of NRC 10 CFR 73.54

2011 - Publication of U.S. NRC RG 1.152, Revision 3 (current version), "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," July 2011

2012 – U.S. NRC endorsement of the NEI 10-04, "Identifying Systems and Assets Subject to the Cybersecurity Rule" to provide guidance on the identification of digital computer and communication systems and networks subject to the requirements of NRC 10 CFR 73.54.

2013 – U.S. NRC endorsement of the NEI 13-10, "Cybersecurity Control Assessments," which was developed by NEI to provide guidance for implementing a consequence-based approach to the implementation of cybersecurity controls for a licensee's critical digital assets (CDAs); the consequence-based approach described in this document will likely be incorporated into a future revision of RG 5.71

2017 – U.S. NRC endorsement of the Nuclear Energy Institute (NEI) 13-10, Revision 6 (current version), "Cybersecurity Control Assessments," August 2017

TBD – U.S. NRC proposed new rule NRC 10 CFR Part 53 with additions to NRC 10 CFR Part 73 in regard to a licensees cybersecurity program adding the concept of a graded approach or consequence informed assessment to accommodate the wide range of technologies being proposed for AR concepts.

Defensive security architecture is described in RG 5.71 section C.3.2.1, as shown in Figure 3-1, to illustrate the separation between security levels. In this architecture, level 4 has the strictest set of requirements and level 0 has the lowest. Guidance is mirrored in NEI 08-09 providing examples of how a licensee can fill-out the cybersecurity plan [14]. Leveraging the same definition of a defensive architecture, RG 1.152 further specifies, during the design phase, the need to place digital safety systems in the highest level of the defensive architecture. The suggestion is to use only one-way communication by means of hardware mechanisms. Additionally, RG 1.152 specifies that safety system should have a higher degree of security controls, down to the hardware level, beyond the security controls implemented at the network level.

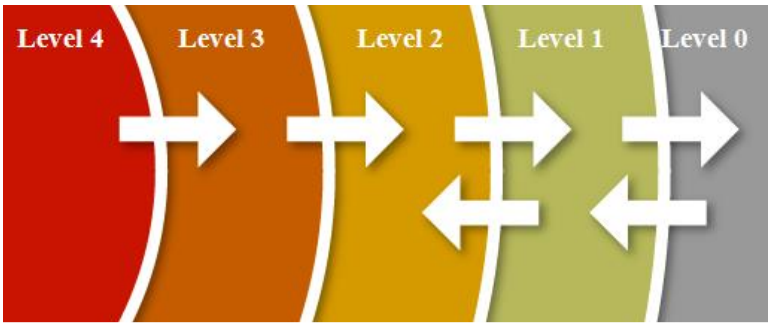

Figure 3-1. Simple defensive architecture for Cybersecurity

NEI 13-10 refines the concept of CDAs by establishing four different types of CDAs: Emergency Preparedness (EP), Balance of Plant (BOP), Indirect, and Direct CDAs [15]. Of the four, only Direct CDAs are high consequence, the other three are low consequence. Security controls are applied commensurate with a CDA's classification based on a full evaluation. How these CDAs are integrated into a defensive architecture is not outlined. Furthermore, interdependence between CDAs is not covered and quantitative analysis methods have not been established.

3.2. NIST SP 800-52 and NIST SP 800-82

A significant amount of the guidance in U.S. NRC RG 5.71 and NRC RG 1.152, including the implementation guidance to the regulation of NEI 08-09 and NEI 3-10, is derived from NIST SP 800-53 NIST SP 800-82. In NIST SP 800-53 three types of architecture are defined:

- Information security architecture - An embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans. [OMB A-130]
- Privacy architecture - An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's privacy protection processes, technical measures, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. [SP 800-37]
- Service-oriented architecture - A set of principles and methodologies for designing and developing software in the form of interoperable services. These services are well-defined business functions that are built as software components (i.e., discrete pieces of code and/or data structures) that can be reused for different purposes. [NIST SP 800-53]

The following security controls for architecture are shown in Table 3-1. Ultimately, NIST SP 800-53 can be applied to IT and OT systems, but NIST SP 800-82 was needed to address specific nuances found in ICS environments.

Table 3-1. NIST SP 800-53 controls relevant to system architecture

Family	Control Number	Control Name	Control Enhancements
Planning	PL-8	Security and Privacy Architectures	PL-8(1) Defense in Depth PL-8(2) Supplier Diversity
Program Management	PM-7	Enterprise Architecture	PM-7(1) Offloading

Family	Control Number	Control Name	Control Enhancements
System and Services Acquisition	SA-17	Developer Security and Privacy Architecture and Design	SA-17(1) Formal Policy Model SA-17(2) Security-Relevant Components SA-17(3) Formal Correspondence SA-17(4) Informal Correspondence SA-17(5) Conceptually Simple Design SA-17(6) Structure for Testing SA-17(7) Structure for Least Privilege SA-17(8) Orchestration SA-17(9) Design Diversity
System and Communications Protection	SC-2	Separation of System and User Functionality	SC-2(1) Interfaces for non-privileged users SC-2(2) Dissociablility
	SC-3	Security Function Isolation	SC-3(1) Hardware Separation SC-3(2) Access and Flow Control Functions SC-3(3) Minimize Nonsecurity functionality SC-3(4) Module Coupling and Cohesiveness SC-3(5) Layered Structures
	SC-4	Information in Shared System Resources	SC-4(1) Security Levels [Withdrawn: Incorporated into SC-4] SC-4(2) Multilevel or Periods Processing
	SC-22	Architecture and Provisioning for Name/Address Resolution Service	none

The ICS Security Architecture, Section 5 of NIST SP 800-82, covers in depth specific architectural considerations for OT environments. The main concept being that IT and OT networks have many differences due to their respective use cases. These differences are covered in NIST SP 800-82 Section 2.4 (Comparing ICS and IT Systems Security). Connecting IT and OT networks poses significant security risk and the overall architecture should outline how IT and OT network segmentation is maintained. Network segmentation within the OT network establishes security domains that increase the effectiveness of applying security controls and reduces complexity.

Since remote connections are not recommended for OT networks insider attacks and social engineering are highly relevant for OT systems. Again, proper network segmentation can make it more difficult for insiders to compromise many systems given limited physical access to isolated, or virtual local area networks. Finally, OT systems have a high risk of negatively impacting the physical environment and is addressed in NIST SP 800-82. Therefore, the safety architecture needs to be considered in the security architecture analysis. Given that accident scenarios are not always the aim of an adversary, it is important to remember that OT processes are critical for human survival and prosperity. Disruption of OT processes cannot be accounted for as a purely financial loss due to associated externalities.

3.3. IEC 62859:2016, IEC 62645:2019, and IEC 63096:2020

The IEC standards outlined is this section are specific to NPPs and mirrors U.S. NRC guidance. The concept of security zones, however, is unique to the IEC standards coupled with the idea of security degrees. Security degrees map to the concept of security levels as defined by U.S. NRC and

NIST. Sections relevant to OT architecture in IEC 62859:2016, IEC 62645:2019, and IEC 63096:2020 have been selected for review.

3.3.1. Requirements IEC 62859:2016 Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Coordinating Safety and Cybersecurity

IEC 62859:2016 Section 5 – Coordinating safety and cybersecurity at the overall architectural level:

This section states that safety features and architecture characteristics such as equipment independence and system reliability have an overlap with security, but specific cybersecurity controls are still required. Fundamental requirements state that cybersecurity shall not interfere with the function or performance of safety systems. From an architectural standpoint the standard suggests that "cybersecurity requirements impacting the overall I&C architecture shall be addressed after the overall I&C architecture design and assignment of the I&C functions have been first made as per subclause 5.4 of IEC 61513:2011. The integration of architectural cybersecurity requirements may lead to an iterative design process." Leveraging safety design features, such as diversity and mitigations, against common cause failure can benefit cybersecurity. However, for the claimed benefit to be valid a cybersecurity analysis is still required.

3.3.2. IEC 62645:2019 Nuclear Power Plants – Instrumentation and Control and Electrical Power Systems – Cybersecurity Requirements

IEC 62645:2019 Section 5.4.3 – Graded approach to I&C security and risk assessment

As seen in the new rule being proposed by the U.S. NRC for ARs, NRC 10 CFR Part 53, IEC 62645:2019 calls for a graded approach with all I&C programmable digital systems being assigned a security degree. A security degree is defined as "gradation of security protection with associated sets of requirements, assigned to a system according to the maximum consequences of a successful cyberattack on this system in terms of plant safety and performance."

For OT, architecture security degrees are equivalent to security levels. Security degrees follow three principles: (1) consequences of a cyberattack regarding safety are of higher importance than attacks regarding plant performance (2) systems are viewed from a functional point of view and the security degree is based on the most sensitive function (3) the consequence-based assignment approach shall be rigorous and repeatable, such that security postures are reproducible and consistent. Security degree assignment should be made as early as possible in the I&C system life cycle. Interfaces between systems with different security degrees needs to be justified.

IEC 62645:2019 Section 6.3.2 – System architecture

"The system architecture is partitioned into a number of interconnected subsystems and components. The arrangement of system subsystems shall comply with security requirements related to the overall security degree of the system."

IEC 62645:2019 Section 7.3 – Security defense-in-depth

"Security defense-in-depth is an approach to security in which multiple and independent security controls, covering organizational, technical and operational aspects, are deployed in an architecture, as no individual security control can provide the expected security. In such an approach, it is the set of diversified and independent security controls which is able to bring the needed prevention, detection, and response capabilities."

3.3.3. IEC 63096:2020 Nuclear Power Plants – Instrumentation, control and electrical power systems – Security controls

IEC 63096:2020 Section 19 – Cybersecurity and architecture

"Provide a set of high-level cybersecurity measures and controls for the I&C and electrical system (ES) architecture.

The objective of the defensive cybersecurity architecture consists of facility or organizational wide controls that apply a graded approach and implement defense in depth. The architecture consists of policy and programmatic requirements to ensure that architecture once constructed provides the greatest level of protection to security zones assigned S1.

The architecture requirements are always applied and always in place. The main objective is to eliminate or reduce cyberattack pathways to sensitive digital assets."

Typically, security controls are thought of as controls applied to a system that is already built. However, IEC 63096 clearly details how the design of the system or architecture itself can be a security control by eliminating cyber-attack pathways in the design phase. Thus two tiers of security controls are possible for OT architectures, controls applied in the design phase and controls applied to the as-built system, Table 3-2.

Table 3-2. Controls regarding cybersecurity and architecture in IEC 63096:2020

Security Control
Ensure that elements within the same security degree all have consistent cybersecurity measures applied. Security Degrees are required by policy to group required protections into stratified levels, thereby reducing complexity of the security programme implementation.
Ensure that security zones segregation is related to their security degree requirements. Security Zones provide physical and logical boundaries (including virtual) wherein security controls are applied to meet the protection requirements demanded by the security degree.
Ensure that security administration systems are segregated from the functional systems.
Ensure that extracted and collected data for lookup purposes do not adversely impact I&C and ES systems
Prevention of weakening a Security Zone by introducing external elements with potential lower security controls

4. CURRENT IMPLEMENTATION - GENERATION II REACTORS

The current generation II nuclear fleet was built between the mid-1960s through the late 1990s and is set to be decommissioned in the 2020-2040s. Currently there are 93 reactors operating, 62 pressurized water reactors (PWRs) and 31 Boiling Water Reactors (BWRs). During the six decades of operational experience PWR and BWR technology has matured through diligent research and iterative design. Table 4-1 gives an overview of the general I&C architectures of generation II reactors. A detailed categorization can be found in R. T. Wood et al. [11].

Table 4-1. General OT architecture of generation II reactors

Architectural Layer	Related Systems	Primary Functions
Site Operations	• Main Control Room • Emergency Operations • Technical Support • Remote operations	Observe and maintain NPP operation. Provide manual human-in-the-loop inputs.
Area Supervisory Control	• Historian • SCADA systems	Store operational data: process and display data
Control and Monitoring Systems	• Reactor protection system • In-core/ex-core instrumentation system • BOP control systems • Turbine control system • Independent sensing and actuation systems • Reactor trip systems • Core protection calculators • Fire detection system • Environmental monitoring system • Alarms/annunciator system • Emergency power system • Engineered safety feature (ESF) systems • Physical protection systems • Feedwater/recirculation systems	Provide open/closed loop control of physical process
Process	• Plant components	Interact with physical process

Generation II reactors have a mixture of analog and digital control systems and were built to maximize economies of scale. The reactors were designed using a domain-driven design philosophy which included independence and redundancy between systems. This section reviews PWR and BWR reactor types to show the difficulty of categorizing these reactors using the concept of a unified OT architecture.

For all reactors licensed by the U.S. NRC the safety architecture categorization divides systems into either safety or non-safety. Under safety systems there are three categories, protection systems, safety monitoring systems, and safety instrumentation systems. Protection systems are generally comprised of the reactor protection system, engineering safety features actuation system, and reactor power cutback system. The reactor power cutback system is also commonly referred to as a core protection calculator by the nuclear industry.

Safety monitoring systems generally include ex-core neutron flux monitoring, inadequate core cooling monitoring, qualified indication and alarm systems, and a reactor coolant pump speed sensing system. Subsystems in each of these broad categories are then classified as category I, II, or III functions based on the severity of the consequence if the function is not performed. There are five critical safety functions that must always be maintained: reactivity/power distribution, primary side heat removal, reactor coolant system integrity, radiation control, and containment conditions. Quantitative analysis of safety function failure or loss can be completed by a probabilistic risk assessment (PRA) and accident analysis codes such as MELCOR or MACCS. This analysis informs the categorization of each system in the safety architecture. Once the accident analysis is complete, subsystem level safety architectural features can be deployed on the hardware and software level. Such as the triple modular redundancy used for reactor protection system hardware, coved in Section 2.3. For digital safety systems, fault-tolerant software and streamlined integrated circuits will also be used to increase the robustness of the code execution and eliminate superfluous features.

For non-safety there are also three categories, they are instrumentation systems, information processing and monitoring systems, and non-safety monitoring systems. Non-safety systems are still extremely important for plant operations and a non-safety system failure could potentially lead to a plant shutdown. These systems, however, are less regulated by the U.S. NRC due to the understanding that failure of a non-safety system does not pose a significant increase in radiological risk to the public. In the instrumentation systems category, the BOP subsystems are included, such as the feedwater or control rod drive mechanism (CRDM) control systems. How exactly BOP systems are implemented varies greatly between reactors, even reactors of the same type, as system modifications are done at the discretion of the licensee. Information processing and monitoring subsystems include the information processing, display panel, and non-safety qualified indication and alarms systems. Non-safety monitoring systems generally include the nuclear steam supply system integrity monitoring, radiation monitoring, reactor coolant pump monitoring, and fixed in-core data acquisition systems. Overall, even non-safety systems can be further categorized by relative importance for plant operation and have additional controls applied accordingly. It is common to have independent and redundant channels for communication with non-safety systems.

Security architectures for generation II reactor systems follow the recommendations outlined in U.S. NRC 5.71 and NRC 1.52 and NEI 13-10. A licensee's security plan would contain the relevant information to comment on specific details of a plant's security architecture. Based on NEI 13-10 the EP, BOP, indirect, and direct CDAs are categorized, with EP having the least and direct CDAs having the most security controls. The U.S. NRC's definition of a defensive architecture is similar to the concept of zones and security levels but is not rigorously defined. Furthermore, the heavy use of analog systems complicates the formation of a cohesive network topology. In general plants use data diodes to separate ICS network interfaces from site operations. There was not a generation II reactor security plan available for this report, therefore the report does not contain information about any specific OT architectural elements.

4.1. Pressurized Water Reactors

Generation II PWRs in the U.S. were designed by Babcock & Wilcox, Combustion Engineering, and Westinghouse (Table 4-2). PWRs generally have five different building areas: the fuel handling, containment, penetration area, auxiliary, and turbine building. There is one steam generator and reactor coolant pump per loop with corresponding hot and cold legs.

Table 4-2. PWRs currently operating

Reactor Type	Number in Operation	Power Range MWth	License Expiration Range
Westinghouse Two-Loop	5	1677-1800	2029-2034
Westinghouse Three-Loop	13	2587-2948	2030-2053
Westinghouse Four-Loop	28	3411-3853	2024-2055
Combustion-Engineering System 80	3	3990	2045-2047
Combustion Engineering	8	2565-3716	2031-2044
Babcock & Wilcox Raised Loop	1	2817	2037
Babcock & Wilcox Lowered Loop	4	2568	2033-2034

Across the reactor types there are four containment types, as summarized in Table 4-3. A useful approach when looking at OT Architecture is to start with system functions rather than specific system implementation. System functions are fundamental and should be the primary focus of safety and security. A comprehensive catalog of generic PWR system functions can be found in R. T. Wood et al., appendixes A and B [16]. Despite several refences that outline PWR system and plant layouts, a high-level overview of PWR OT architecture is not publicly available. Safety and non-safety subsystems are covered in domain specific documents.

Table 4-3. PWR and containment types

Reactor Type	Containment Type
Westinghouse Two-Loop	Dry, Ambient Pressure
Westinghouse Three-Loop	Dry, Ambient Pressure or Dry, Subatmospheric
Westinghouse Four-Loop	Dry, Ambient Pressure or Dry, Subatmospheric or Wet, Ice Condenser
Combustion-Engineering System 80	Large Dry, Ambient Pressure
Combustion Engineering	Dry, Ambient Pressure
Babcock & Wilcox Raised Loop	Dry, Ambient Pressure
Babcock & Wilcox Lowered Loop	Dry, Ambient Pressure

4.2. Boiling Water Reactors

Compared to PWRs, BWRs are a streamlined design eliminating the need for a pressurizer and independent steam generators. All BWR designs in the United States are designed by General Electric. Type 1 reactors introduced in 1955 have been retired. Only one type 2 reactor, Nine Mile

Point 1, remains in operation. The type 2 design introduced natural and forced circulation direct cycle in 1963, eliminating dual cycle heat transfer. Type 3 designs implemented the first jet pump application and improved the ECCS in 1965. Type 4 reactors increased power density in 1966. Type 5 reactors were introduced with the Mark II containment system in 1969, along with improved recirculation system performance and improved ECCS. Also, in 1969, the Mark III containment was introduced with type 6 reactor designs improving core performance and rod control systems. Numerous upgrades to systems, structures, and components (SSCs) have been made since the type 6 and Mark III, but the fundamental aspects of the designs have remained unchanged. Table 4-4 lists the BWRs currently operating in the U.S.

Table 4-4. BWRs currently operating

Reactor Type	Number	Power Range MWth	License Expiration Range
General Electric Type 2	1	1850	2029
General Electric Type 3	5	2004-2957	2031-2032
General Electric Type 4	17	2419-4016	2024-2054
General Electric Type 5	4	3544-3988	2042-2046
General Electric Type 6	4	3091-4408	2024-2045

Similar to PWRs, BWRs employ the same OT architecture strategy. In the case of BWRs the physics of the reactor are different, which leads to a different assortment of safety and security controls. A catalog of generic BWR systems can be found in R. T. Wood et al., appendix A [16].

Table 4-5. BWRs and containment types

Reactor Type	Containment Type
General Electric Type 2	Wet, Mark I
General Electric Type 3	Wet, Mark I
General Electric Type 4	Wet, Mark I or Wet, Mark II
General Electric Type 5	Wet, Mark II
General Electric Type 6	Wet, Mark III

4.3. Architecture Challenges

As observed in the Fukushima Daiichi accident, units 1, 2, and 3 experienced core melt and had no means of passive cooling during the accident progression due to loss of offsite power and onsite diesel generators. Since the Fukushima Daiichi accidents, additional safety requirements have been implemented globally as lessons learned to the generation II fleet. However, the fundamental design flaw requiring active intervention during accident scenarios remains. Advanced reactors have focused on how to integrate passive safety features as a primary safety architectural element.

From a security architecture point of view, the lack of a rigorous definition of a defensive architecture and the compliance-based approach by U.S. NRC has led to a wide range of

implementation strategies. Further complicating a plant's security plan is the hybrid nature of plant systems and domain specific operating departments. Some examples are the physical and cybersecurity groups operating independently of each other, or plants with mixed analog systems and digital systems. Compounding this are upgrades and plant modifications that have been layered over decades of operation and generations of staff.

Cyber and physical vulnerabilities typically emerge at the fault lines in an OT architecture. Lack of coordination and overall system integration of generation II reactors' OT architecture provide, potentially, numerous attack pathways. The question is not if a generation II reactor can be compromised through physical or cyber means, but instead: given an adversary, at each tier, what scenarios can they successfully complete with sufficient confidence? This question is better understood in physical security due to force-on-force exercises and a clear definition of the DBT. New technology such as consumer drones or hybrid cyber-physical scenarios continue to challenge the conception of what attacks can reasonably be accomplished and the timeframe needed to complete threat identification. Tragic events such as the terrorist attacks on 9/11 are a great reminder to never underestimate the ambition or capability of an adversary. Without obtaining detailed safety system categorization or security plans from an operating plant it is impossible to assess the cybersecurity posture of a generation II's OT architecture.

Generation II reactors tend to use large monolithic zones to reduce cabling costs, simplify compliance with multiple-stacked, safety and security requirements, and reliance on data-diodes. Assuming an adversary can circumvent a data-diode pivoting within a monolithic zone is a significant risk. A unified OT architecture and risk informed approach is a required evolution to increase NPP resilience against adversaries. Strategic division of OT zones along with careful configuration and monitoring of communication between zones and security levels is strongly suggested. Once these security levels and zones are designed, based on required plant functions, real CDAs can be selected to be put into specific zones. At this point, threat and vulnerability identification are key to harden the CDA against compromise.

According to NEI 08-09, the attack vectors relevant to NPP CDAs are physical access, supply chain, portable media, and device connectivity (i.e., wired and wireless communication). Based on these attack vectors, security controls are applied to address specific attributes of the CDA, in addition to the security requirements at the assigned security level. Further analysis could determine the need to redesign the selected CDA, or configured zone, because it cannot meet the overall OT architecture requirements. This creates a recursive design loop due to the interaction of safety and security requirements within an OT architecture. Currently this approach is not possible given current risk assessment tools and cost restrictions faced by generation II reactors, the details of which are beyond the scope of this report. See Cyber Risks to Advanced Reactors submitted in conjunction with this report for more information on associated challenges with cyber risk [17].

One challenge with designing a unified architecture is designing plant functions that are categorized based on the consequences. Hazard and Consequence Analysis for Digital Systems (HAZCADS) has been proposed as a method for quantify risks associated with unsafe control actions [18]. However, HAZCADS relies on PRA which uses probabilities in an event tree to determine a top-level outcome. An empirical probability of a cyber initiated event is indeterminate. Therefore, probabilities of 100% must be used to quantify the effects of a cyber initiated event given a worst-case scenario. Systems without a PRA rely on expert opinion-based risk reduction tables to determine if risks associated with a control system are unacceptable. The Electric Power Research Institute's (EPRI's) HAZCADS, Technical Assessment Methodology, and Digital Reliability Assessment Methodology, while certainly promising, have only recently begun to be adopted and

have yet to be widely used in NPPs. The difficulty of categorizing plant functions is further increased when assuming a coordinated attack that compromises multiple systems. In this respect the adversary has an asymmetrical advantage in that they know the desired consequence. The security architect does not know the desired consequence and must analyze each credible attack path. Analysis of individual systems is currently possible, using previously mentioned methods, but extrapolating to dynamic interdependencies between systems is not. Improving the ability to categorize plant functions and iterate on an OT architecture to optimize safety and security is an area of active research.

5. PROPOSED IMPLEMENTATIONS

5.1. Small Modular Light Water Reactors

There are substantial differences between the LWRs being proposed and the current generation II commercial nuclear fleet. See Table 5-2 & Table 5-1 for general design parameters. Note that the data included in table 5-1 applies to individual modules rather than an entire plant. This approach uses NuScale data exactly as provided, without introducing an ambiguity that may be introduced by assuming a specific plant design.

Table 5-1. General design parameters of PWRs surveyed (NuScale and SMR-160, for a single module) [12, 13]

Reactor Type: Pressurized water reactor	Secondary Coolant: Light water
Rx Thermal Power: 200-525 MW	Cooling Method: Natural circulation
Rx Electric Power: 77-160 MW	Power Conversion: Indirect Rankine cycle
Neutron Spectrum: Thermal	Fuel Composition: Uranium dioxide
Operation Lifetime: 60-80 years	Fuel Arrangement: Square bundles
Refueling Cycle: 2 years	Fuel Enrichment: <4.95% U-235
Primary Coolant: Light water	Moderator: Light water

Table 5-2. General design parameters of the small modular BWR surveyed (BWRX-300) [14]

Reactor Type: Boiling water reactor	Secondary Coolant: N/A
Rx Thermal Power: 870 MW	Cooling Method: Natural circulation
Rx Electric Power: 300 MW	Power Conversion: Rankine cycle
Neutron Spectrum: Thermal	Fuel Composition: Uranium dioxide
Operation Lifetime: 60 years	Fuel Arrangement: Square fuel bundles
Refueling Cycle: 1 – 2 years	Fuel Enrichment: 3.4% U-235
Primary Coolant: Light Water	Moderator: Light water

Both PWRs and small modular BWRs are proposing simplified architectures and passive safety features that will reduce overall unit cost and deployment time. Overall architecture simplification can be challenging from an I&C perspective because each control system or component serves multiple roles and can have a more significant impact on the plant. Reduction in overall volume complicates repairability and the design requirements that individual components must meet. Additionally, packaging sufficient redundancy of sensors and actuators without compromising plant performance is also a significant design constraint. The simplification in overall plant architecture is generally supported by passive safety features that require no external input by reactor operators.

It was clarified by Holtec that the following two points in Table 5-3. do not apply to the SMR-160 design: "Internal control rod drive mechanisms: Due to the offset steam generator the SMR-160 is able to utilize standard PWR CRDMs and air cooling, leveraging the operating experience of generation II plants. Helical coil steam generator: The SMR-160 utilizes a straight-tubed once

through steam generator (OTSG). The operation is similar to operating plants using an OTSG, again leveraging operating experience."

NuScale and GEH did not respond to requests for more information to their OT architecture design. NuScale's final safety analysis report (FSAR) however, is a good resource for I&C design information.

Table 5-3. General physical components of PWRs surveyed with unique I&C considerations [3].

Physical Components	Function	Possible Sensor Data	Unique Physical Limits
Internal control rod drive mechanisms	Reactivity control	Rod position Health state of rod drive components	Cannot be accessed by operators for maintenance and secondary verification of rod position
Internal pressurizers	Maintain core pressure and water level	Pressure Level Temperature Injection system flowrate	Time delay between changes in reactor and pressure response Heater and backup heater output Spray mass flowrate
Natural Circulation flow path	Eliminate the need for reactor coolant pumps by inducing natural circulation	Flowrate Pressure Temperature	Potential thermal-hydraulic coupling with the reactor core during transient scenarios Core penetrations will be reduced to maximize flowrate
Helical coil steam generator	Transfer heat from the primary loop to the secondary loop via steam production and maintain natural circulation in core.	Steam mass flow rate Feedwater mass flowrate Steam quality Inlet temperature Outlet temperature Primary coolant leak detection	Sensitive to changes in reactor power given large surface area to volume ratio Difficulty measuring steam quality at specific locations during transient scenarios Tube Dry out

5.2. Heat Pipe Micro Reactors

Heat pipe micro reactors stem from previous work in space nuclear power and propulsion systems that were developed throughout the 1960s-1990s through a joint funding agreement between National Aeronautics and Space Administration (NASA), DoE, and the Department of Defense (DoD) [26]. The demonstrated capabilities of space heat pipe reactors paved the path forward for terrestrial heat pipe micro NPPs (Table 5-4).

Table 5-4. General design parameters of micro heat pipe micro reactors surveyed (Aurora and eVinci reactors) [17, 18]

Reactor Type: Micro heat pipe reactor	Secondary Coolant: Super critical CO2 or Air
Reactor Thermal Power: 4-12MW	Cooling Method: Heat pipes
Reactor Electric Power: 1.5-3.5MW	Power Conversion: Super critical CO2 gas turbine or Open-air Brayton cycle

Reactor Type: Micro heat pipe reactor	Secondary Coolant: Super critical CO2 or Air
Neutron Spectrum: Fast and Thermal	Fuel Composition: Uranium oxycarbide (UCO), TRISO particles in a monolith, Uranium zirconium alloy
Operation Lifetime: 20-40 years	Fuel Arrangement: Hexagonal fuel blocks, Monolithic core
Refueling Cycle: 3-20 years	Fuel Enrichment: ~19.75% U-235
Primary Coolant: Liquid metals via Heat Pipes	Moderator: none, Hydride monolith

The most challenging design constraint for space reactor systems is weight. For terrestrial applications designers are freed from this constraint and can achieve much higher electric power output ~1-3 MWe compared to the goal of ~1-10 KWe for space applications. However, the layout of the reactors is similar. The general physical components with general design considerations are outlined in Table 5-5.

Table 5-5. General physical components of heat pipe micro reactors surveyed with unique I&C considerations [19]

Physical Components	Function	Possible Sensor Data	Unique Physical Limits
Heat pipes	Heat transport from the core to primary heat removal and passive decay heat removal	Temperature	Capillary limit Sonic Limit Entrainment Limit Boiling Limit
Monolith Core	Contain nuclear fuel Moderator (if thermal neutron spectrum) Heat transport	Neutron flux Temperature	Thermal contact with heat pipes
Primary heat exchanger	Primary to secondary loop heat transport	Secondary coolant flow rate Temperature Pressure	Depends on working fluid. Air and critical CO2 have been proposed. Heat exchanger design will be unique to micro heat-pipe reactors.
Passive decay heat removal	Emergency heat removal	On/off state Temperature	Thermal mass of heat sink Thermal contact with heat pipes

Due to the electrical output of MRs remote operation and status monitoring are higher design requirements relative to designs with higher electrical outputs. It may not be economical to support onsite operations and maintenance staff, suggesting the need for autonomous or remote command and control systems. As heat pipe micro reactors have exceptional load following capability, it is critical that control systems are qualified that can safely and securely enable load following. Oklo and Westinghouse did not respond to requests for more information on their designs.

5.3. Gas Cooled Reactors

Several gas cooled reactors (GCRs) have been constructed and operated to test the reactor concept. Reactors of note include the High-Temperature engineering Test Reactor in Japan and the Dragon Experimental Reactor in England. Table 5-6 gives a brief overview of general design parameters for the gas cooled reactor concepts surveyed.

Table 5-6. General design parameters of GCRs surveyed (MMR, BWXT, and Xe-100 reactors) [20-22]

Reactor Type: Gas cooled small modular reactor	Secondary Coolant: Solar salt, 60% NaNO3, 40% KNO3
Reactor Thermal Power: 15-200MW	Cooling Method: Forced convection
Reactor Electric Power: 5-80MW	Power Conversion: Unknown
Neutron Spectrum: Thermal	Fuel Composition: TRISO in Fully Ceramic Micro-Encapsulated Fuel (FCM), Uranium Nitride in TRISO, TRISO
Operation Lifetime: 20-60 years	Fuel Arrangement: Fuel pebbles, Fuel pellets in hexagonal graphite
Refueling Cycle: 20 years to continuous	Fuel Enrichment: 15.5 - 19.75% U-235
Primary Coolant: Helium	Moderator: Graphite

A helium cooled thermal reactor using high-assay low enrichment uranium (HALEU) is the prevailing gas reactor design being targeted for the U.S. market. Helium pressure vessels are difficult to seal, given the atomic size of helium and low molecular weight, and require specialized reactor coolant pumps. This necessitates I&C systems that ensure proper containment and purity of the helium coolant. X-Energy, BWX Technologies, and Ultra-Safe Nuclear Corporation did respond to comments on their OT architecture. These reactor designers were still in the conceptual design phase of OT architecture.

Sodium Fast Reactors (SFRs), Molten Salt Reactors (MSRs), and GCRs all have a similar I&C challenge given the high operating temperatures relative to LWRs. A significant number of NPP I&C components previously developed and tested over decades for LWRs are not compatible with these reactor types due to the high temperatures and physical characteristics of the primary coolant. Table 5-7 lists the general physical components of the GCRs surveyed for this report.

Table 5-7. General physical components of GCRs surveyed with unique I&C considerations

Physical Components	Function	Possible Sensor Data	Unique Physical Limits
Reactor core (TRISO fuel particles or fuel pebbles)	Transport heat to high velocity, pressurized helium coolant	Temperature Flow Vibration Moderator erosion Neutron flux Helium leak Air/water ingress	Large thermal and stress gradients Moderator entrainment Flow mixing and thermal stratification

Physical Components	Function	Possible Sensor Data	Unique Physical Limits
			Max temperature due to possibility of water or air ingress
Pebble fuel inventory control system	Remove pebbles that are spent and maintain accurate pebble inventory	Number of pebbles Burnup	Testing must be nondestructive Unique identification and tracking of pebbles
Helium purification system	Ensure helium coolant purity	Radiation Mass spectrums	Removal of noble gases produced by transmutation

5.4. Sodium Fast Reactors

Several sodium fast reactors (SFRs) have been built and operated globally. In the U.S. the Fast Flux Test Facility was operated from the 1980s to 2000s and was the principal source of liquid metal, fast reactor, and breeder reactor component data. To support next generation reactors the Versatile Test Reactor is currently being planned and will be built at Idaho National Laboratory.

Table 5-8. General design parameters of SFRs surveyed (ARC-100 and Natrium reactors) [28, 29]

Reactor Type: Sodium fast reactor	Secondary Coolant: Light water
Rx Thermal Power: 260-907 MW	Cooling Method: Forced Convection
Rx Electric Power: 100-345 MW	Power Conversion: Steam Rankine Cycle
Neutron Spectrum: Fast	Fuel Composition: Uranium Zirconium Alloy
Operation Lifetime: 60 years	Fuel Arrangement: Fuel bundles
Refueling Cycle: 20 years	Fuel Enrichment: 13.1% U-235
Primary Coolant: Sodium	Moderator: None

Information and operational data from SFR I&C systems is available due to the history and continued U.S. government support of SFR testing facilities. There are unique considerations for commercial reactors, given the different design requirements. One common challenge when working with liquid metal reactors is the opacity of the primary coolant. Visual inspection of components and access to components is greatly limited.

Therefore, I&C systems must factor in independent methods to confirm component integrity and remote/simplified maintenance. Finally, the concern of air/water ingress into the core may limit SFRs to locations with low probability of extreme weather events, unless commensurate measures are taken to mitigate the risk of air/water ingress into the core.

A significant safety advantage of SFR's is the low pressure of the sodium coolant, ensuring leakage events are far slower than pressurized systems. These reactors operate well below the boiling point of sodium which allows a large margin of temperature increase in potential accident events [30]. The high boiling temperature of the coolant allows greater ability to utilize natural convection to extract decay heat from the core in the event of loss of coolant flow. Volatile fission products are highly

soluble in liquid sodium and are entrapped in the coolant if fuel cladding failure occurs. This significantly reduces the risk of fission product release in accident event scenarios. However, these inherent safety characteristics do not eliminate the need for safety systems. Sodium fast reactors may be more dependent on safety system insertion of negative reactivity than LWR's due to a positive reactivity feedback as coolant density deceases [31]. It is likely, depending on the specific design, that boiling coolant or a loss of coolant will increase reactivity.

For sensors and actuators, the environment in the primary loop will require consideration of an increased radiation dose. Sodium is activated in the core producing Na-24, which mutates back to Na-23 through beta decay with a half-life of 15 hours. This also implies the need of an intermediate coolant loop, as any leak of the primary sodium into a steam generator would create a pathway for radiological release in the form of water-soluble sodium hydroxide. A worry not without precedent, as heat exchanger leaks on SFR's have caused numerous plant outages [32]. Detecting these leaks is a safety priority for any SFR control system. Hydrogen detectors can indicate sodium water reactions, and radiological monitoring on the intermediate loop can detect intrusion of the radioactive from the primary loop. Terrapower and ARC did not respond to requests for more information on their designs.

Table 5-9. General physical components of SFRs surveyed with unique I&C considerations

Physical Components	Function	Possible Sensor Data	Unique Physical Limits
Liquid sodium	Primarily loop coolant	Flowrate Temperature Mass spectrums Pressure Air/water ingress	Is opaque in the visible spectrum At standard temperatures and pressures sodium is a solid. Thus, temperature control is needed to prevent freezing during reactor shutdown. Reacts exothermically with water and oxygen. Thus, the addition of an inert gas containment and air/water ingress system is needed.
Intermediate loop	Transfer heat between the primary and secondary loops	Valve positions Temperature Pressure Flowrate	For pool-type SFRs the intermediate loop is in containment and is ideally chemically compatible with sodium and water (assume the use of a steam cycle)

5.5. Molten Salt Reactors

The canonical example of molten salt reactors (MSRs) is the Molten-Salt Reactor Experiment (MSRE) conducted at Oak Ridge National Laboratory (ORNL). This reactor operated from 1965 to 1969 and remains a source of inspiration for reactor designers in the 2020s. Unlike other reactor concepts two different coolants, neutron spectrums, and fuel compositions are currently being

proposed for MSRs targeted for the U.S. market. These can be broadly differentiated by two categories, liquid, and solid fueled reactors. Terrapower and Kairos Power did not respond to requests for more information on their designs.

5.5.1. Liquid Fueled Molten Salt Reactors

Following the example of the MSRE, fuel material is incorporated into the coolant as a fluoride or chloride species. The fuel chemical species is determined by the main halide of the carrier salt, which also influences the neutron spectrum. Heavier halides harden the neutron spectrum and as such fluoride-based salts are used in thermal spectrum reactors and chloride-based salts are used in fast spectrum reactors. The chemical difference of these halides' changes material choices and some operating considerations. The I&C system architectural requirements of these reactors are, however, very similar.

Liquid fuel brings a great number of difficult engineering problems, significant to a control system is a significant radiation environment. This is especially true for liquid fueled MSRs that are considering the use of the thorium cycle, which would greatly increase gamma dose to all components in the primary coolant loop. Unlike solid fuel reactors that contain their fuel in a central location, fuel material and fission products are in direct contact with all components in the primary coolant loop. The main consequence of this is digital and solid-state sensors and components cannot be located within primary containment. Additionally, all sensors must be analog or remotely located, with some designers considering locating critical sensors outside of the biological shield. This would improve serviceability of critical sensors but may also expand security parameters.

Security concerns regarding safety I&C systems are mitigated in many respects by the physics of the system. The primary regulating mechanism for reactor power is thermal expansion of the liquid fuel [33]. Precise control over the reactivity insertion into the core and I&C intervention to change power output or ensure safe shut down is unnecessary. In the event of any loss of power or heat rejection, the reactor can safely shut down without power or operator intervention. Below the core vessel a freeze plug that leads to a drain tank can be used to hold the fuel in a sub critical configuration. Should the cooling of the freeze plug stop, such as during a plant black out, the plug will melt and the fuel salt would drain into the tank [34]. This physics-based regulation of the nuclear reaction reduces the need for high consequence, high reliability systems that would be vulnerable to damage or interference. Thus, the primary security and safety concerns of these reactors would come from inventory control, a significant engineering challenge.

Precise chemistry control of the salt for a liquid fueled reactor must be maintained. Neutron poisons must be removed, redox potential controlled, and fissile loading maintained. The isotopic and chemical composition of the materials in the salt are continuously changing during reactor operation. Thus, the chemical composition of the salt must be monitored and continuously processed to maintain ideal conditions. The consequences of poor chemistry control can be severe. Plate out of noble metals in the salt is expected and can aid in reducing corrosion on surfaces by providing a protective layer. When fissile materials are allowed to plate out they can collect in areas like heat exchangers and result in unintended criticality [35].

Salt chemistry is slowly changing, the associated systems are important to the operation and safety of the facility, but the plant can maintain safe operation and shut down should these systems become disabled. Problems occur when measurements of salt conditions are inaccurate over larger time scales. The measurements of salt chemistry should be considered highly critical and sensitive for the safety of the system and for accurate accounting of material inventory. Accounting for the nuclear

material inventory will be one of the most difficult tasks in a liquid fuel MSR. The necessity of fuel materials being removed from the reactor frequently to be reprocessed makes accurate measurements of salt chemistry, and thus inventory, vital to security.

With the notable exception of integral MSRs, liquid fueled MSRs are defacto fuel reprocessing facilities. They must remove neutron poisons and the corrosive and gaseous fission products from the fuel salt [36]. Scalable methods for reprocessing fuel salt enable the possibility of removing fissile materials from the salt. Depending on the process, these materials may be of significant purity and certainly constitute a proliferation risk. This makes the accountancy of materials in the salt of vital importance from both an operational and a proliferation standpoint. Any part of the facility that measures salt composition and processes the salt must considered high consequence security areas and control systems.

The reduction of dependance on high reliability safety and control systems could be interpreted as greater resilience to cyber and physical security threats. This can be true in the sense that conventional fuel damaging events are not physically possible. However, due to the need of continuous separation and removal of fission products, large amounts of radioactive material and gas are collected and stored outside of the reactor. The release or theft of these materials constitute a serious risk and a potential target for cyber-physical attacks.

Table 5-10. General design parameters the chloride fast reactor surveyed (Terrapower's Molten Chloride Fast Reactor) [32]

Reactor Type: Chloride fast reactor	Secondary Coolant: Unreported
Rx Thermal Power: 600-2500 MW	Cooling Method: Forced convection
Rx Electric Power: 228-950 MW	Power Conversion: Unreported
Neutron Spectrum: Fast	Fuel Composition: Uranium chloride (UCl3 or UCl4)
Operation Lifetime: Unreported	Fuel Arrangement: Liquid fuel salt
Refueling Cycle: Continuous	Fuel Enrichment: Unreported
Primary Coolant: Chloride salt	Moderator: None

Table 5-11. General physical components of MSRs surveyed with unique I&C considerations

Physical Components	Function	Possible Sensor Data	Unique Physical Limits
Fuel salt reprocessing system	Removes neutron poisons and corrosive agents from the fuel salt	Flowrates Tank levels Mass spectrums Fuel inventory	Requires extremely volatile chemicals for fuel separation Large on-site fuel inventory

Physical Components	Function	Possible Sensor Data	Unique Physical Limits
			Radioisotopes are converted to gaseous/liquid states introducing unique, potential release mechanisms
Corrosion monitoring system	Monitors structural health of reactor components and chemical purity of the molten salt	Mass spectrums Opacity Material samples	Local freezing and salt eutectics due to component corrosion is difficult to model/measure
Fuel catch system	Emergency reservoir for nuclear fuel	State of reservoir (Open/closed) Neutron flux Temperature Air/water ingress	Passive systems operate given complete loss of on-site electrical power. Additional systems may be needed to further isolate the emergency reservoir

5.5.2. Solid Fueled Molten Salt Reactors

Many of the chemistry and radiological challenges present in liquid fueled MSR designs can be mitigated by containing the fuel in solid form. Instrumentation on the primary coolant loop will have the advantage of a reduced radiation environment compared to their liquid fueled counter parts. The designs receiving the greatest consideration are those that contain their fuel in multi-layer pebbles with embedded TRISO fuel particles. Effectively the same fuel configuration that many pebble bed high temperature gas reactors (HTGRs) intend to use [37]. These fuel pebbles can self-pack in a pebble bed configuration in a graphite reflected core. Reactivity is maintained with control rods in the graphite reflector. The major difference between these reactors and HTGRs is the coolant which requires special considerations.

Though the fuel is not dissolved in the salt and is much cleaner, it still requires purification. Fluoride-Lithium-Beryllium (FLiBe) salt is the selected coolant for these reactors for its neutronic and thermal properties. The lithium in FLiBe captures neutrons and forms tritium, which must be captured from the salt. If allowed to absorb into the core and pebble graphite, tritium will degrade the structural integrity of the nuclear graphite. Fission products and fuel material can be released into the salt from broken or damaged pebbles. To keep the salt clean, it is filtered through activated carbon [38]. The control system will need to monitor tritium concentration in the salt to ensure the condition of the filters and integrity of the nuclear graphite in the core. Additionally, fission product concentration in the salt will need to be monitored to ensure the condition of the fuel pebbles.

With the fuel in solid form the reactivity feedback from thermal expansion is far less than that of the liquid fueled MSR. The primary thermal feedback is doppler broadening, which is less effective than that of thermal expansion of liquid fuel [39]. As a result, reactivity control is more dependent on the control rods, and safe shut down should be assured with redundant negative reactivity insertion systems. One such system suggested is the use of neutron absorbing blades that would be driven into the pebble bed [40]. These safety and control systems would need to be highly reliable and secure.

One of the benefits shared with liquid fueled MSR's is the ability to continuously refuel. With the pebble bed reactors this is accomplished be continuously exchanging the pebbles. Unlike high temperature GCR's, pebbles are extracted at the top of the core as they are buoyant in the salt coolant [41]. Pebbles are removed and sorted by a pebble fragment sorting system that separates fragments of damaged pebbles from intact pebbles. The intact pebbles are then analyzed to determine burn up and mechanical condition. High burn up pebbles are rejected to spent fuel storage while low burn up pebbles are returned to the reactor. This system constitutes one of the most complex systems in the plant and is intended to operate automatically. The control system for the pebble handling system will be highly complex and the spent pebble storage will need to be monitored to ensure sub-critical configuration of the pebbles in storage.

Though the control systems of pebble bed salt cooled reactors are aided by some of the inherent physics-based safety of the reactor, they must still rely on the function of control and safety rods to safely shut down the reactor. A coolant salt chemistry monitoring and filtration system will be required to maintain the condition of the coolant. The control system will also include a complex pebble handling system and inventory control system.

Table 5-12. General design parameters of the fluoride salt cooled reactor surveyed (Hermes Reduced-Scale Test Reactor) [38]

Reactor Type: Fluoride salt cooled reactor	Secondary Coolant: 60/40 nitrate salt or solar salt
Rx Thermal Power: 320 MW	Cooling Method: Forced convection
Rx Electric Power: 140 MW	Power Conversion: Steam Rankine Cycle
Neutron Spectrum: Thermal	Fuel Composition: Uranium oxycarbide (UCO), TRISO particles in fuel pebbles
Operation Lifetime: 20 years (vessel) 80 years (plant)	Fuel Arrangement: Pebble Bed
Refueling Cycle: Continuous Refueling	Fuel Enrichment: ~19.75% U-235
Primary Coolant: LiF-BeF2	Moderator: Graphite

Table 5-13. General physical components of solid fuel MSRs surveyed with unique I&C considerations

Physical Components	Function	Possible Sensor Data	Unique Physical Limits
Fuel salt filtration system	Removes tritium and fission products from the coolant salt	Flowrates Mass spectrums Tritium concentration	Requires condition monitoring of activated carbon filters

Physical Components	Function	Possible Sensor Data	Unique Physical Limits
			Gaseous fission products and tritium must be contained Must ensure tritium does not degrade nuclear graphite
Corrosion monitoring system	Monitors structural health of reactor components and chemical purity of the molten salt	Mass spectrums Opacity Material samples	Local freezing and salt eutectics due to component corrosion is difficult to model/measure
Fuel pebble handling system	Maintain correct reactor fuel loading	Radiation spectrum from pebble Pebble mechanical condition Position measurements from pebble recovery, disposal, and loading mechanical systems	Highly complex mechanical pebble handling system Large number of measurements and sensors to determine pebble burn up and condition Requires complex control logic
Passive Residual Heat Removal System	Emergency heat removal	Flowrate Inlet/outlet temperature	In emergency situations verification that the emergency heat removal system has properly engaged could be challenging given the passive nature of the system and loss of on-site power.

6. CONCLUSIONS

Previous work on NPP OT architectures has highlighted that next generation reactors will need novel control systems to accommodate unique physical and operational characteristics. These systems have yet to be deployed and collecting information on these new designs remains challenging. Nevertheless, a key aspect of the security analysis will be to determine the impact of passive safety features on OT architecture and the potential for degradation of passive safety systems during an attack. Such an analysis can be coupled with a safety analysis using a spectrum of hazards approach. Overall, the concept of OT architecture presented in this report can provide a framework to begin to unify safety and security-based analysis to mitigate architectural vulnerabilities in the design phase.

It has been widely shown, in a broad range of domains, that a suboptimal architecture leads to inherent vulnerabilities, lack of operational resilience, and future inflexibility. This is true for generation II reactors, which have shown that ad hoc security is expensive, inefficient, and cannot fully address security concerns in some cases. Current and future research projects in OT architectures for ARs are prioritizing system resilience under attack, advanced intrusion detection systems, joint cyber-physical security operation centers, and novel risk assessment methodologies and tools. Basing future risk assessment methodologies on quantifiable and reproduceable metrics, as well as coordinating with safety requirements is key.

Based on surveying twelve reactor designs it was found that the OT architecture of ARs are underdeveloped, and a domain-driven approach is being taken for each facet of the reactor design. This is despite the fact that the concept of safety and security architectures are well established, and advanced OT architectures need to leverage enabling technologies to be economically viable. Iterating on an OT architecture in the construction or operational phase of a system's lifecycle is prohibitively expensive. This may cause advanced reactors to run into similar architectural challenges faced by the generation II fleet.

A potential reason that AR designers have underdeveloped OT architectures is that vendors are not responsible for cyber initiated events and the security plan is produced and maintained by the licensee. The licensee is required to have a cybersecurity plan, which is reviewed by the NRC for compliance only. The NEI documents aid the industry on compliance with the cybersecurity rule without providing a quantifiable or reproducible security risk assessment. A graded approach is introduced in NEI 13-10, to reduce the number of security controls required by introducing four types of CDAs with varying security requirements. It is not rigorously specified however, how these CDAs are implemented within an OT architecture.

Designers of ARs will most likely seek further exceptions under a risk informed, technology inclusive framework citing passive safety features and field programmable gate array (FPGA) based control systems. The risk informed framework, NRC 10 CFR Part 53, is currently under development for ARs. Ultimately reactor licensees assume all long-term costs and regulatory burden with respect to the security plan. Inefficiency in security analyses may increase costs and the absorbed risks by licensees.

REFERENCES

[1] Zhang, F., Hines, J. W., and Coble, J. B., 2020, "A Robust Cybersecurity Solution Platform Architecture for Digital Instrumentation and Control Systems in Nuclear Power Facilities," Nucl Technol, 206(7), pp. 939-950.
[2] Guo, Y., Lou, X., Bajramovic, E., and Waedt, K., "Cybersecurity risk analysis and technical defense architecture: Research of ICS in nuclear power plant construction stage," Proc. Proceedings of the 3rd IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts (ICONS 2020).
[3] International Atomic Energy Agency, 2017, "Instrumentation and Control Systems for Advanced Small Modular Reactors," Vienna.
[4] Hahn, A., Sandoval, D. R., Fasano, R., and Lamb, C., 2021, "Automated Cyber Security Testing Platform for Industrial Control Systems," 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), A. N. Society, ed.
[5] Greenfield, D., 2020, "Is the Purdue Model Still Relevant?," https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant.
[6] International Atomic Energy Agency, TBD, "NST047 - Computer Security Techniques at Nuclear Facilities," Vienna.
[7] Rowland, M. T., Dudenhoeffer, D. D., and Purvis, J. S., 2017, "Computer Security for I&C Systems at Nuclear Facilities," Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC & HMIT 2017), pp. 11-15.16.
[8] NIST, 2015, "NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security."
[9] NIST, 2020, "NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations."
[10] International Electrotechnical Commission, 2019, "IEC 62645:2019: Nuclear power plants - Instrumentation, control and electrical power systems - Cybersecurity requirements," IEC, Geneva.
[11] International Electrotechnical Commission, 2019, "IEC 62859:2016/AMD1:2019 : Amendment 1 - Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity," IEC, Geneva.
[12] International Electrotechnical Commission, 2020, "IEC 63096: Nuclear power plants – Instrumentation, control and electrical power systems – Security controls," IEC, Geneva.
[13] C. Chenoweth, J. Green, T. Shaw, M. Shinn, G. Simonds, and J. Pezeshki, November 2014, "NUREG/CR-7141: The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors."
[14] Nuclear Energy Institute, 2010, " NEI 08-09: Cyber Security Plan for Nuclear Power Reactors."
[15] Nuclear Energy Institute, 2017, "NEI 13-10 Cyber Security Control Assessments Rev. 6."
[16] Wood, R. T., Joseph III, R. A., Korsah, K., Muhlheim, M. D., and Mullens, J. A., 2012, "Classification Approach for Digital I&C Systems at U.S. Nuclear Power Plants," U.S. NRC, Washington, DC,.
[17] Fasano, R., Hahn, A., James, J., Lamb, C., and Haddad, A., 2021, "Cyber-Physical Risks for Advanced Reactors," DOE NE Report M2CT-21SN1104024.
[18] EPRI, 2021, "HAZCADS: Hazards and Consequences Analysis for Digital Systems – Revision 1," Palo Alto, CA.
[19] NRC, 1995, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement (60 FR 42622)," Federal Register.
[20] NRC, 2016, "Staff Safety Evaluation Report for NuScale Power, LLC Licensing Topical ReportTR-0515-13952-NP, "Risk-Significance Determination," Revision 0 (ML16181A218)."

[21] NRC, 2021, "NuScale Small Modular Reactor Design Certification (NRC-2017-0029),"Federal Register.
[22] NRC, 2017, "SAFETY EVALUATION OF THE NUSCALE POWER, LLC TOPICAL REPORT TR-0815-16497-P, "SAFETY CLASSIFICATION OF PASSIVE NUCLEAR POWER PLANT ELECTRICAL SYSTEMS," REVISION 1 (ML17205A380)."
[23] NuScale, 2019, "Accident Source Term Methodology (TR-0915-17565)."
[24] NuScale, 2015, "NuScale Power, LLC Submittal of NuScale Preliminary Concept of Operations Summary and Response to NRC Questions on Control Room Activities (NRC Project No. 0769) ".
[25] NuScale, 2021, "Lessons-Learned from the Design Certification Review of the NuScale Power, LLC Small Modular Reactor."
[26] El-Genk, M. S., 1994, A Critical Review of Space Nuclear Power and Propulsion 1984-1993.
[27] Poston, D. I., Gibson, M. A., Sanchez, R. G., and McClure, P. R., 2020, "Results of the KRUSTY Nuclear System Test," Nuclear Technology, 206(sup1), pp. S89-S117.
[28] ARC Clean Energy, 2021, "ARC-100," https://www.arcenergy.co/.
[29] TerraPower, 2021, "Natrium," https://www.terrapower.com/our-work/natriumpower/.
[30] Ruggieri, J.-M., Ren, L., Glatz, J.-P., Ashurko, I., Hayafune, H., Kim, Y., and Hill, R., 2017, "Sodium-Cooled Fast Reactor (SFR) System Safety Assessment," GEN IV International Forum.
[31] Qvist, S., and Greenspan, E., 2014, "An Autonomous Reactivity Control system for improved fast reactor safety," Progress in Nuclear Energy, 77, pp. 32-47.
[32] Aoto, K., Dufour, P., Hongyi, Y., Glatz, J. P., Kim, Y.-i., Ashurko, Y., Hill, R., and Uto, N., 2014, "A summary of sodium-cooled fast reactor development," Progress in Nuclear Energy, 77, pp. 247-265.
[33] Singh, V., Lish, M. R., Chvala, O., and Upadhyaya, B. R., 2017, "Dynamics and control of molten-salt breeder reactor," Nuclear Engineering and Technology, 49, pp. 887-895.
[34] Elsheikh, B. M., 2013, "Safety assessment of molten salt reactors in comparison with light water reactors," Journal of Radiation Research and Applied Sciences, 6(2), pp. 63-70.
[35] Holcomb, D., Kisner, R., and Cetiner, S., 2018, "Instrumentation Framework for Molten Salt Reactors," Oak Ridge National Laboratory, Oak Ridge, TN.
[36] Holcomb, D. E., Flanagan, G. F., Patton, B. W., Gehin, J. C., Howard, R. L., and Harrison, T. J., 2011, "Fast Spectrum Molten Salt Reactor Options," Oak Ridge National Laboratory, Oak Ridge, Tennessee.
[37] Power, K., 2018, "Design Overview of the Kairos Power Fluoride Salt-Cooled, High Temperature Reactor," NRC.
[38] Forsberg, C. W., Carpenter, D. M., Whyte, D. G., Scarlat, R., and Wei, L., 2017, "Tritium Control and Capture in Salt-Cooled Fission and Fusion Reactors," Fusion Science and Technology, 71(4), pp. 584-589.
[39] Cisneros, A. T., Scarlat, R. O., Laufer, M. R., Greenspan, E., and Peterson, P. F., "Pebble Fuel Design for the PB-FHR," Proc. ICAPP.
[40] Chang, S., Gonzalez, A., Kong, J., and Satterlee, N., 2012, "PB-FHR Reserve Shutdown System," No. UCBTH-12-008, University of California, Berkeley.
[41] Vergari, L., and Fratoni, M., 2021, "Spent fuel management strategies for fluoride-cooled pebble bed reactors," Nuclear Engineering and Design, 378.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Technical Library	01977	sanddocs@sandia.gov

This page left blank

Sandia National Laboratories

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