Advanced Reactor Safeguards & Security

Design of Defensive Cybersecurity Architectures for Sodium-Cooled Fast Reactors

Prepared for
US Department of Energy

Lee T. Maccarone, Robert J. Brulles, Michael T. Rowland, Jenna deCastro

Sandia National Laboratories

September 2025

SAND2025-12466R

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

This report presents the design of defensive cybersecurity architectures (DCSAs) for Sodium-Cooled Fast Reactors (SFRs). A DCSA is a cybersecurity design feature that places systems into security zones in a graded approach according to the importance of the functions performed by the systems. DCSA design efforts for advanced reactors may commence as early as the system-level design phase. This design approach is consistent with the draft regulatory guide for advanced reactor cybersecurity programs (DG-5075) and enables advanced reactor designers to consider the effects of security-by-design (SeBD) features on their DCSAs. Integration of DCSA design and other cybersecurity activities with the traditional design process as part of a SeBD framework may enable advanced reactor designers to improve the security posture of their plants while reducing implementation and operating costs. This report provides a DCSA template for an exemplar SFR and how the template may be optimized for a given SFR design.

ACKNOWLEDGEMENTS

This report was written for the Advanced Reactor Safeguards and Security program area in the U.S. Department of Energy Office of Nuclear Energy and satisfies milestone M3RS-25SN0702011. The authors would like to acknowledge the program leadership provided by Dan Warner (DOE-NE) and Ben Cipiti (Sandia National Laboratories).

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

EXECUTIVE SUMMARY

A defensive cybersecurity architecture (DCSA) is a key cybersecurity design feature to prevent access to attack pathways to those digital technologies that perform or support significant functions of advanced reactors (ARs). The International Atomic Energy Agency (IAEA) defines a DCSA as the "Arrangement of [digital] systems according to the design requirements, constraints and measures that are to be imposed during the life cycle of a system, such that systems that perform identified facility functions of significance to the safety and security of the facility and that are assigned to computer security levels at the facility level have the required level of protection" [1]. The DCSA aims to provide increasing protection based on significance of the functions to safety, security, or safeguards (3S). The increasing protection is key to ensure that the adversary will need to overcome multiple, diverse, and independent measures prior to successfully completing an attack.

This report evaluates the instrumentation and control (I&C) architecture and interdependencies of sodium-cooled fast reactors (SFRs) to derive DCSA passive requirements. This analysis approach is consistent with the Tiered Cybersecurity Analysis (TCA) detailed in the U.S. NRC draft regulatory guide "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53" (DG-5075) [2]. The TCA approach presented in DG-5075 leverages the security-by-design (SeBD) features of the plant as the foundation of cybersecurity analysis. A DCSA designed as part of the DG-5075 approach is designed to deny the adversary access to the plant functions needed to cause an accident sequence that is unmitigated by the plant's physical design.

Security levels are assigned to functions based on their importance to plant safety. Systems that perform multiple functions are placed in a zone based on the security level assigned to the system's most important function. Based on the systems' functions, systems are categorized as being likely to be licensed as one of the following categories for systems, structures, and components (SSCs): safety-related (SR), non-safety related with special treatment (NSRST), or non-safety related with no special treatment (NST) [3, 4, 5]. Security levels are assigned based on these classifications.

The resulting DCSA template is shown in Figure 1. This DCSA template is consistent with both the RG 5.71 approach and the DG-5075 approach.

Security level 1 consists of a zone containing the information technology (IT) network, business systems, and engineering systems. Systems in this level have access to the Internet via a firewall and wireless networks are permitted. Portable media and mobile devices (PMMD) are widely used in these systems within this security level.

Security level 2 consists of three zones containing authorized document management systems, work control systems, and the engineering historian. PMMD are used within systems in these security levels. Bidirectional wired network communication through a firewall is permitted between security levels 1 and 2.

Security level 3 consists of several zones containing both NSRST and NST plant systems and supervisory control systems. The main control room (MCR) human-machine interface (HMI) and Distributed Control System (DCS) serve as supervisory controllers. Any PMMD brought from a lower security zone to a zone belonging to security level 3 must first be processed through a portable media and mobile device scanner. Wired network communication into security level 2 from security level 3 is permitted (e.g., the engineering historian receives data from the operations historian), but security level 2 is only permitted to send handshaking or acknowledgement signals to security level 3.

Security level 4 consists of two zones containing the plant SR systems. Analog signals are used for communications from the RPS to RSS. Any PMMD brought into security level 4 must first be scanned. One-way communication enforced by a data diode is permitted from security level 4 to security levels 3 and 2.

DCSA requirements are associated with passive measures focusing on denial of adversary access through the eliminating, mitigating, or controlling attack pathways. There are five commonly accepted attack pathways:

1. Physical Access
2. Wired Network Connectivity
3. Wireless Network Connectivity
4. Portable Media and Mobile Device
5. Supply Chain.

This report excludes supply chain attack pathway due to the need to impose requirements on external parties. These requirements are not reflected in passive DCSA elements, although active DCSA requirements may detect supply chain compromises.

Cybersecurity controls in nuclear facilities are essential to maintain the integrity and safety of CDAs against a wide range of cyber threats. Within the context of DCSA, cybersecurity controls may be applied to support the three defensive strategies: (1) fortification, which strengthens defenses around CDAs; (2) chokepoints, which limit control access to critical systems; and (3) anti-access/area denial, which prevents unauthorized access to sensitive areas. Together, these strategies achieve defense-in-depth (DiD) and support a comprehensive cybersecurity framework designed to detect, prevent, and respond to cyber attacks.

This report was written to demonstrate DCSA design approaches and to provide a template DCSA design for an SFR to be available for industry use. It is important to note that the DCSA design template and cybersecurity controls provided in this report are intended to serve as starting points for AR designers and are not prescriptive. Further optimization of the DCSA and controls may be valuable given the unique design and performance requirements of the plant.

This report is similar in structure to the previous report that developed a DCSA design for a high-temperature, gas-cooled reactor (HTGR) [6]. In comparison to the HTGR report, this report offers expanded discussion on the defensive strategies and their relationships, and an expanded treatment of cybersecurity controls within the context of the DCSA design. Cybersecurity controls from U.S. NRC RG 5.71 are identified and aligned with the defensive strategies, and example implementations of the technical controls are provided. These controls examples and the relationships between defensive strategies provide a useful basis for the development of a cybersecurity plan. For additional background material on DCSA and for a DCSA design approach leveraging probabilistic risk analysis (PRA), readers are encouraged to refer to [6].

The application of technical controls to specific systems in addition to a base level of security requirements provided by the security level is likely to result in additional DCSA design improvements via the DG-5075 approach. Potential DCSA design improvements include the merging of zones and reassignment of lower security levels to certain zones as appropriate to the unique plant design. Further research is needed to evaluate the sufficiency of these controls for their impact on DCSAs to be realized.

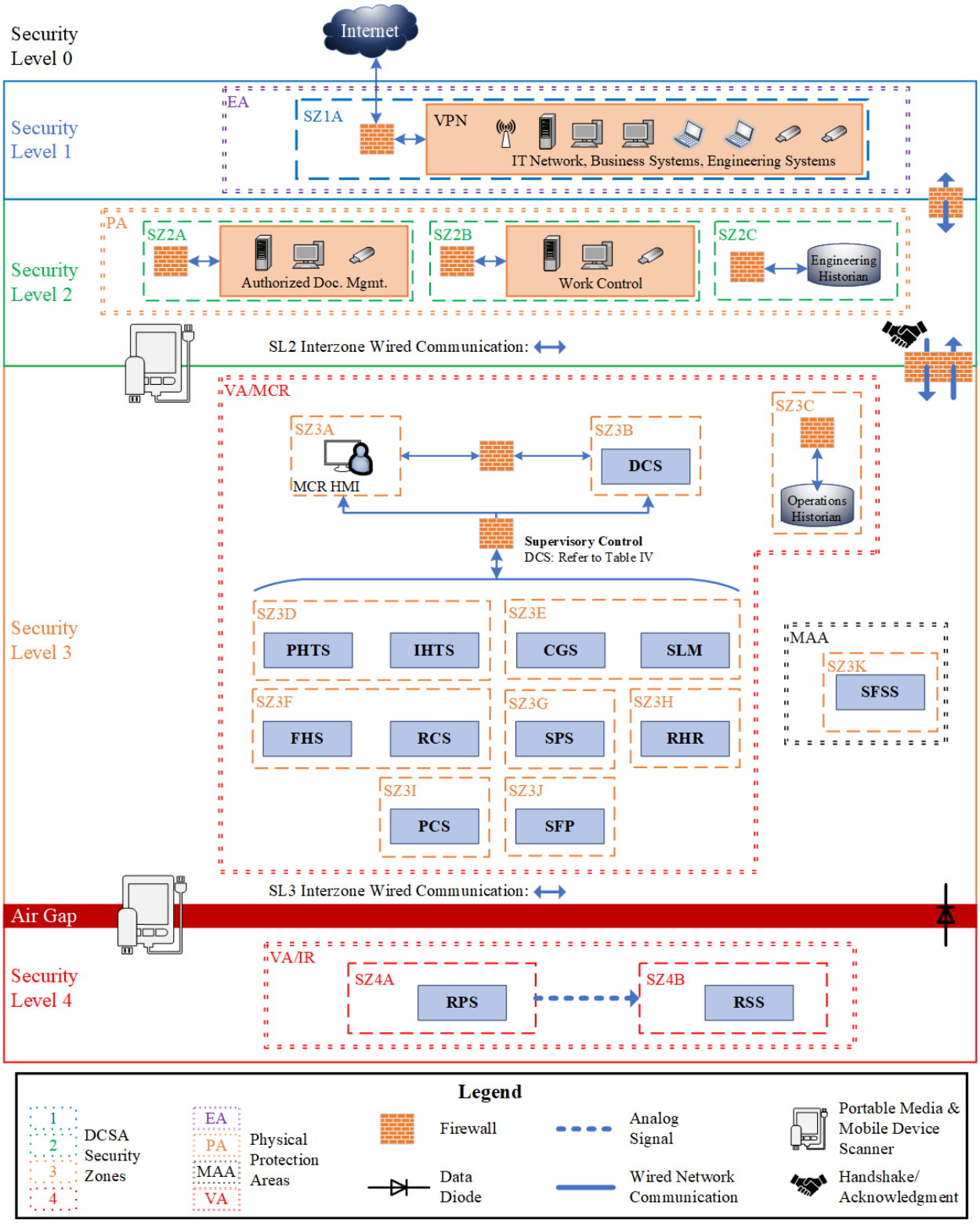

Figure 1. SFR DCSA Template

This page left blank

ACRONYMS AND TERMS

Acronym/Term	Definition
ACL	Access control list
AFSA	Adversary Functional Scenario Analysis
AOO	Anticipated operational occurrence
API	Application programming interface
APT	Advanced persistent threat
AR	Advanced reactor
ARC	Advanced Reactor Concepts
BDBE	Beyond design basis event
BIOS	Basic Input/Output System
BN	Bistrye Neitrony (Fast Neutron)
BOR	Broya Opytnaya Reaktor (Boiling Experimental Reactor)
CAD	Computer-aided design
CCTV	Closed-circuit television
CDA	Critical digital asset
CEAS	Cyber Extension to Safety Accident Scenario Analysis
CFR	Code of Federal Regulations
CGS	Cover Gas System
CLI	Command-line interface
CSP	Cybersecurity plan
DBA	Design basis accident
DBE	Design basis event
DBT	Design basis threat
DCS	Distributed Control System
DFR	Dounreay Fast Reactor
DCSA	Defensive cybersecurity architecture
DG	Draft guide
DHX	Direct heat exchanger
DiD	Defense-in-depth
DMZ	Demilitarized zone
DRACS	Direct Reactor Auxiliary Cooling System
EA	Exclusion area
EBR	Experimental Breeder Reactor
EPRI	Electric Power Research Institute
ESF	Engineered safety feature

Acronym/Term	Definition
ESF	Event sequence frequency
FBTR	Fast Breeder Test Reactor
FFTF	Fast Flux Test Facility
FHS	Fuel Handling System
FHSS	Fuel Handling and Storage System
FSS	Fuel Storage System
FW	Firewall
GPO	Group policy object
HMI	Human-machine interface
HTGR	High temperature, gas-cooled reactor
HTS	Heat Transfer System
IAC	Intermediate Air Cooling System
IAEA	International Atomic Energy Agency
I&C	Instrumentation and control
IDPS	Intrusion detection and prevention systems
IDS	Intrusion detection system
IHTS	Intermediate Heat Transfer System
IP	Internet Protocol
IPL	Independent protection layer
IR	Instrumentation room
IRACS	Intermediate Reactor Auxiliary Cooling System
ISO	International Standards Organization
ISP	Intermediate sodium pump
IT	Information technology
KNK	Kompakte Natriumgekuehlte Kernreaktoranlage (Compact Sodium-Cooled Nuclear Reactor)
LAA	Limited access area
LOCA	Loss-of-coolant accident
LWR	Light water reactor
MAA	Material accountability area
MAC	Media access control
MCR	Main Control Room
MFA	Multi-factor authentication
ML	Main line
NDHX	Natural draft heat exchanger

Acronym/Term	Definition
NGIPS	Next-generation intrusion prevention system
NPP	Nuclear power plant
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSRST	Non-safety related with special treatment
NSS	Nuclear Security Series
NST	Non-safety related with no special treatment
NTP	Network Time Protocol
PA	Protected area
PAM	Privileged access management
PCR	Platform configuration register
PFBR	Prototype Fast Breeder Reactor
PFR	Prototype Fast Reactor
PHTS	Primary Heat Transfer System
PII	Personally identifiable information
PMMD	Portable media and mobile devices
PRA	Probabilistic risk assessment
PRACS	Primary Reactor Auxiliary Cooling System
PRISM	Power Reactor Innovative Small Module
PSP	Primary sodium pump
RAC	Reactor Air Cooling System
RB	Reactor building
RCCS	Reactor Cavity Cooling System
RCS	Reactivity Control System
RCSS	Reactivity Control and Shutdown System
RF	Radio frequency
RHR	Residual Heat Removal System
RPS	Reactor Protection System
RSS	Reserve Shutdown System
RG	Regulatory guide
RVACS	Reactor Vessel Auxiliary Cooling System
SCPCS	Steam Cycle Power Conversion System
SeBD	Security-by-design
SEFOR	Southwest Experimental Fast Oxide Reactor
SFR	Sodium-cooled fast reactor

Acronym/Term	Definition
SFSS	Spent Fuel Storage System
SFP	Sodium Fire Protection System
SG	Steam generator
SGACS	Steam Generator Auxiliary Cooling System
SIEM	Security information and event management
SL	Security level
SLM	Sodium Leak Management System
SMB	Server Message Block
SMR	Small modular reactor
SNR	Schneller Natriumgekühlter Reaktor (Fast Sodium-Cooled Reactor)
SOC	Security operations center
SPAN	Switched port analyzer
SPS	Sodium Processing System
SR	Safety-related
SSCs	Systems, structures, and components
SSH	Secure Shell
SSID	Service set identifier
STPA	Systems-Theoretic Process Analysis
SZ	Security zone
TAM	Technical Assessment Methodology
TCA	Tiered Cybersecurity Analysis
TCP	Transmission Control Protocol
THETA	Thermal Hydraulic Experimental Test Article
TKIP	Temporal Key Integrity Protocol
TLS	Transport layer security
TTPs	Tactics, techniques, and procedures
UPS	Uninterruptible power supply
VA	Vital area
VCCS	Vessel Cavity Cooling System
VLAN	Virtual local area network
VM	Virtual machine
VRF	Virtual routing and forwarding
WNA	World Nuclear Association
WPA	Wi-Fi Protected Access

1. INTRODUCTION

A defensive cybersecurity architecture (DCSA) is a key cybersecurity design feature to prevent access to attack pathways to those digital technologies that perform or support significant functions of advanced reactors (ARs). The International Atomic Energy Agency (IAEA) defines a DCSA as the "Arrangement of [digital] systems according to the design requirements, constraints and measures that are to be imposed during the life cycle of a system, such that systems that perform identified facility functions of significance to the safety and security of the facility and that are assigned to computer security levels at the facility level have the required level of protection" [1]. A DCSA aims to apply a graded approach and implement defense-in-depth (DiD) by providing sufficient protection to functions important to safety, security, or safeguards (3S). A DCSA needs to ensure that the adversary must overcome multiple, diverse, and independent measures of increasing robustness prior to successfully completing an attack.

Most nuclear power plants (NPPs) in the U.S. commercial fleet were designed, implemented, and initially operated without considerations for cybersecurity. The absence of cybersecurity design features resulted in cybersecurity controls being "wrapped-around" systems to prevent access of adversaries to significant and vulnerable components of these systems. The existing fleet leverages a combination of strict physical protection, isolation, and air-gaps to reduce cybersecurity risks to meet U.S. Nuclear Regulatory Commission (NRC) guidance. These air-gapped systems require strong on-site physical protection, access control, and extensive measures to track and control portable media and mobile device usage. Often, this results in the construction of a single large layer within the DCSA that requires extra effort to physically protect networks and components, and to manage access control.

AR designers can consider cybersecurity from the start of the design process to avoid the wrap-around security measures often applied for the existing fleet. Designers are considering effective cybersecurity as a fundamental part of the design basis of the reactor. This provides an opportunity to potentially reduce costs and effort in establishing effective cybersecurity programs via integration of cybersecurity analysis with the design process.

This report was written to demonstrate DCSA design approaches and to provide a template DCSA design for a sodium-cooled fast reactor (SFR) to be available for industry use. It is important to note that the DCSA design template provided in this report is intended to serve as a starting point for AR designers and is not prescriptive. Further optimization of the DCSA design may be valuable given the unique design and performance requirements of the plant.

This report evaluates the instrumentation and control (I&C) architecture and interdependencies of an SFR to derive DCSA passive requirements. This analysis approach is consistent with the Tiered Cybersecurity Analysis (TCA) detailed in the U.S. NRC draft regulatory guide "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53" (DG-5075) [2]. The TCA approach presented in DG-5075 leverages the security-by-design (SeBD) features of the plant as the foundation of cybersecurity analysis. A DCSA designed as part of the TCA approach is designed to deny the adversary access to the plant functions needed to cause an accident sequence that is unmitigated by the plant's physical design.

This report is similar in structure to the previous report that developed a DCSA design for a high-temperature, gas-cooled reactor (HTGR) [6]. A brief background section is presented with essential DCSA material, but for greater discussion readers are encouraged to refer to [6]. The introductory material in this report contains an expanded discussion on the defensive strategies contributing to effective DCSA design. This report also offers an expanded treatment of cybersecurity controls

within the context of the DCSA design. Cybersecurity controls from U.S. NRC RG 5.71 are identified and aligned with the defensive strategies, and example implementations of the technical controls are provided. These controls examples and the relationships between defensive strategies provide a useful basis for the development of a cybersecurity plan.

This report aims to develop requirements for passive DCSA measures by:

- Indicating the stringency of the requirements (i.e., security level) for each function and its associated system.
- Aligning technical and operational cybersecurity controls from U.S. NRC RG 5.71 with the defensive strategies.
- Assigning applicable technical and operational cybersecurity controls to each security level and providing examples of technical implementations.

2. BACKGROUND

This section provides a conceptual overview of advanced reactor SeBD considerations, DCSAs, and defensive cybersecurity strategies. Much of this section is quoted or based on material in the previous HTGR DCSA report [6]. Sections 2.1-2.3 are minimally quoted from [6] because they provide essential background material on SeBD for this report. Please refer to [6] for expanded versions of these sections. Section 2.4 expands the discussion of defensive strategies in [6] to provide a literature review of the strategies and an explanation of their fundamental relationships.

2.1. The Tiered Cybersecurity Analysis (TCA)

Under the United States Nuclear Regulatory Commission (US NRC) Regulatory Guide 5.71 [7], licensees of light water reactors (LWRs) have been required to broadly apply a large set of technical and operational cybersecurity controls to all identified critical digital assets (CDAs). For advanced reactors (ARs), this asset-centric approach places a large time and resource burden on the licensee and does not allow the licensee the flexibility to prioritize the systems with the greatest potential for physical harm. The U.S. NRC staff has recommended the addition of 10 CFR Part 53, "Risk-Informed, Technology-Inclusive Regulatory framework for Commercial Nuclear Plants" and provided a draft proposed Part 53 rulemaking package to the Commission (SECY-23-0021) [8, 9].

The U.S. NRC has published a draft regulatory guide "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53" (DG-5075) [2]. The methodology is pre-decisional, but the concepts are referred to in this report as the Tiered Cybersecurity Analysis (TCA). The TCA is a cybersecurity assessment methodology that aligns domestic standards, international standards, and technical guidance to select SeBD requirements to develop defensive network architectures and apply effective cybersecurity controls [10, 11].

The TCA consists of three tiers and is shown in Figure 2. Tier 1 is Design Analysis and focuses on evaluating the capability of SeBD features to eliminate or mitigate accident sequences caused by a cyber-adversary who is limited only by the physics of the plant design. Tier 2 is Denial of Access Analysis and focuses on developing passive Defensive Cyber Security Architecture (DCSA) features and passive cybersecurity plan (CSP) controls to deny the adversary access to the functions needed to conduct attacks that were not eliminated by SeBD features. Finally, Tier 3 is Denial of Task Analysis and focuses on preventing the adversary from conducting the specific tasks needed to conduct attacks that are not eliminated by SeBD or prevented by denial of access. The outcome of Tier 3 analysis is the selection of active CSP controls. Further descriptions of each tier are provided in the following sections.

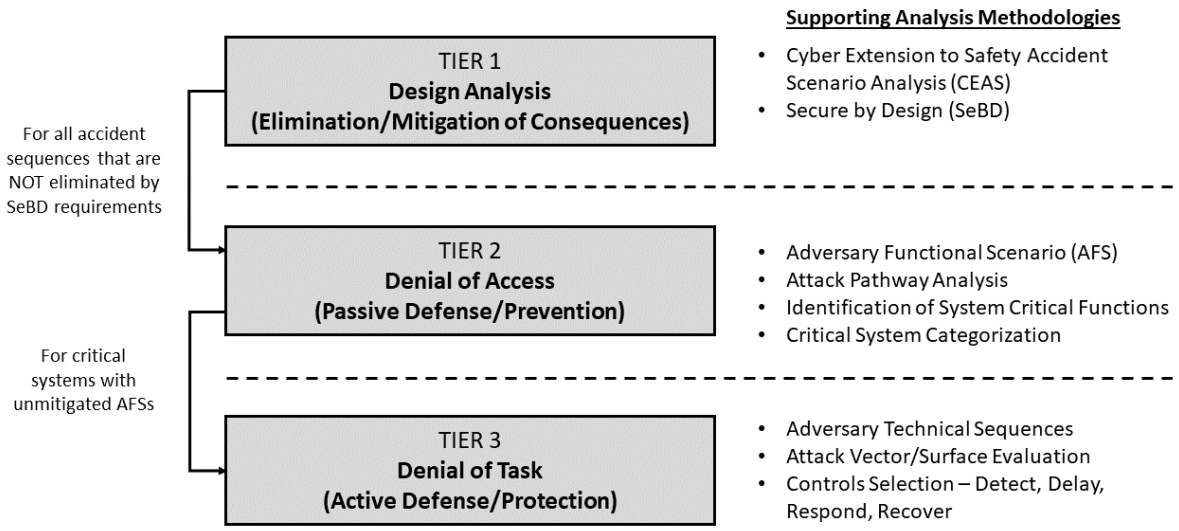

Figure 2: Tiered Cybersecurity Analysis (TCA) [12]

2.1.1. Tier 1 Analysis

The goal of Design Analysis is to evaluate the plant's safety design features and determine if they can be credited as SeBD features. Design features analyzed and verified to prevent an attack from leading to an unacceptable consequence from a specific scenario can be credited, therefore eliminating the need for a more detailed analysis of the scenario. In such cases, the design feature eliminates or avoids the evaluated impact(s) of an attack (e.g., radiological sabotage). Alternatively, some design features may delay or reduce an attack's impact. These design features are valuable to the security of the plant, but scenarios associated with these measures would still require Tier 2 analysis because the impact is not eliminated or avoided.

Tier 1 analysis is performed under the assumption that the adversary that is limited only by the physical design features of the plant design. This adversary is assumed to have access to any digital system, component, or network in the plant, and is assumed to be capable of implementing any control action within the capability of the system. Tier 1 findings that a scenario is mitigated by SeBD requirements cannot be invalidated by changes to the design basis threat because the adversary has already been assumed to have full control over the control surface of the plant. Supporting methodologies include Systems-Theoretic Process Analysis (STPA), analysis of the plant safety basis, and controlled process analysis [13]. Modeling and simulation are useful tools for conducting Tier 1 analysis [14, 15, 16, 17].

2.1.2. Tier 2 Analysis

The goal of Tier 2 analysis is "Denial of (adversary) Access" to functions (and associated systems) important to a set of scenarios with unacceptable consequences that are not addressed in Tier 1. Tier 2 evaluates adversary attack pathways[1] and identifies passive measures to deny adversary access to system and network.

[1] Attack pathways consist of (i) physical access, (ii) wired network connectivity, (iii) wireless network connectivity, (iv) portable media and mobile device, and (v) supply chain. Tier 2 does not consider supply chain attack pathway, as this pathway cannot be directly managed by the acquirer (e.g., licensee, vendor).

Adversary assumptions for Tier 2 include being able to achieve their objective if they gain access to the appropriate systems. Tier 1 scenarios and safety analyses are taken as inputs and used to identify adversary functional scenarios associated with unacceptable consequences. One method to represent attack sequences and bound the scope of scenarios is to use traditional PRA event trees [18]. Each plant function that must operate to mitigate an accident should be considered. This analysis should examine each system in the sequence of plant functions required for accident mitigation and identify available pathways for an adversary. The results of Tier 2 analysis are passive or deterministic DCSA or cybersecurity plan (CSP) elements. The analysis in this report aligns with Tier 2 analysis.

2.1.3. Tier 3 Analysis

The goal of "Denial of Task" Analysis is to provide risk-informed control measures to adversary functional scenarios that are not mitigated by the passive DCSA and CSP elements identified in Tier 2. In Tier 3, it is assumed that the adversary has obtained the access required to achieve their objective and control measures must be implemented to prevent the adversary from completing their objective. Generally, a body of controls may consist of baseline controls and risk-informed controls. Baseline controls apply broadly and provide information security assurance while risk-informed controls treat a specific identified risk. There are several methods that can be leveraged to identify applicable risk-informed controls (e.g., combining control action modeling using STPA and adversary sequence modeling using attack tree modeling).

2.2. Alignment of Cybersecurity Design Activities and Phases of Plant Design

The World Nuclear Association (WNA) has defined a series of four design maturity phases to describe the development of small modular reactors (SMRs) [19]. The design maturity phases are shown in Figure 3. The TCA can be aligned with the WNA phases of design maturity to enhance the efficiency of cybersecurity analysis throughout the design process. The proposed alignment of the TCA and WNA design phases is summarized in Table I. The concept and plant-level design phases align with Tier 1 of the TCA. Upon completion of these design phases, the impact of SeBD features can be analyzed. The system-level design phase aligns with Tier 2 of the TCA. This alignment occurs because the system-level design phase results in the design of I&C functional requirements and architectures and a DCSA is the primary output of Tier 2 analysis. The component-level design phase aligns with Tier 3 of the TCA. This alignment occurs because the component-level design phase provides the level of detail required to create the attack scenarios required for Tier 3 analysis. Improper alignment of the TCA with the WNA design phases may result in less efficient cybersecurity analysis and increased cybersecurity costs [10]. For additional information on this topic, please refer to [10, 20].

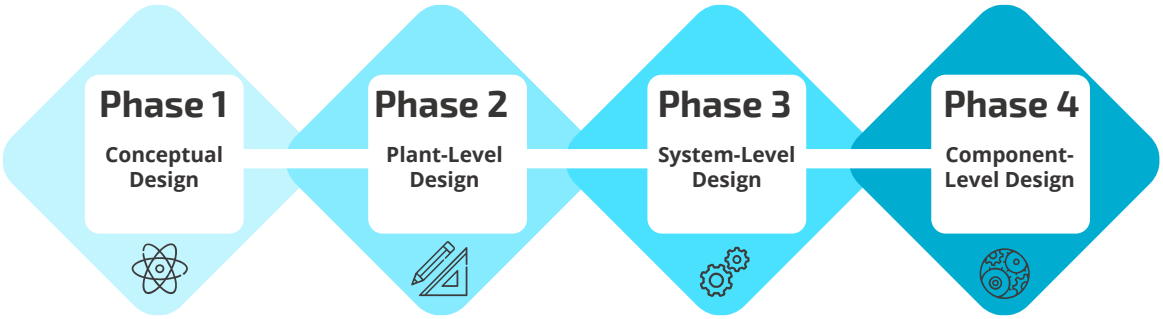

Figure 3: Plant Design Phases of Maturity [19]

Table I. WNA Design Phases and TCA Tiers [10]

WNA Design Phase	TCA Tier
Conceptual Design & Plant-Level Design	Tier 1 (Design Analysis)
System-Level Design	Tier 2 (Denial of Access)
Component-Level Design	Tier 3 (Denial of Task)

2.3. Defensive Cybersecurity Architectures

The U.S. NRC RG 5.71 states:

"An overall cybersecurity defensive strategy for a site must employ defense-in-depth strategies to protect CDAs from cyberattacks up to and including the DBT [design basis threat]. One acceptable method for achieving this goal is to incorporate a defensive architecture that establishes formal communication boundaries (or security levels) in which defensive measures are deployed to detect, prevent, delay, mitigate, and recover from cyberattacks. An example of such a defensive architecture is one that includes a series of concentric defensive levels of increasing security that conceptually correspond to existing physical security areas at a facility (e.g., vital area, protected area, owner-controlled area, corporate accessible area, public area)" [7].

The IAEA defines the features of DCSA in the Nuclear Security Series (NSS) publication 17-T [1]. Several key definitions are quoted below from NSS 17-T.

- Facility Function: "a coordinated set of actions and processes that need to be performed at a nuclear facility" [1].
- Security Level: "a designation that indicates the degree of security protection required for a facility function and consequently for the system that performs that function" [1].
- System: "A set of components which interact according to a design so as to perform a specific (active) function, in which an element of the system can be another system, called a subsystem" [21].
- Security Zone: "a logical and/or physical grouping of digital assets that are assigned to the same computer security level and that share common computer security requirements owing to inherent properties of the systems or their connections to other systems" [1].

The relationships between these four elements are shown in Figure 4. Figure 4 depicts relationships common in existing fleet, leveraging the wrap-around approach. Security level requirements are shown as only related to zone boundaries, as system designs of existing fleet are unlikely to consider

system changes for cybersecurity. However, the current design maturity of AR designs may allow for system design changes to simplify implementation and monitoring of cybersecurity as well as providing protection integrated within the system, unable to be bypassed by simple access to the internal areas of the zone.

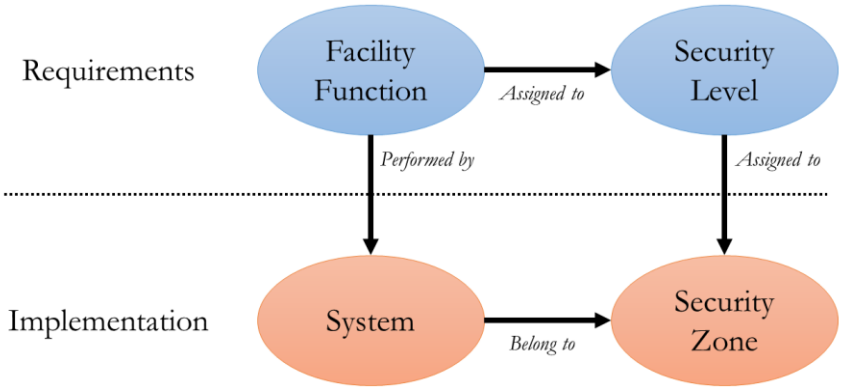

Figure 4. Relationship Between DCSA Elements (Adapted from [1])

A zone is a region bounded by logical and physical protections which contains at least one system. Communication between assets within a zone is trusted, while communication between different zones is restricted and controlled [1]. DCSA levels provide a framework for implementing a graded approach where security measures correspond to the significance of the functions assigned to each level. Each facility function is assigned a level based on its criticality. The stringency of measures put in place for a given level is directly related to the significance of the function protected by the level. Levels allow flexibility in security requirements across the facility which allows designers to prioritize the areas of greatest risk. Each level includes one or more zones. Zones enable DiD if systems performing redundant functions are placed in separate zones. By placing systems performing redundant functions in separate zone, the adversary is forced to compromise multiple zones in order to prevent the function from being performed. Figure 5 provides an example of how DCSA zones and levels would be implemented. Note that Figure 5 shows the level nomenclature used by U.S. NRC; IAEA follows a nomenclature that ranges from security level 1 to 5, with security level 1 receiving the most stringent security requirements.

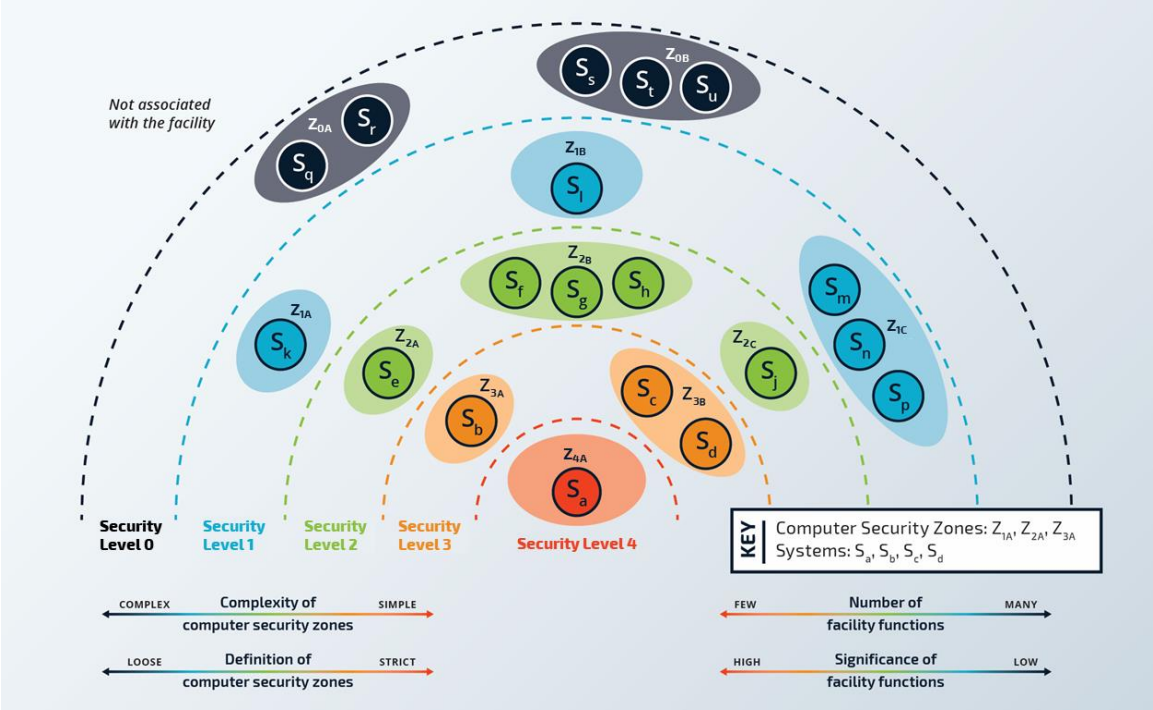

Figure 5. Conceptual DCSA Model [1]

Security levels are a fundamental concept necessary to apply a graded approach to cybersecurity. Security Levels are unique sets of graded requirements that provide the basis for selection of cybersecurity controls implemented within zones, including their boundaries.

The U.S. NRC RG 5.71 identifies five security levels as shown in Figure 6. DCSAs implemented within the existing fleet and the example provided in are based upon the Biba trust model [22]. Security levels 1-4 are applied to zones (and their composite systems and digital assets) that are owned by the licensee. Level 0 is the Internet.

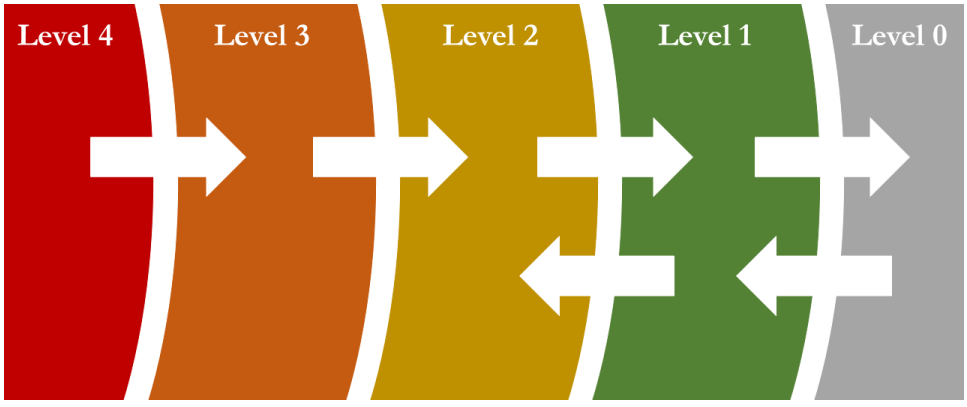

Figure 6. Simplified Defensive Cybersecurity Architecture [7]

Adhering to a graded approach, the set of requirements applied to Level 4 are significantly more stringent than the set of requirements at Level 1. There may also be common or generic requirements that apply to all security levels controlled by the licensee (i.e., Levels 4 through 1).

IAEA NSS 17-T provides an example set of requirements based on a wrap-around approach to security [1]. For IAEA Security Level 2, approximately equivalent to U.S. NRC Level 3, the example requirements (in addition to the generic requirements) listed are:

1. Only an outward, unidirectional networked flow of data is allowed from level 3 to level 2 systems (note: these levels have been translated from IAEA levels to U.S. NRC level equivalents).
2. Only necessary acknowledgement messages or controlled signal messages can be accepted in the opposite (inward) direction (e.g. for TCP/IP (Transmission Control Protocol/Internet Protocol)).
3. Remote maintenance is not allowed.
4. The number of staff given access to the systems is kept to a minimum, with a clear distinction between users and administrative staff.
5. Physical and logical access to systems is strictly controlled and documented.
6. Administrative access from other computer security levels is avoided. If this is not possible, such access is strictly controlled (e.g. by adopting the two person rule and two factor authentication).
7. All reasonable measures are taken to ensure the integrity and availability of the systems.

Requirements 1-3 focus on eliminating, prohibiting or strictly controlling the direction of network communications for the wired or wireless network pathways between zones assigned lower security levels. Requirements 4-6 impose management controls to control personnel and system access to zones (and systems) assigned security level 3. Finally, requirement 7 demands assessment of all measures that ensure integrity and availability to determine whether they can reasonably be applied. Reasonableness considerations may include cost, resources, feasibility to implement, and potential adverse impacts to system(s) behavior.

2.4. Defensive Cybersecurity Strategies

DCSA requirements are associated with passive measures focusing on denial of adversary access through the eliminating, mitigating, or controlling attack pathways. There are five commonly accepted attack pathways:

1. Physical Access
2. Wired Network Connectivity
3. Wireless Network Connectivity
4. Portable Media and Mobile Device
5. Supply Chain.

This report excludes supply chain attack pathway due to the need to impose requirements on external parties. These requirements are not reflected in passive DCSA elements, although active DCSA requirements may detect supply chain compromises.

The three types of defensive strategies detailed below provide key aspects of both passive and active defense [23, 24].

1. **Fortification:** A defensive barrier or other reinforcement built to strengthen a function, system, or zone against a malicious act. Fortification may include physical barriers and structures such as walls, hardened doors, or fences, or technical barriers such as cryptographic primitives, data diodes, and network segmentation. Approaches that enhance fortification are system hardening such as the removal of unnecessary ports and services.

Unnecessary system services must be removed or disabled from devices to reinforce them against vulnerabilities in these services [24].

2. **Chokepoint:** A strategic narrow route or gateway linking one zone, area, or network, to another. Chokepoints may include wired conduits between zones, entry control points to protected areas, and access points that connect adjacent networks. Chokepoints are most effective when all traffic is first forced to pass through it and provide a key location to deploy both authentication and detection technical measures. For example, network intrusion detection at the only chokepoint to a zone could monitor all communications entering and exiting that zone [24].
3. **Area or Access Control:** The selective restriction of either access or denial to a place or other resources. Access control aims to prevent adversarial access to either an internal area or components of zones and systems. Access control can be passive, such as USB port blockers, walls, locked doors, and filtering, or active, such as intrusion protection systems or transitions between operating modes [24].
4. **Deception:** False impersonation or mimicry of attractive targets to influence an adversary to attack them in place of real targets. This strategy involves the creation of decoys and honeypots to trick and trap adversaries, gain valuable threat intelligence, and update active defense measures. Deception may enable the disclosure and identification of threat actors' locations, names, and other information. Deception is generally not used within the existing fleet, but if wireless communications were to be implemented it would be beneficial to provide false wireless networks, among other targets, to gain situational awareness of potential local adversary activity. An active directory decoy could just be a dummy file system that notifies analysts when accessed [24].

Typically, these types of defensive strategies are combined into an overall plan for DiD to meet all requirements necessary to ensure sufficient cybersecurity. For example, deficient fortification of boundaries may allow an adversary to avoid or bypass a chokepoint, thereby avoiding the detection measures that have been implemented within the chokepoint. This is especially significant for wireless technologies, where the wireless signal may extend past the chokepoint thereby allowing an adversary to interact directly with devices and systems located on the protected side of the chokepoint.

U.S. NRC RG 5.71 specifies the need for:

1. A defensive architecture that describes a physical and logical network design that implements successive security levels separated by boundary control devices with segmentation within each security level [7].
2. A defensive strategy that employs multiple, diverse, and mutually supporting tools, technologies, and processes to effectively perform timely detection of, protection against, and response to a cyberattack [7].

The first element of the defensive architecture addresses prevention of access to successive layers of security. Access prevention is generally achieved via passive features. The second element to implement detection, protection, and response capabilities is addressed by active defensive features. These two elements are addressed within successive tiers (Tiers 2 & 3) of the TCA detailed within U.S. NRC DG-5075 [2]. The U.S. NRC's DiD concept is shown in Figure 7. The three defensive strategies are shown within this concept in Appendix A in [6].

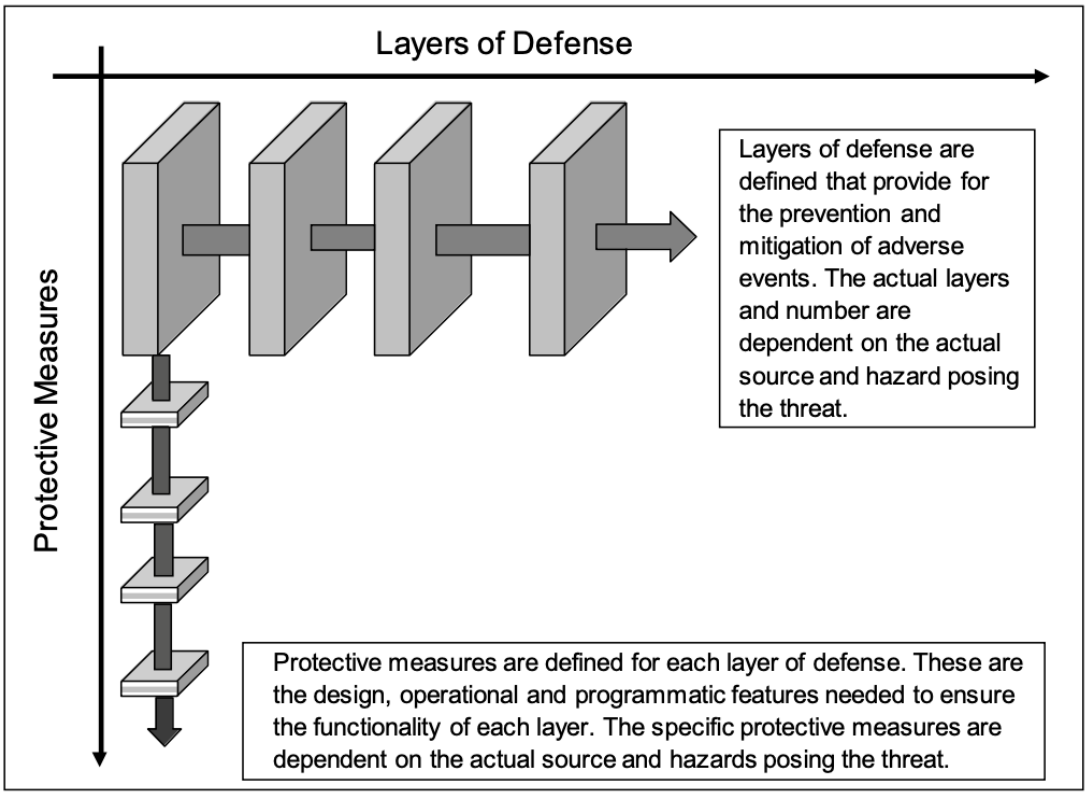

Figure 7. U.S. NRC's Defense-in-Depth Concept [25]

The remainder of this section describes the defensive strategies and their complementary nature in greater detail. The remainder of this section is quoted from a conference paper written over the course of this research [24].

2.4.1. Fortification

Fortification refers to the proactive strengthening of systems to make them resilient against attacks. Traditional security practices focused primarily on hardening systems by securing known attack vectors and ensuring that vulnerabilities were patched. However, in the modern threat landscape, fortification involves a multifaceted approach that adapts to evolving adversary tactics.

The National Security Agency (NSA) outlines several mitigation strategies that focus on fortifying systems to counter Advanced Persistent Threats (APTs). These strategies include immediate software updates, defending privileged accounts, and enforcing signed software execution policies. One key tactic discussed is rapidly applying patches to address discovered vulnerabilities before attackers can exploit them. The NSA stresses that automating the patching process is essential, as threats such as "N-day" exploits can be just as damaging as zero-day vulnerabilities. This approach emphasizes the need for continuous vigilance, ensuring that systems are updated regularly to minimize exposure to known threats [26].

Additionally, the concept of defendable architectures takes fortification a step further by focusing on a concept researchers termed “intelligence-driven defense”. The prevailing argument is that systems are protected purely through hardening, but the system may be made more resilient to a wide array of attack strategies by routinely gathering threat intelligence and leveraging it to enhance fortification strategies. The focus is on creating a defendable system that leverages information from past attacks

to either manually or automatically update system defenses. The authors argue that dynamic defense mechanism enables organizations to address not only current threats but also emerging tactics that may not have been anticipated at the time of the system's design; which is critical considering that tactics, techniques, and procedures (TTPs) evolve and therefore so should the defense to them. In this context, fortification becomes an ongoing process that continuously evolves as attackers develop new TTPs [27, 26]. Granted, it is assumed that an organization can afford both the technology and has the resources to implement such a robust defense architecture proposed by Fitch and Muckin.

While the idea of fortification is not always explicitly categorized in every document, modern defense tactics such as continuous patching, privileged access management, active monitoring, and deploying firewalls —all addressed in the literature—serve the same purpose of building stronger, more resilient defenses that can withstand both known and evolving threats [27, 26, 28]. One example of this is the Cyber Security Technical Assessment Methodology (TAM) developed by the Electric Power Research Institute (EPRI). The TAM is designed to enable facilities to conduct a thorough, methodical attack surface assessment and then select different mitigation strategies to minimize exploit impacts thus fortifying an organization's overall cybersecurity posture [29].

2.4.2. Chokepoints

Chokepoints, or strategically placed control points within a network, are essential for slowing down or stopping attackers. These control points restrict the movement of malicious actors and prevent lateral spread across systems. By segmenting networks and monitoring traffic through critical chokepoints, organizations can contain threats within specific boundaries, preventing them from affecting broader systems. These measures help isolate sensitive networks and services, ensuring that even if one segment is compromised, the damage is contained. For example, isolating critical infrastructure networks from less sensitive environments prevents attackers from using a compromised system as a launch point to access more critical assets.

Chokepoints not only limit the spread of attacks but also integrate intelligence-driven defense capabilities. By collecting and analyzing threat intelligence from various sources, organizations can build adaptive chokepoints that evolve in response to attacker behaviors. This method involves analyzing historical data, identifying attack patterns, and adjusting chokepoint defenses accordingly [27]. In this way, chokepoints serve as active defense points that react to new and changing threats.

Though the term "chokepoint" may not always be used directly in the literature, the concept is effectively addressed through discussions on network segmentation, application-aware defenses, and intelligent traffic monitoring. These measures serve to strategically control the flow of information, slowing down or halting the adversary's movements within networks, and create a location in which network monitoring can be deployed to record traffic and perhaps install Intrusion Detection Systems (IDS) [27, 30, 31]. One current shortcoming of chokepoints lies in increased use of cloud service providers. In 2021, researchers determined that cloud service providers or third-party firewalls available in commercial clouds could provide all functions of traditional network monitoring making using chokepoints in these environments difficult [30].

Another interesting perspective on the use of chokepoints is that not only are they a defense tactic, but they may also serve as an attack path that adversaries can use to broaden the impact of their attack. However, cybersecurity professionals can also use these same chokepoints as a method to reduce their organization's attack surface [32, 33].

2.4.3. Access Control

Access control mechanisms are designed to ensure that only authorized individuals can interact with specific resources within a system. These mechanisms are crucial for preventing unauthorized access, particularly to sensitive information and critical infrastructure [34, 35].

The NSA's Mitigation Strategies advocate for the use of privileged access management (PAM) systems and tiered administrative access. These systems automate credential management and limit the number of individuals with high-level access, thus reducing the risk of privilege escalation attacks [26]. PAM solutions are essential in environments where attackers often target administrator credentials to gain high-level access and move laterally through networks. By limiting access to critical systems and enforcing strong authentication protocols, organizations can significantly reduce the risk of a breach.

Moreover, Fitch and Muckin stress the importance of integrating intelligence-driven defense with access control systems. In these systems, access controls are continuously updated based on evolving threat intelligence. For instance, the design of a system may incorporate advanced multi-factor authentication (MFA) mechanisms, ensuring that only authorized personnel can access critical systems, through specific network paths to detect and alert on abnormal user behavior [27].

While access control is often discussed in terms of role-based access or privileged access management, the broader concept of intelligent, adaptive access controls —enabled by continuous threat monitoring and intelligence sharing—is an essential part of these defense strategies [27, 36, 37].

2.4.4. Deception

Deception technologies create false targets or misleading information to confuse or misdirect the adversary, thereby protecting real assets, enabling intelligence-gathering about the adversary, and buying time for defenders to respond. These tactics exploit the asymmetry of information in cybersecurity, where defenders often know less about the attacker's plans than the attackers know about the system's vulnerabilities.

The use of deception is gaining prominence as part of modern defense strategies. Fitch and Muckin's report describes incorporating deception into cybersecurity designs by leveraging threat intelligence to anticipate and deceive adversaries [27]. For example, deploying honeypots or honeynets can mislead attackers into engaging with fake systems, allowing defenders to monitor their tactics and respond without exposing real, critical assets [27, 38].

"A Game-theoretic Taxonomy and Survey of Defensive Deception" further highlights how deception can be implemented using game theory approaches. By analyzing attacker behavior and crafting misleading strategies, organizations can deceive attackers into taking actions that expose their methods or lead them into traps. Techniques such as moving target defense, perturbation, and obfuscation are examples of how deception can be structured to disrupt attackers' plans and mislead them about the network's structure and vulnerabilities [39].

According to cybersecurity company Fortinet, deception is beneficial for two key reasons. First, the proper application of deception technology allows defenders to record adversary activities and creates an opportunity to gather valuable intelligence. Second, deception technologies enable defenders to see which of their assets adversaries deem valuable [38, 28].

Deception, when combined with other defensive strategies, creates a comprehensive strategy for protecting critical systems. It can slow down adversaries, reduce the likelihood of a successful

breach, and buy valuable time for defenders to act. However, it is also important to understand that any deceptive techniques that are applied must be carefully maintained to remain effective as adversaries must engage with them to be operational [40].

2.4.5. Relationships Between Defensive Strategies

The following relationships were defined to establish the fundamental relationships between the defensive strategies:

1. Requires: The implementation of one strategy necessitates the implementation of another for effectiveness.
2. Enhances: The implementation of one strategy improves the effectiveness of another.
3. Weakens: The implementation of one strategy undermines or negates the effectiveness of another.

The relationships between defensive strategies are shown in . The relationships shown in Figure 8 are built upon specific proper implementation assumptions that are discussed in greater detail below.

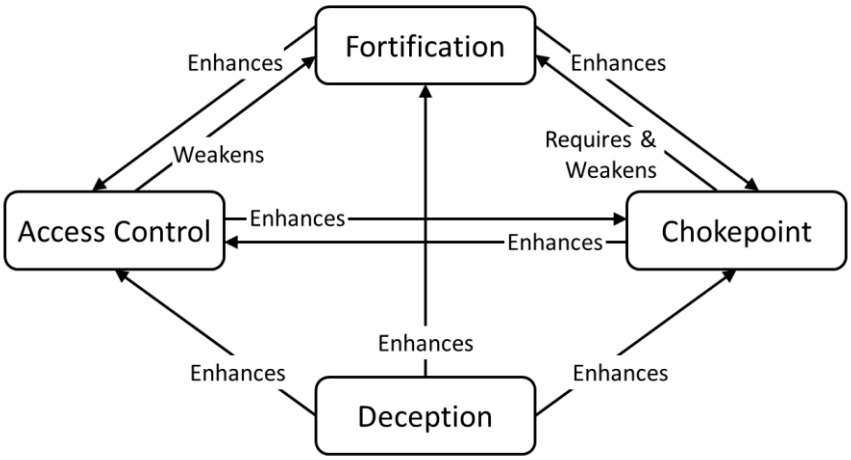

Figure 8. Defensive Strategies and Their Relationships [24]

Chokepoints require and weaken fortification. Chokepoints require fortification because the strategic narrow route provided by a chokepoint cannot exist without a restriction of movement in the area adjacent to the chokepoint. Consider an asset surrounded by a wall with one small gap serving as a chokepoint to funnel all free motion through a single known pathway. The gap cannot exist without the wall. Chokepoints weaken fortification because they present an opportunity for the adversary to bypass the established barrier.

Fortification enhances chokepoints by increasing the difficulty of the adversary to circumvent the chokepoint. Consider two applications of chokepoints and fortification in the physical domain: (1) a chain-link fence with a gate and (2) a concrete wall with an identical gate. An adversary would be able to circumvent the gate more easily in the first scenario than the second, therefore the increased fortification provided by the concrete wall enhances the chokepoint value provided by the gate.

Access control weakens fortification. The rationale for this relationship is identical to that for the weakening relationship between chokepoints and fortification. Access control presents an opportunity for the adversary to bypass the established barrier.

Fortification enhances access control. The rationale for this relationship is identical to that for the enhancing relationship between fortification and chokepoints. Increases in fortification adjacent to the access control point increases the difficult of the adversary to bypass access control.

Access control enhances a chokepoint. One purpose of a chokepoint is to slow down the spread of the adversary through a network. Access control supports this purpose by providing a means to verify that the individual passing through a chokepoint is authorized to do so. If an access control measure is implemented at a chokepoint, an adversary without authorized credentials or the means to bypass the access control measure would be stopped, thereby achieving the purpose of the chokepoint.

Chokepoints enhance access control. An effective chokepoint limits the adversary's ability to bypass the access control mechanism. Consider two scenarios: (1) a guard checking badges at a 2 ft. gap in a fence and (2) a guard checking badges at a 20 ft. gap in a fence. An adversary would be able to circumvent the gate more easily in the first scenario than in the second, therefore the increased chokepoint efficacy provided by the smaller gap enhances the access control provided by the guard. Note that this scenario also demonstrates the enhancing relationship between fortification and access control. A chokepoint can also enhance access control by establishing a location where an access control mechanism is implemented. A chokepoint is the means to define the path/location where an individual must verify identity.

Deception enhances fortification, access control, and chokepoints. These enhancing relationships exist because deception provides intelligence for the system defender to improve the implementation of the defensive strategies. If adversary activity is identified in the deception environment, the defender may be able to identify how the adversary defeated/circumvented the fortification, chokepoint, and/or access control strategies implemented in the deception environment, and address those vulnerabilities in the real system. The defender may also identify what targets are valued by the adversary, and enhance the defensive strategies employed around the legitimate targets. This strategy becomes more effective as the deception environment approaches the adversary's expectations of the true operational environment and as the deception environment approaches the legitimate environment. If the deception environment is too similar to the legitimate environment, the adversary may be able to gather offensive intelligence to be used in future attacks.

This page left blank

3. SODIUM FAST REACTORS

This section contains descriptions of the systems generally found in both constructed and conceptual SFRs. A list of constructed SFRs is provided in Table II. The designs of these reactors and publicly available conceptual designs were used to inform the SFR description in this section. Seven of the constructed reactors are currently operating.

Table II. Constructed SFRs [41]

Facility	Country	Purpose	Commissioned	Shutdown
Experimental Breeder Reactor – I (EBR-I) [42]	US	Demonstrate power from fission	1951	1963
Dounreay Fast Reactor (DFR) [43]	UK	Materials testing & breeding	1959	1977
Fermi 1 [44]	US	Prototype power breeder	1963	1972
Experimental Breeder Reactor – II (EBR-II) [45]	US	Prototype integral breeder	1964	1994
Rapsodie [46]	France	Experimental fast flux source	1967	1983
Southwest Experimental Fast Oxide Reactor (SEFOR) [47]	US	Safety & transient testing	1969	1972
Broya Opytnaya Reaktor – 60 (BOR-60) (“Boiling Experimental Reactor”) [48]	USSR/ Russia	Materials & fuel irradiation	1969	--
Phenix [49]	France	Prototype power breeder	1973	2010
Bistrye Neitrony – 350 (BN-350) (“Fast Neutron”) [50]	USSR/ Kazakhstan	Power and desalination	1973	1999
Prototype Fast Reactor (PFR) [51]	UK	Prototype power breeder	1974	1994
Kompakte Natriumgekuehlte Kernreaktoranlage - II (KNK-II) (Compact Sodium-Cooled Nuclear Reactor) [52]	Germany	Experimental fast reactor	1977	1991
Joyo [53]	Japan	Materials & fuel irradiation	1977	--
Bistrye Neitrony – 600 (BN-600) (“Fast Neutron”) [54]	USSR/ Russia	Commercial power generation	1980	--
Fast Flux Test Facility (FFTF) [55]	US	Fuels & materials testing	1982	1992
Fast Breeder Test Reactor (FBTR) [56]	India	Test fast breeder fuel	1985	--
Superphenix [57]	France	Large prototype breeder	1986	1997

Facility	Country	Purpose	Commissioned	Shutdown
Schneller Natriumgekühlter Reaktor - 300 (SNR-300) ("Fast Sodium-Cooled Reactor") [58]	Germany	Prototype power breeder	--	--
Monju [59]	Japan	Prototype power breeder	1994	2016
China Experimental Fast Reactor (CEFR) [60]	China	Experimental fast reactor	2010	--
Bistrye Neitrony – 800 (BN-800) ("Fast Neutron") [61]	Russia	Power and fuel burning	2016	--
Prototype Fast Breeder Reactor (PFBR) [62]	India	Prototype power breeder	--	--

At the time of publication of this report, there are three commercial SFR designs in progress for deployment in the U.S.:

1. ARC-100 (ARC Clean Technology)[2] [63]
2. Aurora Powerhouse (Oklo)[3] [64, 65]
3. Natrium (TerraPower)[2] [66, 67]

The SFR DCSA design presented in Section 4 is based upon assumptions regarding the individual systems, their functions, and their interdependencies. These assumptions are itemized throughout this section.

A set of fundamental sensors and actuators are specified in Appendix A for each system to accomplish their functions. In many cases, there is a diverse set of devices that could be implemented to achieve the required function. For generalizability of these results and to avoid prescriptive engineering implementations, the actuators and sensors are described in terms of their subfunctions to be performed, rather than describing specific technologies to be implemented.

3.1. Reactor System

This section describes the nuclear fuel, the fuel configuration, and the reactor operating modes.

3.1.1. Nuclear Fuel

Historically, SFRs have used either metallic or oxide fuels. Many SFRs deployed outside the U.S. have used oxide fuel [46, 68, 69], while the SFRs deployed in the U.S. have used metallic fuel [42, 45]. ARC-100, Aurora, and Natrium all propose to use metallic fuel, specifically uranium-zirconium (U-Zr) alloys [63, 65, 66]. Metallic fuels offer several benefits including high thermal conductivity, which aids in effective heat transfer and keeps the centerline temperature of the fuel lower, thereby reducing thermal stresses and improving useful operational life [70]. Based on the historical use of

[2] The Natrium and ARC-100 reactors leverage the GE Hitachi Power Reactor Innovative Small Module (PRISM) concept [108]

[3] The Aurora Powerhouse reactor originally used heat pipes as the core cooling mechanism, however Oklo has since pivoted to liquid sodium coolant. Public documentation for the sodium-cooled design is limited in comparison to the heat pipe design.

metallic fuels in SFR deployments in the U.S. and public documentation of SFRs in development, our plant design assumption is:

A.1. The nuclear fuel is a metallic U-Zr alloy

Assumption A.1 is important for the design of a DCSA within the context of the TCA because the use of a metallic fuel may act as a physical robustness factor that eliminates or mitigates the effects of a cyber-attack. Metallic fuels offer several benefits including high thermal conductivity, which aids in effective heat transfer and keeps the centerline temperature of the fuel lower, thereby reducing thermal stresses and improving useful operational life [70]. The effective heat transfer of metallic fuels may mitigate the effects of cyber-attacks that impair the heat rejection pathway from the nuclear fuel to the sodium coolant and ultimately to the power conversion cycle.

3.1.2. Nuclear Fuel Configuration

The configuration and material properties of SFR fuel assemblies are built to optimize neutron economy. Operating in a fast neutron spectrum, these reactors minimize neutron moderation, allowing for efficient fission and fuel utilization [70, 71]. The fast spectrum also enables the burning of long-lived actinides, contributing to advanced fuel cycles focused on minimizing radioactive waste.

The fuel elements (pins) typically consist of fuel pullets, upper and lower axial blanket fuels, and a fission gas plenum inside a stainless steel cladding [41, 72]. The pins are then bundled in a fuel assembly with spacers to ensure sodium coolant flow between the pins. An example of a typical fuel assembly is shown in Figure 9.

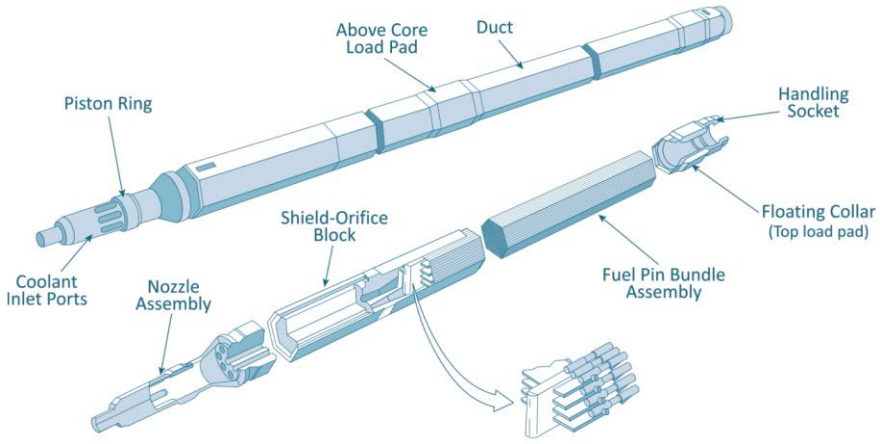

Figure 9. The ARC-100 Fuel Assembly [63]

The original proposed fuel assembly for the Aurora design was different from traditional fuel assemblies because of the integrated heat pipes. The original Aurora design integrated the components of the fuel assembly with a heat pipe to form a "reactor cell". With the Aurora design pivoting to liquid sodium coolant, it is assumed that their fuel assemblies will be similar to traditional designs.

The fuel assemblies are typically arranged in a compact hexagonal lattice, achieving power densities of 300–500 kW/L [73]. There are three common configurations of the fuel pins within the hexagonal lattice: homogeneous, axially heterogeneous, and radially heterogeneous [73]. The ARC-

100 is radially heterogeneous (Figure 10) [63]. To our knowledge, the Aurora and Natrium core configurations are not publicly available (redacted in [65] and [74], respectively).

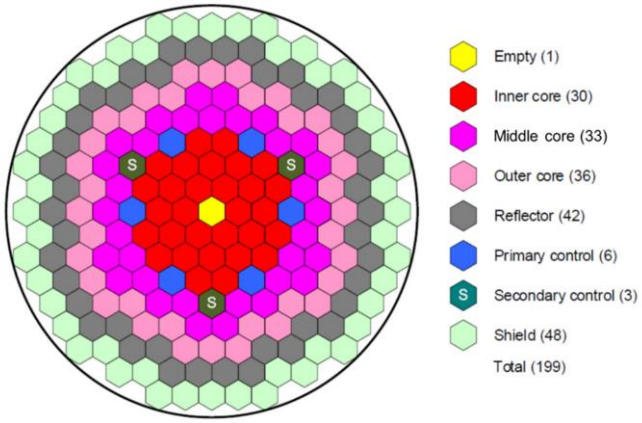

Figure 10. ARC-100 Core Cross-Section (Radially Heterogenous) [63]

Based on current industry trends, our plant design assumptions are:

A.2. The SFR fuel elements, fuel assemblies, and core design provide multiple robust layers of defense to protect against release of radionuclides for design-basis accidents [41].

A.3. The SFR fuel elements, fuel assemblies, and core design provide multiple robust layers of defense that increase the grace period for operator action in design-basis accident scenarios [75].

Assumptions A.2 is important for the design of a DCSA within the context of the TCA because the use of a multiple robust layers of defense may act as a physical robustness factor that eliminates or mitigates the effects of a cyber-attack. These considerations may include lower steady-state and transient fuel temperatures, large temperature margin to fuel melting, and significant cooling capability for damaged fuel pins in some beyond design-basis accident scenarios [75].

While assumption A.3 is not directly applicable to DCSA design as part of an isolated Tier 2 analysis, it is important when considering the complete TCA process. Assumption A.3 is most directly applicable to Denial of Task Analysis (Tier 3) which is focused on detection and interruption of cyber-attacks before consequences of concern can occur. For implementation of this assumption in Tier 3 analysis, more specific data would need to be presented to determine timelines for operator action. This consideration affects DCSA design because if a plant designer intends to credit this assumption in Tier 3, then the architecture must ensure that operators have access to sufficient data to detect the cyber-enabled accident scenario is occurring and access to the control surface necessary to interrupt the progression of the scenario.

3.1.3. Reactor Operating Modes

SFRs operate under three primary modes: start-up, steady-state, and shutdown, each requiring coordination between the core, coolant systems, and other plant systems:

1. Start-Up: The purpose of this operating mode is to achieve criticality in the core. In this mode of operation, the core slowly brought up to criticality and allowed to slowly come up to temperature using the startup/shutdown system. During startup, the reactor is gradually

heated to prevent thermal stress on its components. This is achieved through controlled sodium flow and precise adjustments of reactivity using control rods [76].

2. Steady-State: In this mode of operation, power is adjusted by changing the coolant mass flow rate through the core via the coolant pressure or the sodium pump speed control. In steady-state operation, the coolant is maintained at near-atmospheric pressure and a temperature of 510–550°C, below sodium's boiling point, ensuring thermal stability and effective heat removal [76]. The reactor outlet temperature is manipulated using the control rods.
3. Shutdown: The purpose of this operating mode is to shutdown the reactor and remove decay heat. In this mode of operation, control rods are inserted and decay heat is removed via either the start-up/shutdown cooling system or the residual heat removal system [75].

These modes are documented in the following assumption:

A.4. The reactor has three operating modes: start-up, steady-state, and shutdown

Assumption A.4 is important for DCSA design because it informs the interdependencies between plant systems required to achieve the functions performed during each operating mode. The close integration of these systems is important for plant performance. The coolant loop's ability to transfer heat directly affects the reactor's ability to maintain safe operating temperatures and provide the necessary cooling for decay heat removal [76]. Furthermore, the interaction between the reactor core and sodium coolant supports inherent safety features, such as reducing reactivity during transients through sodium's thermal expansion [70].These interdependencies affect the data flow requirements between DCSA zones.

3.2. Fuel Handling and Storage System (FHSS)

The purpose of the Fuel Handling and Storage System (FHSS) is to fuel the reactor and store spent fuel. It is assumed that the FHSS consists of two subsystems:

A.5. The Fuel Handling and Storage System (FHSS) consists of two subsystems: the Fuel Handling System (FHS) and the Spent Fuel Storage System (SFSS)

Assumption A.5 is important for DCSA design because it informs the interdependencies between plant systems required to achieve their objective to control fresh fuel injections, spent fuel removal and fuel storage. The following sections describe the FHS and SFSS in greater detail.

3.2.1. Fuel Handling System (FHS)

The FHS functions are:

F.FHS.1. Load fuel into the reactor [77]

F.FHS.2. Move spent fuel from the reactor core to the short-term storage location [77, 63]

F.FHS.3. Move spent fuel from the short-term storage location to the long-term storage location [77, 63]

F.FHS.4. Maintain operation [77]

The fuel loading operation loads new fuel assemblies into the top of the reactor. The fuel unloading operation extracts fuel assemblies and moves them to a short-term in-vessel fuel storage location to allow for thermal decay [77, 63]. After sufficient decay, the spent fuel is transferred to a the SFSS. The SFSS is discussed in greater detail in the following section.

The fundamental sensors and actuators necessary for FHS operation are summarized in Table XI and Table XII, respectively.

3.2.2. Spent Fuel Storage System (SFSS)

The primary function of the Spent Fuel Storage System (SFSS) is:

F.SFSS.1. Store spent fuel [71]

The spent fuel is deposited into casks, drums, or tanks by the FHS. The storage geometry ensures that the spent fuel remains subcritical and the decay heat can be removed by air or water cooling [71]. The SFSS assumptions are:

A.6. The Spent Fuel Storage System (SFSS) is passively air-cooled via natural convection

A.7. The Spent Fuel Storage System (SFSS) operates independently of other plant systems

Assumption A.6 is important for DCSA design because it affects the control surface of the SFSS and is a non-cyber IPL that may mitigate or eliminate the consequences of a cyber-attack. Assumption A.7 is important for DCSA design because it affects the interdependencies between the SFSS and other plant systems.

The fundamental sensors and actuators necessary for SFSS operation are summarized in Table XIII and Table XIV, respectively [78].

3.3. Reactivity Control and Shutdown System (RCSS)

The purpose of the Reactivity Control and Shutdown System (RCSS) is to control the reactivity of the core by absorbing neutrons [75]. Based on documentation of the historical SFRs and public ARC-100, Aurora, and Natrium design reports [75, 63, 65, 67], it is assumed that the RCCS consists of two subsystems:

A.8. The Reactivity Control and Shutdown System (RCSS) consists of two subsystems: the Reactivity Control System (RCS) and Reserve Shutdown System (RSS).

Assumption A.8 is important for DCSA design because it informs the interdependencies between plant systems required to achieve their functions. The following sections describe the RCS and RSS in greater detail.

3.3.1. Reactivity Control System (RCS)

The primary functions of the Reactivity Control System (RCS) are:

F.RCS.1. Control reactivity by manipulating control rod position [63, 66, 79]

F.RCS.2. Achieve hot shutdown state by inserting control rods [63, 75, 67]

F.RCS.3. Achieve cold shutdown state by inserting control rods in conjunction with the RSS [63, 75, 67]

F.RCS.4. Insert control rods during a reactor trip [63, 75, 67]

The RCS manipulates the reactivity of the core by inserting or withdrawing control rods to absorb neutrons [79, 41]**.** The RCSs of historical SFRs have typically implemented control rod systems [41]. The ARC-100 and Natrium designs use a control rod system while the Aurora design uses a control drum system [63, 65, 67]. It is unclear whether the control drum system will be switched to a control rod system given Aurora's change from a heat-pipe design to a sodium-cooled design. Control drums are rotated to position reflectors and absorbs towards the core to control reactivity (Figure 11). Control drum systems are less common than control rod systems, but control drums are being included in other AR designs (e.g., the Westinghouse eVinci microreactor [80] and U.S. DOE MARVEL microreactor [81]). The functions of a control drum RCS are identical to those

listed above if the word "rod" is replaced with "drum" and "insert" is replaced with "rotate". Given the trend towards control rod RCSs, we will use control rod terminology throughout this section.

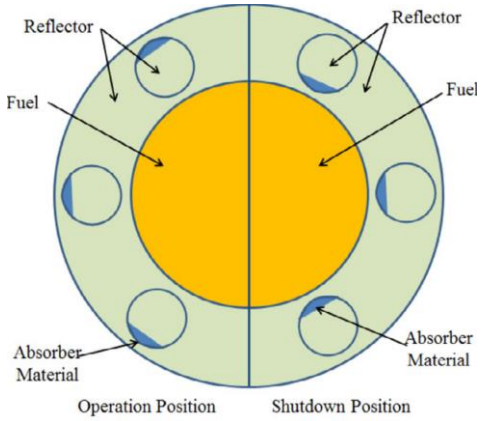

Figure 11. Control Drum RCS [82]

The ARC-100 RCS design has six control rods and the number of control rods in the Natrium design was not publicly available [63, 66]. The configuration of the ARC-100 control rods is shown in Figure 9. The six RCS control rods are labelled as "Primary Control". The three "Secondary Control" rods will be discussed in the following section.

The control rods typically remain partially inserted and are manipulated incrementally to meet operational needs. During a reactor trip, the control rods are quickly fully inserted to achieve safe shutdown [75].

All previous SFRs have had control rods that insert from the top of the reactor [41], and ARC-100 and Natrium documentation indicate that the control rods will insert from the top of the reactor [63, 66], therefore it is assumed that:

A.9. The Reactivity Control System (RCS) control rods insert from the top of the reactor.

A.10. If the Reactivity Control System (RCS) control rods are released, gravitational forces are sufficient to fully insert the control rods into the reactor.

Assumptions A.9 and A.10 are important for DCSA design because they inform the actuation requirements of the RCS control rods during a reactor trip.

All three focal SFRs in this work use their primary control rods/drums for routine reactivity control and hot shutdown (i.e., subcritical reactor with core and coolant at high temperatures) [63, 65, 67], therefore it is assumed that:

A.11. The insertion of the Reactivity Control System (RCS) control rods provides sufficient neutron absorption for hot shutdown.

The ARC-100 documentation specifies that the RCS control rods have sufficient reactivity worth to bring the reactor from any operating condition to a cold shutdown state [63]. The public Aurora and Natrium do not state whether the RCS control drums/rods have sufficient worth for that operation. It is assumed that:

A.12. The insertion of both the Reactivity Control System (RCS) control rods and/or the Reserve Shutdown System (RSS) control rods are necessary to provide sufficient neutron absorption for cold shutdown.

Assumptions A.11 and A.12 are important for DCSA design because they inform the interdependencies between plant systems required to achieve their functions.

The fundamental sensors and actuators necessary for RCS operation are summarized in Table XV and Table XVI, respectively [63, 66, 79].

3.3.2. Reserve Shutdown System (RSS)

The primary functions of the Reserve Shutdown System (RSS) are:

F.RSS.1. Achieve cold shutdown state by inserting shutdown rods in conjunction with the RCS [75]

F.RSS.2. Drop shutdown rods during a reactor trip [75]

The RSS manipulates the reactivity of the core by inserting shutdown rods to absorb neutrons [75]. The ARC-100 and Aurora RSS designs have three shutdown rods and the public Natrium documentation does not specify the number of shutdown rods [63, 65]. The ARC-100 shutdown rods are labelled as "Secondary Control" in Figure 9. The Aurora documentation further states that the three shutdown rods are included for redundancy and only one of the three is required to shut down the reactor at any temperature condition [65]. Unlike the RCS control rods, the RSS shutdown rods are fully withdrawn when not in use, and are rapidly inserted when needed [75].

Following the same logic as applied to Assumptions A.9 and A.10, it is assumed that:

A.13. The Reserve Shutdown System (RSS) shutdown rods insert from the top of the reactor.

A.14. If the Reserve Shutdown System (RSS) shutdown rods are released, gravitational forces are sufficient to fully insert the control rods into the reactor.

The fundamental sensors and actuators necessary for RSS operation are summarized in Table XVII and Table XVIII, respectively [63, 66, 79].

3.4. Heat Transfer System (HTS)

The purpose of the Heat Transfer System (HTS) is to transfer thermal energy from the reactor to the balance of plant system [73, 75]. Based on documentation of the historical SFRs and public ARC-100, Aurora, and Natrium design reports [75, 63, 65, 67], it is assumed that the HTS consists of two subsystems:

A.15. The Heat Transfer System (HTS) consists of two subsystems: the Primary Heat Transfer System (PHTS) and Intermediate Heat Transfer System (IHTS).

Assumption A.8 is important for DCSA design because it informs the interdependencies between plant systems required to achieve their functions. The following sections describe the PHTS and IHTS in greater detail.

3.4.1. Primary Heat Transfer System (PHTS)

The primary functions of the Primary Heat Transfer System (PHTS) are:

F.PHTS.1. Provide cooling to the reactor core [73, 75]

F.PHTS.2. Transport thermal energy to the Intermediate Heat Transfer System (IHTS) [83]

Liquid sodium coolant offers benefits including:

1. High thermal conductivity [84, 85]
2. High heat transfer at moderate velocities [84, 85]

3. Low pumping power [84, 85]
4. High boiling temperature [84, 85]
5. Low melting temperature [84, 85]
6. Preclusion of chemical attack on steel structures [84, 85]
7. Low neutron absorption cross-section [86]

The use of liquid sodium does require robust containment and monitoring measures due to sodium's reactivity with air and water [87, 88].

There are two common configurations of the PHTS in SFR designs: pool-type and loop-type. Both designs are driven by the primary sodium pump (PMP) that pumps coolant through the reactor core and through a heat exchanger where thermal energy is transferred to the IHTS. Pool-type designs include a heat exchanger and primary sodium pump within the reactor vessel, while loop-type designs separate the heat exchanger and pump from the reactor vessel. The pool-type configuration is shown in Figure 12 and the loop-type configuration is shown in Figure 13. While loop-type designs offer a more compact reactor vessel and easier maintenance, pool-type designs offer large thermal inertia and contain the primary sodium in a single vessel, thereby reducing risk of loss-of-coolant accidents (LOCAs) [73, 88]. Both design types operate near atmospheric pressure and are technologically feasible [89].

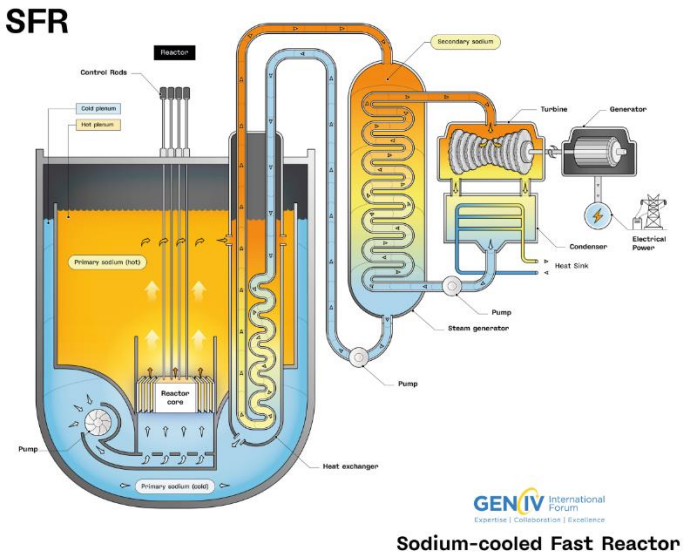

Figure 12. SFR Pool-Type Design [90]

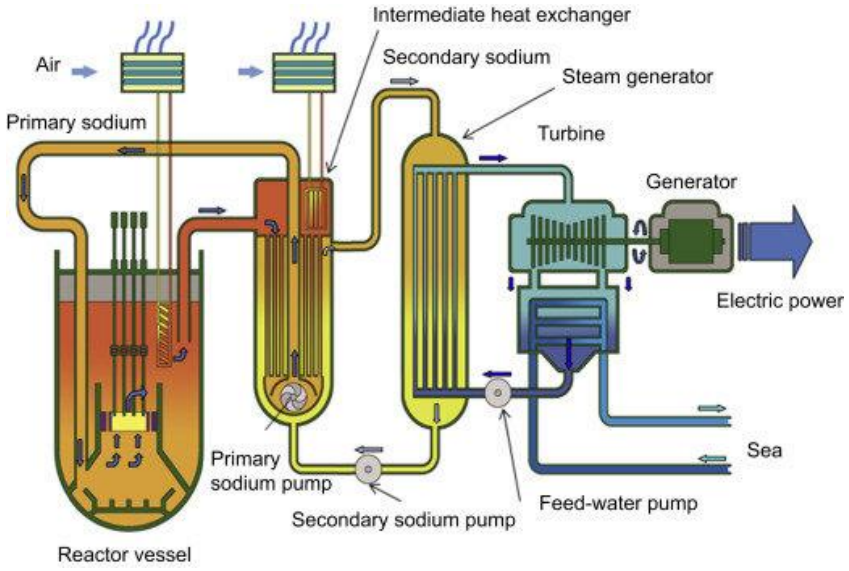

Figure 13. SFR Loop-Type Design [73]

A summary of the historical designs is provided in Table III (quoted directly from [73]). Historically, the U.S. has implemented loop-type SFRs, with EBR-II being the only pool-type design. The ARC-100 and Natrium designs use a pool-type configuration [63, 66]. The Aurora documentation does not directly state whether a pool-type or loop-type configuration will be used, but given Oklo's research at the Thermal Hydraulic Experimental Test Article (THETA) facility it is reasonable to assume that pool-type configuration is likely for the Aurora reactor [91, 92]. THETA is a pool-type sodium research facility at Argonne National Laboratory [91].

Table III. Historical Pool-Type and Loop-Type SFRs [73]

Country	Pool	Loop
U.S.	EBR-II	EBR-I, Fermi, SEFOR, FFTF
U.K.	PFR	DFR
France	Phenix, Superphenix	Rapsodie
Germany		KNK-II, SNR-300
Russia	BN-600, BN-800	BOR-60, BN-350
India	PFBR	FBTR
China	CEFR	
Japan		Joyo, Monju

Based on the U.S. industry trends, we assume:

A.16. The Primary Heat Transfer System (PHTS) uses a pool-type design

Assumption A.16 is important for DCSA design because it informs interdependencies required for the PHTS to perform its functions.

The fundamental sensors and actuators necessary for PHTS operation are summarized in Table XIX and Table XX, respectively [73, 67]

3.4.2. Intermediate Heat Transfer System (IHTS)

The primary functions of the Intermediate Heat Transfer System (IHTS) are:

F.IHTS.1. Transport thermal energy to the Power Conversion System (PCS) [83]

F.IHTS.2. Isolate radioactive sodium in the Primary Heat Transfer System (PHTS) from the non-radioactive Power Conversion Systems (PCS) [83]

Like the PHTS, the IHTS uses liquid sodium as its working fluid. The intermediate sodium pump (ISP) pumps coolant through a heat exchanger where thermal energy is received from the PHTS via a heat exchanger, and then passes that thermal energy to the PCS via another heat exchanger. The IHTS provides a layer of DiD to prevent the release of radionuclides into the PCS in the event of a leak of the primary coolant. There is little variability in IHTS design in comparison to differences between loop and pool type PHTSs. The ARC-100 and Natrium documentation specify that an IHTS is to be implemented [63, 66]. Given the prevalence of IHTSs in SFR designs, it is possible that an IHTS could be implemented for the Aurora design, however this information is not available in documentation due to Aurora's history with heat pipe designs [65].

The fundamental sensors and actuators necessary for IHTS operation are summarized in Table XXI and Table XXII, respectively [73, 67].

3.5. Sodium Processing System (SPS)

The primary functions of the Sodium Processing System (SPS) are:

F.SPS.1. Remove chemical impurities from the sodium [93, 94, 95]

F.SPS.2. Remove radionuclide impurities from the sodium [93, 94, 95]

The purpose of SPS is to provide clean sodium to be circulated by the PHTS and IHTS [93]. Impure sodium coolant poses several risks including:

- Increased corrosion due to oxygen, potentially causing plugging [93].
- Increased dose rates due to radioactive corrosion products and fission products [93].
- Reduced detection capability of sodium-water interactions due to hydrogen [93].

The three primary means for sodium purification are cold traps, hot traps, and cesium traps. Cold traps primarily remove oxygen and operate by cooling the sodium, causing impurities to crystallize on the trap. Hot traps operate at or above operating temperatures, and can be used to achieve very low levels of oxygen. Hot traps are not strictly necessary for SFRs. Cesium traps use methods such as graphite filters to capture cesium that is not well-captured by cold traps [93]

There is very little documentation available describing the SPS plans for the ARC-100, Aurora, or Natrium designs. A schematic of the EBR-II SPS is shown in Figure 14. The EBR-II SPS originally used a cold trap system, and was augmented to include cesium traps.

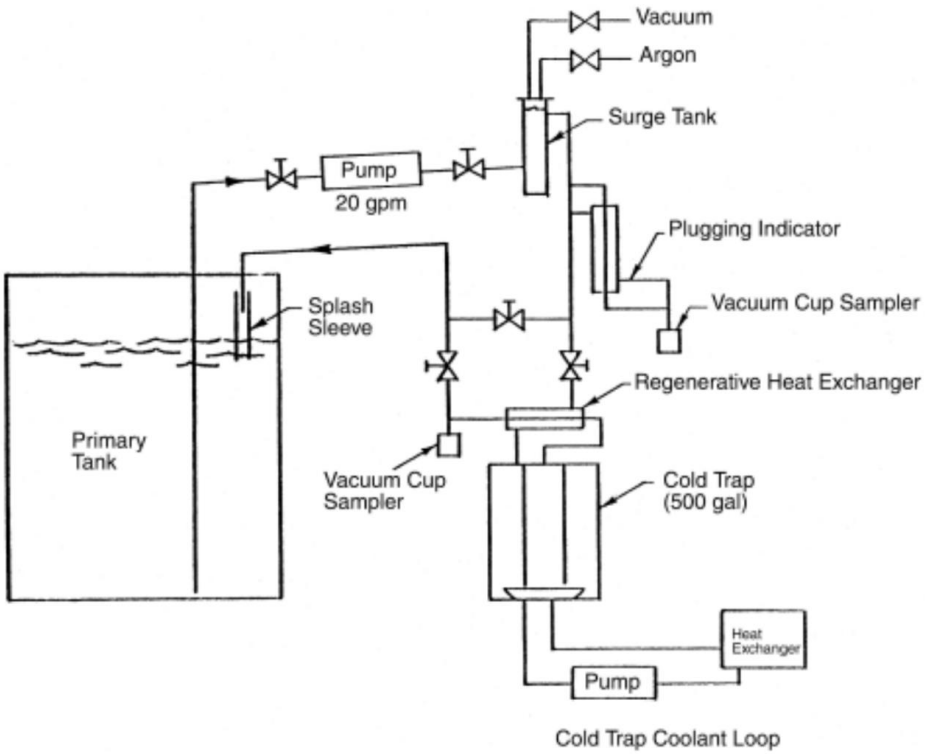

Figure 14. EBR-II SPS Schematic (before installation of cesium trap) [93]

The fundamental sensors and actuators necessary for SPS operation are summarized in Table XXIII and Table XXIV, respectively [96].

3.6. Sodium Leak Management System (SLM)

The primary functions of the Sodium Leak Management System (SLM) are:

F.SLM.1. Detect sodium leaks from the reactor vessel, PHTS, and IHTS [75, 93, 97]

F.SLM.2. Contain sodium leaks from the reactor vessel, PHTS, and IHTS [75, 93, 97]

F.SLM.3. Mitigate sodium leaks from the reactor vessel, PHTS, and IHTS [75, 93, 97]

Due to sodium's reactivity with air and water, it is important that any leaks in sodium throughout the plant are promptly detected, contained, and mitigated. Detection of leaks can include chemical, thermal, or optical methods. Bypass valves can be used to redirect sodium away from the leaking area to a secondary containment. Inert chemicals may be applied to leaks to minimize hazardous sodium reactions [75, 93, 97].

The fundamental sensors and actuators necessary for SLM operation are summarized in Table XXV and Table XXVI, respectively [75, 93, 97].

3.7. Sodium Fire Protection System (SFP)

The primary functions of the Sodium Fire Protection System (SFP) are:

F.FPS.1. Detect sodium fires from leaks from the reactor vessel, PHTS, and IHTS [75, 93, 98]

F.FPS.2. Extinguish sodium fires from leaks from the reactor vessel, PHTS, and IHTS [75, 93, 98]

Due to sodium's reactivity with air and water, it is important that any fires involving sodium are promptly detected and extinguished. The SFP continuously monitors for signs of sodium fires using measurements of smoke, flames, temperature increases, and changes in pressure due to fire. Dry powder extinguishing agents or inert gas are used to suppress sodium fires. The SFP works in conjunction with the SLM to ensure hazardous sodium fires do not occur or are properly extinguished [75, 93, 98].

The fundamental sensors and actuators necessary for SFP operation are summarized in Table XXVII and Table XXIV, respectively [75, 93, 98].

3.8. Cover Gas System (CGS)

The primary functions of the Cover Gas System (CGS) are:

F.CGS.1. Prevent sodium oxidation [75, 93]

F.CGS.2. Control pressure in reactor vessel [75, 93]

F.CGS.3. Support detection of sodium leaks [75, 93]

The cover gas system consists of the piping and quality systems necessary to maintain a layer of inert argon gas in the reactor vessel above the sodium pool. This layer prevents sodium oxidation by preventing the sodium from contacting air or moisture. The CGS also maintains a slight positive pressure over the sodium pool to prevent air ingress while allowing for thermal expansion of the sodium. Contaminants in the cover gas may be indicative of leaks in the PHTS. Historically, some SFRs have used active circulation of cover gas and others have used passive circulation. Gas may be purged for maintenance operations [75, 93].

The fundamental sensors and actuators necessary for CGS operation are summarized in Table XXV. SLM Sensors

Sensor ID	Sensor Purpose
SLM.S.1	Sodium leak detectors
SLM.S.2	Measures temperatures in areas where sodium may leak
SLM.S.3	Smoke detectors
SLM.S.4	Measures sodium pressure
SLM.S.5	Measures cover gas composition

Table XXVI. SLM Actuators

Actuator ID	Actuator Purpose
SLM.A.1	Sodium isolation valves in PHTS
SLM.A.2	Sodium isolation valves in IHTS
SLM.A.3	Sodium drain valves
SLM.A.4	Sodium cooling system actuators

Table XXVII. SFP Sensors

Sensor ID	Sensor Purpose
SFP.S.1	Flame detectors
SFP.S.2	Measures temperatures in areas where sodium may leak

Sensor ID	Sensor Purpose
SFP.S.3	Smoke detectors
SFP.S.4	Gas composition sensors
SFP.S.5	Measures pressure in areas where sodium may leak

Table XXVIII. SFP Actuators

Actuator ID	Actuator Purpose
SFP.A.1	Sodium isolation valves in PHTS
SFP.A.2	Sodium isolation valves in IHTS
SFP.A.3	Inert gas injection valves
SFP.A.4	Ventilation dampers
SFP.A.5	Interlock actuators

Table XXIX and Table XXX, respectively [75, 93].

3.9. Residual Heat Removal System (RHR)

The primary functions of the Residual Heat Removal System (RHR) are:

F.RCCS.1. Control reactor vessel temperature in normal operations [75, 85, 99]
F.RCCS.2. Control guard vessel temperature in normal operations [75, 85, 99]
F.RCCS.3. Control reactor vessel temperature in accident conditions [75, 85, 99]
F.RCCS.4. Control guard vessel temperature in accident conditions [75, 85, 99]
F.RCCS.5. Residual/decay heat removal in accident conditions [75, 85, 99]

There are many potential implementations of the RHR [75, 85, 99]. Figure 15 shows the most common implementations.

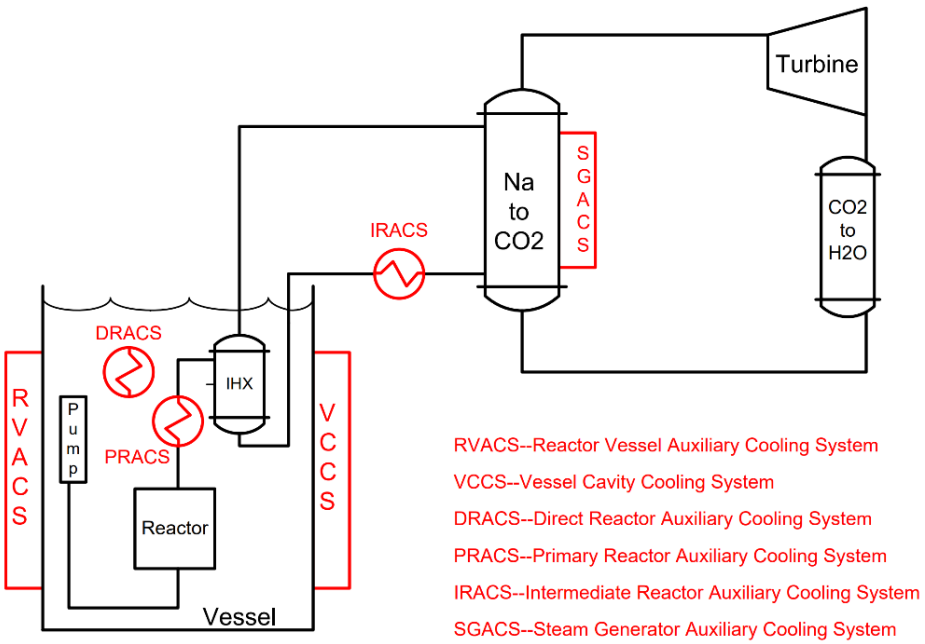

Figure 15. RHR Implementation Options [75, 85]

The ARC-100 design documentation discusses implementation of a Direct Reactor Auxiliary Cooling System (DRACS) and a Reactor Vessel Auxiliary Cooling System (RVACS) [63], and the Natrium design documentation discusses implementation of an RVACS and an Intermediate Reactor Auxiliary Cooling System (IRACS)[4] [66]. The Aurora documentation specifies that an RHR such as an RVACS is not necessary for their design because of the small amount of decay heat, however the source for this statement was for the heat pipe version of the Aurora reactor and the design may be different for the sodium-cooled version [65]. The DRACS, RVACS, and IRACS are discussed in the remainder of this section.

3.9.1. Direct Reactor Auxiliary Cooling System (DRACS)

The DRACS as implemented in the ARC-100 design will remove thermal energy from the reactor pool via the direct heat exchanger (DHX) and transfer the energy to the atmosphere via the natural draft heat exchanger (NDHX) [63]. A diagram of the DRACS is shown in Figure 16. The primary coolant is a sodium-potassium alloy that circulates passively via natural circulation. The secondary coolant is air and it is circulated actively via a fan in normal operations, but can also be circulated passively via a damper system as backup [63].

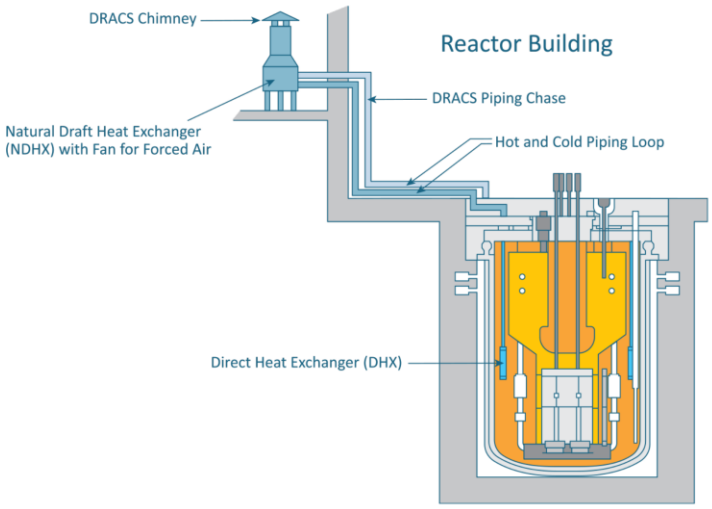

Figure 16. DRACS Schematic [63]

Based on the ARC-100 documentation we assume:

A.17. The Direct Reactor Auxiliary Cooling System (DRACS) is operable by both active and passive means.

Assumption A.19 is important for DCSA design because it affects the control surface of the DRACS and is a non-cyber IPL that may mitigate or eliminate the consequences of a cyber-attack.

[4] The Natrium documentation refers to the RVACS as the Reactor Air Cooling System (RAC) and the IRACS as the Intermediate Air Cooling System (IAC) [68].

The fundamental sensors and actuators necessary for DRACS operation are summarized in Table XXV. SLM Sensors

Sensor ID	Sensor Purpose
SLM.S.1	Sodium leak detectors
SLM.S.2	Measures temperatures in areas where sodium may leak
SLM.S.3	Smoke detectors
SLM.S.4	Measures sodium pressure
SLM.S.5	Measures cover gas composition

Table XXVI. SLM Actuators

Actuator ID	Actuator Purpose
SLM.A.1	Sodium isolation valves in PHTS
SLM.A.2	Sodium isolation valves in IHTS
SLM.A.3	Sodium drain valves
SLM.A.4	Sodium cooling system actuators

Table XXVII. SFP Sensors

Sensor ID	Sensor Purpose
SFP.S.1	Flame detectors
SFP.S.2	Measures temperatures in areas where sodium may leak
SFP.S.3	Smoke detectors
SFP.S.4	Gas composition sensors
SFP.S.5	Measures pressure in areas where sodium may leak

Table XXVIII. SFP Actuators

Actuator ID	Actuator Purpose
SFP.A.1	Sodium isolation valves in PHTS
SFP.A.2	Sodium isolation valves in IHTS
SFP.A.3	Inert gas injection valves
SFP.A.4	Ventilation dampers
SFP.A.5	Interlock actuators

Table XXIX. CGS Sensors

Sensor ID	Sensor Purpose
CGS.S.1	Measures gas pressure
CGS.S.2	Measures gas temperature
CGS.S.3	Measures gas oxygen content
CGS.S.4	Measures gas humidity

Sensor ID	Sensor Purpose
CGS.S.5	Measures gas isolation valve position
CGS.S.6	Measures gas purge valve position

Table XXX. CGS Actuators

Actuator ID	Actuator Purpose
CGS.A.1	Control gas supply pathway
CGS.A.2	Gas isolation valve
CGS.A.3	Gas purge valve
CGS.A.4	Gas pressure regulator

Table XXXI and Table XXXII, respectively [63, 100, 99].

3.9.2. Reactor Vessel Auxiliary Cooling System (RVACS)

The RVACS operates by natural circulation of air around the guard vessel and is always in operation. A diagram of the RVACS is shown in Figure 17. Radiative heat transfer is the dominant mechanism for heat transfer from the reactor vessel to the guard vessel, however there is also limited convective heat transfer. Natural convection is the dominant heat transfer mechanism between the guard vessel and the air duct wall. Natural circulation of hot rising air transfers the thermal energy to atmosphere as the ultimate heat sink [66].

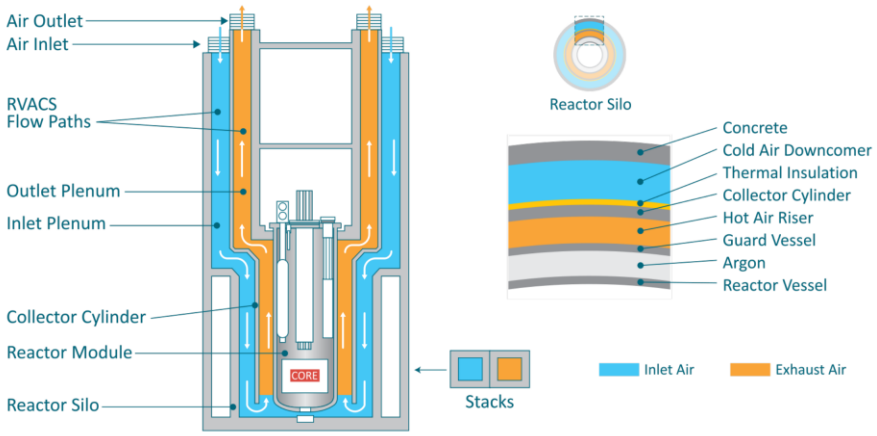

Figure 17. RVACS Schematic [63]

Based on the ARC-100 and Natrium documentation we assume:

A.18. The Reactor Vessel Auxiliary Cooling System (RVACS) operable by passive means.

Assumption A.19 is important for DCSA design because it affects the control surface of the RVACS and is a non-cyber IPL that may mitigate or eliminate the consequences of a cyber-attack.

The fundamental sensors necessary for RVACS operation are summarized in Table XXXIII [63, 66, 101, 99]. Although the RVACS is designed to utilize passive cooling, actuators may still be implemented for auxiliary functions and safety.

3.9.3. Intermediate Reactor Auxiliary Cooling System (IRACS)

An IRACS utilizes a heat exchanger integrated into the secondary sodium coolant loop to remove decay heat [99]. In the case of the Natrium design, heat is removed from the intermediate heat exchanger and a sodium-air heat exchanger transfers the heat to atmosphere [66]. The Natrium IRACS is used during normal shutdown cooling in outages and can be operated in both active and passive modes. In the active mode, the air in the sodium-air heat exchanger is blown by a fan, and in the passive mode, natural circulation flow is achievable by passive actuation of dampers (similar to the passive DRACS operation) [66].

Based on the Natrium documentation we assume:

A.19. The Intermediate Reactor Auxiliary Cooling System (IRACS) is operable by both active and passive means.

Assumption A.19 is important for DCSA design because it affects the control surface of the IRACS and is a non-cyber IPL that may mitigate or eliminate the consequences of a cyber-attack.

The fundamental sensors and actuators necessary for IRACS operation are summarized in Table XXXIV and Table XXXV, respectively [99, 66]

3.10. Power Conversion System (PCS)

The primary functions of the Power Conversion System (PCS) are:

F.PCS.1. Transfer heat from the secondary coolant loop to the tertiary loop [41]

F.PCS.2. Residual heat removal during off-normal operation [41]

F.PCS.3. Generate electricity [41]

To our knowledge, all constructed SFRs with a PCS have implemented a steam cycle. The ARC-100 and Natrium designs utilize a steam cycle, while the Aurora design utilizes a supercritical CO_2 (sCO_2) system [63, 66, 65]. All proposed implementations perform the functions enumerated above, however the Natrium design implements an additional energy storage system in conjunction with the PCS [66, 102]. Steam cycles and sCO_2 are discussed below for completeness; however, given their functional equivalence, the distinction is not of particular importance for DCSA design.

3.10.1. Steam Cycle Power Conversion System (SCPCS)

The ARC-100 and Natrium designs both utilize a Steam Cycle Power Conversion System (SCPCS) [63, 102]. Neither design publicly specifies the specific steam cycles to be used, however the Natrium design does state that superheated steam will be used with a reheater [66]. While the details of the steam cycle are important for power generation efficiency, they are not of particular importance for DCSA design besides understanding how the control surface maps to consequence analysis results of Tier 1 and understanding any broader information interdependencies between systems. Rankine cycles are common steam cycles and are also in consideration for other AR designs [103]. Therefore we assume:

A.20. If implemented, the Steam Cycle Power Conversion System (SCPCS) utilizes a Rankine cycle.

Assumption A.20 is important for DCSA design because it informs the control surface of the SCPCS and the interdependencies between plant systems.

An overview of the SCPCS is shown in Figure 18. Thermal energy is transferred from the sodium in the secondary loop to the feedwater in the tertiary loop via the steam generator. The high-quality

steam is then passed through the turbine-generator system to produce electricity. The turbine exhaust is then condensed and pumped back through the steam generator [6].

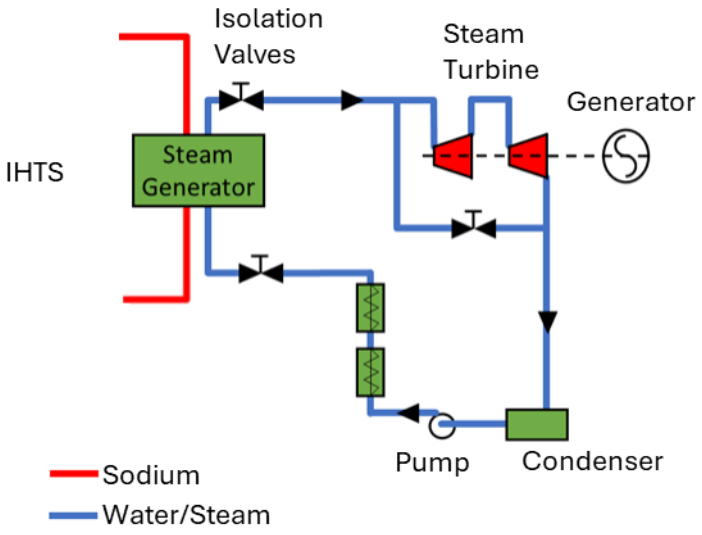

Figure 18. SCPCS Overview [104]

The fundamental sensors and actuators necessary for SCPCS operation are summarized in Table XXXVI and Table XXXVII, respectively [105, 106, 107, 108].

3.10.2. Supercritical Carbon Dioxide Power Conversion System (SCDPCS)

The Aurora design utilizes a Supercritical Carbon Dioxide Power Conversion System (SCDPCS) [65]. Some technical benefits of sCO_2 cycles over traditional steam cycles include:

- Higher thermal efficiencies [109, 110, 111]
- Compact configuration [109, 110, 111]
- Reduced capital costs [109, 110, 111]

Several Brayton cycle test loops have been operated using sCO_2 [112, 113]. We assume:

A.21. If implemented, the Supercritical Carbon Dioxide Power Conversion System (SCDPCS) utilizes a Brayton cycle.

Assumption A.21 is important for DCSA design because it informs the control surface of the SCDPCS and the interdependencies between plant systems.

An overview of the SCDPCS is shown in Figure 19. Thermal energy is transferred from the sodium in the secondary loop to the carbon dioxide in the tertiary loop via the heater. The carbon dioxide is then passed through the turbine-generator system to produce electricity. The turbine outlet then passes through a recuperator to improve cycle efficiency by minimizing waste heat. The carbon dioxide is then precooled, compressed, returned through the recuperator, and back through the heater system [112, 113].

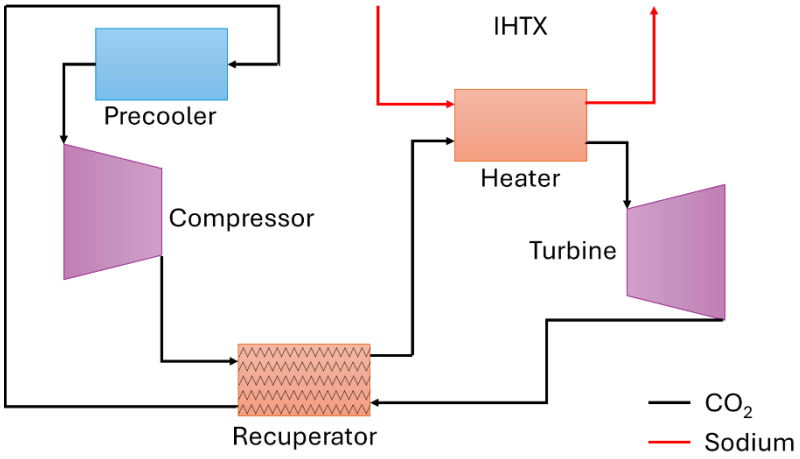

Figure 19. SCDPCS Overview [113]

The fundamental sensors and actuators necessary for SCDPCS operation are summarized in Table XXXVI and Table XXXVII, respectively [113, 112, 110].

3.10.3. Thermal Energy Storage System (TESS)

The proposed Natrium design includes a Thermal Energy Storage System (TESS) [66, 102]. Although the Natrium design is the only design of the three SFRs focused on in this report, the concept of a TESS or thermal battery system is used in other AR designs [114, 115, 116]. The primary function of the TESS is:

F.TESS.1. Store thermal energy generated by the nuclear island to be converted to electric power by the Power Conversion System (PCS) [66, 116]

Performance of this function is useful for two scenarios:

1. Enable continuous steady-state operation of the nuclear power plant given variable electricity demand [116]
2. Ensure consistent electricity generation during plant outages [116]

Potential benefits of this approach include increased operational flexibility, improved efficiency, and improved safety [116].

TESSs may be designed in a variety of configurations [116]. TerraPower has grouped their PCS and TESS into an energy island (EI). An overview of the Natrium EI design is shown in Figure 20. The TESS consists of two salt tanks: a hot tank and a cold tank. The hot salt is pumped into the hot tank from the reactor, then salt is pumped from the hot tank for conversion of thermal energy to electricity via the PCS, and finally, the cold salt is deposited in the cold tank, where it is either pumped back to the reactor or to the outlet of the hot tank for attemperation [66]. TerraPower has issued reports documenting their strategy for decoupling their nuclear island (NI) and EI [117, 118] and the U.S. NRC has issued an exemption for TerraPower to begin construction of the EI for the Natrium demonstration reactor (Kemmerer Unit 1) [119]. The topic of NI and EI decoupling is recommended for further analysis as it has significant implications for DCSA design and is a well-suited for the consequence-focused analysis structure of the TCA.

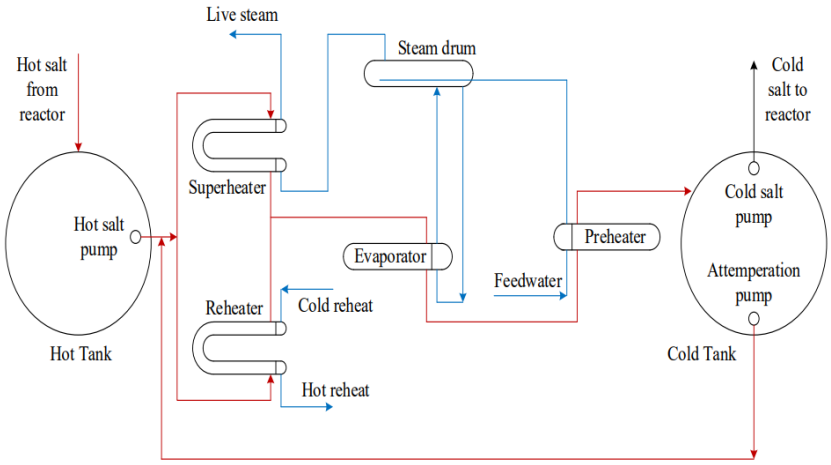

Figure 20. Natrium EI Design [66]

The fundamental sensors and actuators necessary for TESS operation are summarized in Table XL and Table XLI, respectively [66, 116, 117, 67].

3.11. Distributed Control System (DCS)

The primary functions of the Distributed Control System (DCS) are:

F.DCS.1. Coordinate control actions between plant systems to maintain operations [6, 67]

F.DCS.2. Coordinate control actions between plant systems to transition the plant between states [6, 67]

The DCS is a supervisory control system that utilizes sensor data from multiple plant systems to coordinate actuation among those systems [6, 67]. There is little information available about the specific DCS control approach to be used for the three focal SFRs of this work. A potential high-level control approach is shown in Table IV, based on references from other AR designs [120]. The fundamental sensors and actuators required for DCS operation are shown in Table XLII and Table XLIII, respectively [120]. It is assumed that:

A.22. The Distributed Control System (DCS) does not have independent actuators. The DCS provides signals to other plant systems that then respond by actuating.

Assumption A.22 is important for DCSA design because it informs the interdependencies between the DCS and other plant systems.

Table IV. DCS Control Approach [6]

Controlled Variable	Controlled Variable System	Manipulated Variable	Manipulated Variable System
SG Inlet Temperature	PCS	Control Rod Position	RCS
Main Steam Pressure	PCS	PSP Speed	PHTS
Main Steam Pressure	PCS	ISP Speed	IHTS
Main Steam Temperature	PCS	Feed Pump Speed	PCS
Electrical Load	PCS	Turbine Throttle Valve Position	PCS

3.12. Reactor Protection System (RPS)

The primary functions of the Reactor Protection System (RPS) are:

F.RPS.1. Sense design basis accident conditions [75, 63, 67, 121]

F.RPS.2. Prevent release of radionuclides in response to design basis accidents [75, 63, 67, 121]

The Natrium design will use the Curtiss-Wright RadICS platform for the RPS [67]. The RadICS platform has been accepted for use in safety-related (SR) I&C systems by the U.S. NRC [122]. To perform its functions, the RPS must detect an event that requires intervention and initiate the appropriate intervention [75, 63, 67]. The RPS can initiate a scram (i.e., deenergize the control rod solenoids to drop the rods into the reactor core) or execute engineered safety features (EFSs). The reactor scram conditions listed in the Natrium documentation are [67]:

- High neutron flux
- High hot pool temperature
- High primary sodium level
- High power-to-flow ratio
- High cold pool temperature
- High positive neutron flux rate
- High negative neutron flux rate
- Low primary sodium level
- Low power, high neutron flux
- Loss of primary sodium flow
- Loss of power to RPS
- Manual trip

The conditions monitored for initiation of an ESF are summarized in Table V [67].

Table V. RPS ESF Response and Initiation Conditions [67]

ESF	Initiation Conditions	Parameter System
PSP Trip	High cold pool temperature	PHTS
	Reactor scram	RPS
	Low neutron flux	RCS
PSP Trip	Manual trip	MCR
ISP Trip	High cold pool temperature	PHTS
	Reactor scram	RPS
	Low neutron flux	RCS
ISP Trip	High primary sodium level	PHTS
	Reactor scram	RPS
	Low neutron flux	RCS
ISP Trip	Manual trip	MCR

ESF	Initiation Conditions	Parameter System
SPS Trip	Low primary sodium level	PHTS
SPS Trip	Manual trip	MCR

To comply with requirements for RPS reliability, redundancy, and independence [123, 124, 125, 126], the following requirements/assumptions are applied to each of the scram and ESF initiation conditions. These requirements are not exhaustive, but are a fundamental list pertinent to DCSA design [126, 67].

A.23. Four independent measurement channels are provided for each Reactor Protection System (RPS) trip criterion.

A.24. The Reactor Protection System (RPS) shall trip the reactor if two-out-of-four measurement channels exceed the allowable threshold.

A.25. No single failure will prevent the Reactor Protection System (RPS) from tripping the reactor.

A.26. Manual actuation shall be available for the Reactor Protection System (RPS) and be independent of automatic actuation.

The fundamental sensors and actuators necessary for RPS operation are summarized in Table XLIV and Table XLV, respectively [67, 63, 126]. Sensors RPS.S.1-32 either provide trip parameters to the RPS or are used by the RPS to calculate trip parameters. Sensors RPS.S.33-72 are used to monitor actuation of plant systems by the RPS trip. It is assumed that:

A.27. The Reactor Protection System (RPS) has independent actuators to drop the control rods and the reserve shutdown rods.

A.28. The Reactor Protection System (RPS) provides trip signals to other plant systems that then respond by actuating.

Assumptions A.23 - A.28 are important for DCSA design because they inform the interdependencies between the RPS and other plant systems.

This page left blank

4. SFR DCSA DESIGN

This section provides the SFR DCSA template derived from the analysis performed in preceding sections, and an example of the application of cybersecurity controls to the DCSA as part of a graded approach. First, the functions identified in Section 3 are assigned to security levels according to their importance to plant safety. Second, systems are assigned to security zones based on logical and physical communication requirements between the systems.

Security levels are assigned to functions based on their importance to plant safety. Systems that perform multiple functions are placed into a security zone based on the security level assigned to the system's most important function. Based on the functions enumerated in Section 3, systems are categorized as being likely to be licensed as one of the following categories for systems, structures, and components (SSCs): safety-related (SR), non-safety related with special treatment (NSRST), or non-safety related with no special treatment (NST) [3, 4, 5]. The resulting security levels according to these classifications are shown in Table VI. Note that these SSC classifications may vary depending on the requirements of the specific SFR design.

Table VI. SFR DCSA Security Levels by SSC Classification

Security Level	SSC Classification	Systems
0	No classification – not owned or operated by operator	• Internet
1	No classification – no safety impact	• IT systems • Corporate business systems • Corporate engineering systems
2	No classification – business and operations management	• Authorized document management • Work control • Engineering historian
3	Non-safety related with no special treatment	• PCS • PHTS • IHTS • FHS • SFSS • Operations historian
	Non-safety related with special treatment	• DCS • RHR • RCS • SPS • SLM • SFP • CGS
4	Safety-related	• RPS • RSS

4.1. DCSA Template

The SFR DCSA template is shown in Figure 21. This DCSA template is consistent with both the RG 5.71 approach and the DG-5075 approach. This DCSA design template is intended to serve as

a starting point for AR designers and is not prescriptive. Further optimization of the DCSA design may be valuable given the unique design and performance requirements of the plant.

Security level 1 consists of a zone containing the IT network, business systems, and engineering systems. Systems in this level have access to the Internet via a firewall. Security level 1 is the only security level where wireless networks are permitted. Portable media and mobile devices are widely used in these systems within this security level. Systems in this zone are within the plant exclusion area (EA) and may be contained within an area of greater physical protection such as a limited access area (LAA).

Security level 2 consists of three zones containing authorized document management systems, work control systems, and the engineering historian. Portable media are used within systems in these security levels. Systems within this zone are within the plant protected area (PA). Bidirectional wired network communication through a firewall is permitted between security levels 1 and 2.

Security level 3 consists of several zones containing both NSRST and NST plant systems and supervisory control systems. The main control room (MCR) human-machine interface (HMI) and DCS serve as supervisory controllers. Operators in the MCR may interface with the DCS. The relationships between the DCS and its subordinate systems are discussed in Section 3. An architecture for a typical system is given in Figure 22. Any portable media or mobile devices brought from a lower security zone to a zone belonging to security level 3 must first be processed through a portable media and mobile device scanner. This may be necessary for system updates or maintenance. Most systems in this level are in the MCR within the plant vital area (VA), except the SFSS which is in a material accounting area (MAA). Wired network communication into security level 2 from security level 3 is permitted (e.g., the engineering historian receives data from the operations historian), but security level 2 is only permitted to send handshaking or acknowledgement signals to security level 3.

Security level 4 consists of two zones containing the plant SR systems: the RPS and RSS. Analog signals are used to for communications from the RPS to RSS. Similar to security level 3, any portable media or mobile devices brought into security level 4 must first be scanned. The systems in this level are in the instrumentation room (IR) within the plant vital area (VA). The IR is separated from the MCR. One-way communication enforced by a data diode is permitted from security level 4 to security levels 3 and 2.

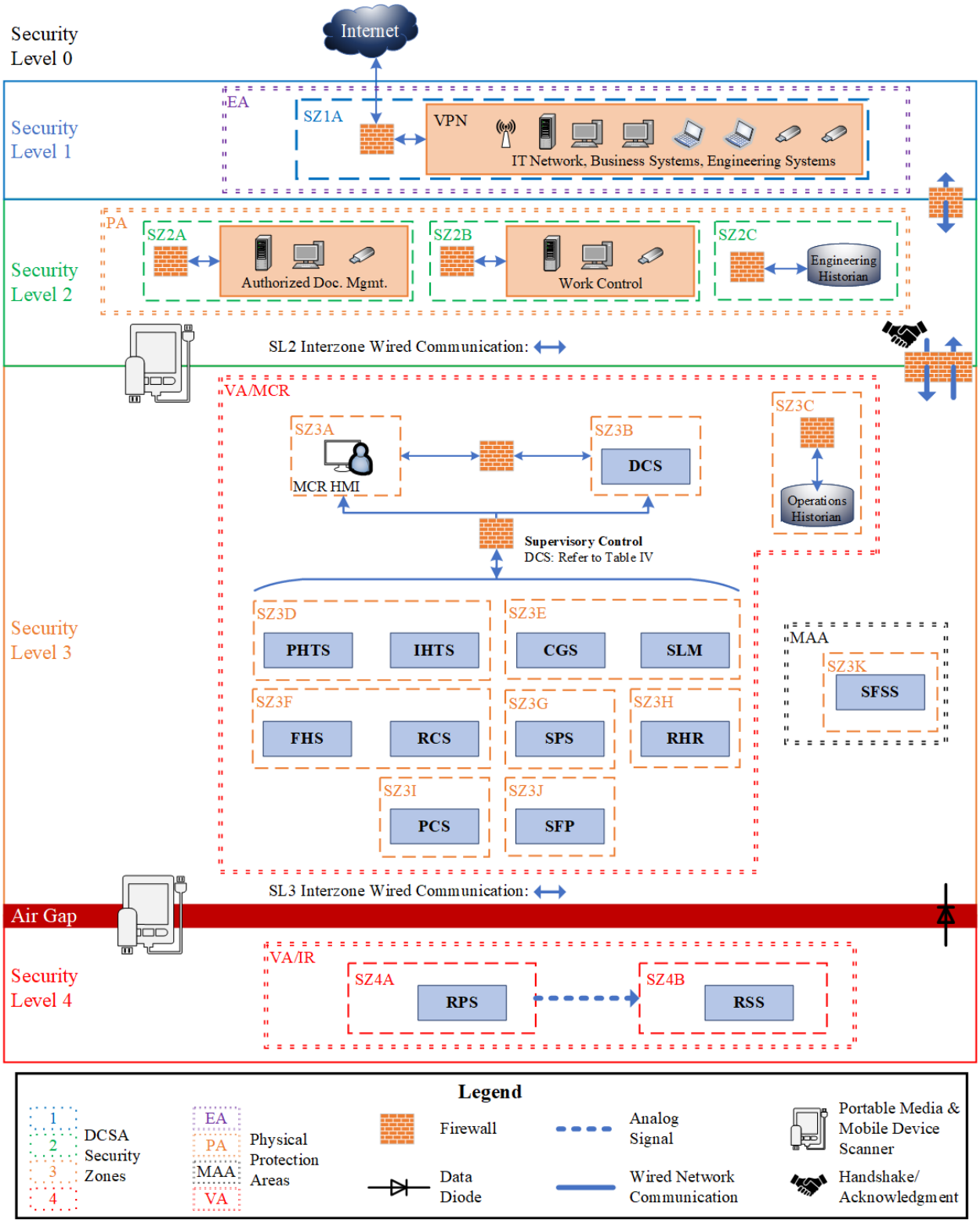

Figure 21. SFR DCSA Template

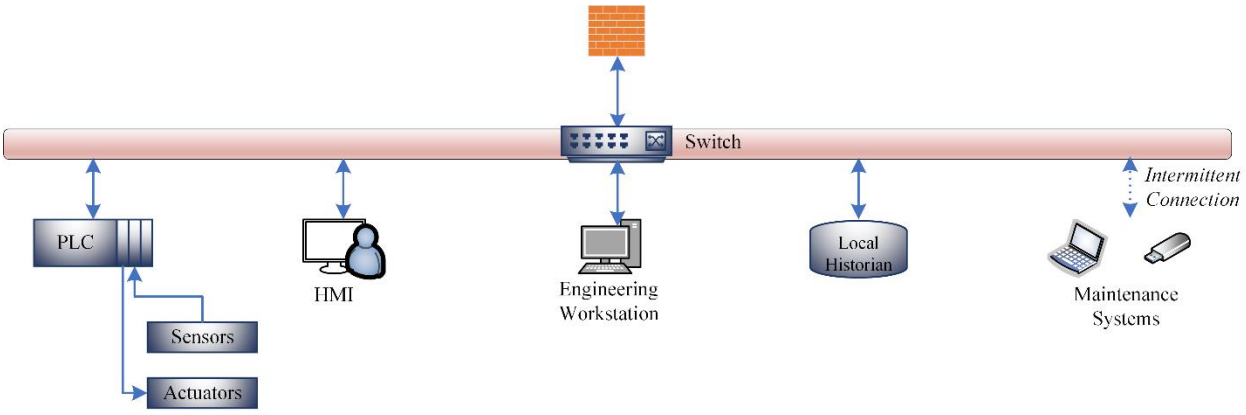

Figure 22. Example System Architecture

Two potential areas for optimization of this SFR DCSA using the DG-5075 approach discussed in the following subsections.

4.1.1. Security Level 2 Requirements May be the Basis of Protection for Some NST Systems

The primary driver for placing all NST and NSRST systems in security level 3 is the information dependence between the supervisory control systems in security level 3 and the subordinate systems. One example of this is that the DCS relies on information from the PCS to command the RCS (Table IV). Without considering information dependencies, the PCS would belong to security level 2 and the DCS and RCS would belong to security level 3. Because the DCS and RCS are protected according to security level 3 requirements, and handshakes/acknowledgements are the only communication allowed from security level 2 to 3, the PCS must also be placed in security level 3.

Using the DG-5075 approach, some NST systems may be able to be protected by security level 2 requirements if additional security requirements are applied to specific systems. For example, asymmetric cryptography or application firewalls may be used to place NST systems that provide data for supervisory control (e.g., PCS) in security level 2 rather than security level 3 [127, 128, 129]. Additional analysis is required to ensure that these cybersecurity measures are sufficient to prevent the adversary from accessing security level 3 from security level 2.

4.1.2. Multiple NST Systems May Be Assigned to the Same Zone

When using a consequence-focused analysis method such as modeling and simulation of cyber-attack scenarios, systems may be placed in the same zone when an unacceptable consequence does not occur for the set of adversary access scenarios considered in Tier 2 analysis. The key assumption of Tier 2 Adversary Functional Scenario Analysis (AFSA) is that if an adversary has access to the functions performed by a system, then they can manipulate those functions in the manner that is most conducive to the progress of the attack. The zone assignments in this template were developed based on interdependency analyses and assumptions about system performance characteristics generally common to SFRs as described in the open-source literature.

When using event tree analysis as described in [6, 18], systems may be placed in the same zone if there is not an unacceptable change in event sequence frequency (ESF) when all combinations of compromised functions are considered up to a set of the size maximum credible cyber threat. For example, if the designer applies event tree analysis to defend against an adversary capable of compromising up to three zones, the designer would consider the changes in ESFs for all

combinations of three compromised functions for all of the event trees comprising the design basis. If there was not a case where the ESF increased from a beyond-design basis event (BDBE) to design-basis event (DBE) or anticipated operational occurrence (AOO), then the systems performing those functions may be placed in the same DCSA zone. Some of the most impactful candidates for merged zones are likely to be either supervisory control zones being merged with one or more zones corresponding to subordinate systems, or zones corresponding to subsets of subordinate systems being merged.

4.1.3. DCSA Considerations for Physical Protection Systems

Additional analysis should be performed for comprehensive design of DCSA for physical protection systems (PPS). The primary functions performed using PPS are detection, delay, and response of/to adversary activity [130]. The detection, delay, and response functions are interdependent – they must occur in that order. The interdependencies between these functions will affect the assignment of systems to security zones and the communications performance requirements between security zones. If cyber-effects analysis can be applied to system performance data, analysis can be performed to obtain design constraints on security zone assignments for PPS. One approach is using force-on-force modeling and simulation and the statistical analysis of system effectiveness for cyber-attack scenarios. This approach was demonstrated in [131] for detection systems of a conceptual small modular reactor (SMR) PPS. A performance-based DCSA design for these detection systems was achieved by conducting logistic regression analysis on the defender's win rates for a set of cyber-enabled physical intrusions. Future work should examine the DCSA design of PPS including the delay response functions and the degree to which generalized PPS DCSAs may be designed for ARs.

This page left blank

5. PASSIVE CYBERSECURITY CONTROLS

Cybersecurity technologies when implemented properly can address multiple defensive strategies simultaneously across several attack pathways. Firewalls fall under the classification of a chokepoint, essentially "a strategic narrow route or gateway linking one zone to another" forcing all traffic through controlled points and providing a key location to deploy security measures. While the starting classification of a chokepoint is fitting, depending on the features utilized and how the firewall is applied, this can cross over into additional areas such as fortification and access control.

The most classic example is the firewall, which can perform network and/or application data filtering, potentially used as an IDS/IPS, allowing VPN access to segments of the network, web content filtering, among other capabilities. Cybersecurity controls that stem from optimal installation of a firewall can cover both wired and wireless attack pathways.

1. Establish a secure perimeter for inbound network connections (Fortification)
2. Strict network segmentation and isolation for critical systems (Chokepoint)
3. Treat wireless connections as outside security boundary and prohibit wireless for critical functions (Access Control)

There are many factors to consider when it comes to how a cybersecurity control is addressed, which can have effects on the degree of coverage, the defensive strategy being addressed or in some instances, covering multiple strategies. See below for some examples:

- Control: Basic restrictions on media use, such as disabling USB ports
- Implementation options:
    - Disable USB ports by removal of USB drivers on workstations. Effective but potentially circumventable without appropriate privilege management.
    - Utilizing an endpoint detection response tool such as Crowdstrike, Sentinel or Microsoft Defender. This would be managed at a server where policies would be retrieved by agents installed on endpoints such as workstations and servers. This works so long as the agent has obtained the policy that applies restrictions to the workstation, and the agent itself is not tampered with.
    - Physical disconnection of wiring support for USB ports. This adequately restricts the user from utilizing the USB ports so long as physical access is also restricted.

While at first, the control of basic restrictions on media use falls under the defensive strategy of fortification, depending on location and method of the can also be considered anti-access.

A technology well fitted for the realm of a nuclear plant, data diodes (or unidirectional security gateways), act as one-way gateway devices used to enforce unidirectional data flow between networks of different security levels. This technology allows data to be sent out of high-security zones (e.g. reactor or safety systems) to lower security zones or corporate systems, while preventing any incoming traffic to the critical zone. This supports strong isolation controls; NRC guidance explicitly recommends such one-way communication mechanisms (e.g. "implementation of data diodes to enforce one-way data flows" as a security control [6]). By physically blocking all reverse traffic, a diode protects the wired network connectivity pathway into critical systems, effectively acting as an anti-access measure that prevents adversaries from establishing any interactive access into sensitive networks. In practice, data diodes help implement multiple cybersecurity controls (e.g. inbound traffic denial, controlled data export) and create layered security barriers. This algins with a defense-in-depth strategy by adding a hardened boundary that an attacker cannot traverse, while still permitting necessary data monitoring or business integration from the secure zone [6].

The remainder of this section provides example applications of passive technical and operational cybersecurity controls to address the four attack pathways within scope of DCSA design: physical access, wired connectivity, wireless cone activity, and portable media and mobile devices. Controls from U.S. NRC Reg. Guide 5.71 Appendix B and C are referenced for technical and operational controls, respectively. At increased security levels, the controls are compounded, meaning for example that at Level 2, it is intended that all Level 1 controls, plus the additional Level 2 controls, are applied and so on as the levels increase. Active controls may be assigned as part of Denial of Task Analysis in the DG-5075 approach.

The controls for the physical access, wired, wireless, and portable media cybersecurity control tables are informed by Reg Guide 5.71 Rev1 Appendix B and C [7]. However, they have been adapted to apply a graded approach and implement DiD in accordance with their assigned security level. These controls are intended to serve as a starting point for AR designers and are not prescriptive. Further optimization of the controls may be necessary given the unique design and performance requirements of the plant.

Generally, the requirements are associated with security level applying a graded approach. The graded requirements (i.e., goals) associated each security level are specified below:

- **Security Level 1: Available**
  Implement policies to ensure all access points are identified and that basic security controls are in place to allow authorized personnel access while preventing unauthorized entry. Ensure all access-related actions are documented and monitored
- **Security Level 2: Controlled**
  Establish both policy-driven and technical controls to manage and monitor access, ensuring only authorized personnel can enter sensitive areas. Implement systems to log all access attempts and provide alerts for any unauthorized access attempts.
- **Security Level 3: Mitigated**
  Deploy advanced technical controls to actively prevent unauthorized access, including the use of encryption, secure authentication, and continuous monitoring. Implement systems to automatically detect and respond to any potential access breaches.
- **Security Level 4: Eliminate or Stringent Restrictions on Access**
  Eliminate attack pathways not needed, and where not possible strictly limit, control and monitor authorized access in real time to reduce the likelihood of unauthorized access to as low as possible. Enforce strict technical controls that restrict access to only essential personnel through the use of multi-factor authentication and physical barriers.

5.1. Physical Access Cybersecurity Controls

Physical access to critical systems is a significant cybersecurity concern, as unauthorized access can lead to direct tampering with or sabotage of essential infrastructure. The attack pathway often begins with physical entry into secured areas, where the adversary can manipulate, disable, or extract information from CDAs. This threat requires controls that fortify the physical environment, establish choke points that can be monitored, and enforce strict access control measures to prevent unauthorized intrusions.

The controls outlined in Table VII provide a layered defense strategy to mitigate these risks. At Level 1, basic access control mechanisms such as user ID and password, combined with general awareness training, create an initial barrier that deters casual intruders and ensures that all personnel

understand the importance of security. As the security level increases, controls evolve to include encryption of data at rest, the use of tamper-evident seals, and the implementation of automated mechanisms for detecting unauthorized access, all of which fortify the environment against more sophisticated attacks. At the highest security level, network access control, cryptographic communication, and rigorous personnel security policies establish multiple choke points and reinforce access control. These measures collectively ensure that any attempt to physically breach the system is met with multiple layers of defense, making it exceedingly difficult for an attacker to succeed. Implementing layered physical access controls ensures that unauthorized access to CDAs is effectively prevented through fortified environments and multiple security checkpoints.

Table VII. Physical Access Attack Pathway Cybersecurity Controls

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
1	B.2.2	Auditable Events	Logging of access to systems	Fortification	1. Ensure that Windows Event ID 4624 and 4625, Linux PAM/SSH auth logs, badge-reader events, and PLC/HMI session logs 2. Correlated physical-to-logical audit: Link door-controller logs such as with system log-ins (root SSH to switch a-42, 14:04) via a ticket number or personnel ID for forensics.
	B.3.7	Transmission Confidentiality	Enforcing physical security measures for wiring closets and network hardware	Access Control	1. Layered enclosure protection: Lock racks with electronic strikes tied to the PACS; mount the racks inside a locked closet; place the closet inside a badge-restricted corridor. 2. Cable management & seal-in: Route copper and fiber through overhead ladder trays with locked cover plates. Utilize tamper-evident seals to patch-panel doors and to cover unused switch ports.
				Fortification, Chokepoint	Out-of-band console isolation: Isolate the management network for switch/router serial consoles using a dedicated firewall. Require MFA over SSH to the console server, blocking local console ports.
	B.3.9	Cryptographic Key Establishment and Management	Limited physical access controls, such as keycard access	Fortification, Access Control	Role-based badge profiles: Define granular access zones (ex. CCR, UPS room, network racks) and map each job role to exactly the zones required; push profiles to the programmable automation controllers (PACS).
				Chokepoint, Access Control	Anti-pass-back & tailgate detection: Enable “must-exit-to-re-enter” logic and add optical tailgate sensors on single-person portals; deny the badge if it was not recorded exiting.
	C.10.2	Awareness Training	General awareness training on physical security and cybersecurity	N/A	Operational Control: N/A
2	B.1.13	Automated Marking	Use of automated labeling for	Fortification	Regex & ML classifiers: detect PII, export-controlled data, or “NRC Safeguards” phrases in real time; matching files are auto-encrypted or blocked from removable media.

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
			information classification and protection	Access Control	Mandatory label enforcement in productivity tools: Office, Adobe, and CAD plugins force a label before save; unlabeled documents cannot be printed or emailed.
	B.1.18	Insecure and Rogue Connections	Procedures to promptly identify and remove or disable any unauthorized physical connections or interfaces	Fortification	Physical inspection: Quarterly review of racks and raceways, cross-checked against the diagram and change-control tickets.
	B.1.18	Insecure and Rogue Connections	Procedures to promptly identify and remove or disable any unauthorized physical connections or interfaces	Fortification, Access Control	Switch port security: shut or restrict a port if a new MAC address appears or the MAC count exceeds one.
	B.2.12	Audit Generation	Capability to compile audit records of physical access with correlated timestamps	Fortification	1. Device time-sync enforcement: configure door controllers, badge readers, cameras, kiosks, and access servers to reject/flag if clock drift exceeds a specified threshold. Alert the SOC if threshold is exceeded. 2. Centralized log collection: forward all physical-access events (PACS, turnstile, man-trap, lock sensors, chassis-intrusion switches, escort events), to a hardened log collector or SIEM via TLS (such as syslog-TLS, HTTPS, or native API).
				Fortification, Chokepoint	Single authoritative time source: enforce device and server clocks to a secure, authenticated NTP hierarchy, and require ISO-8601 timestamps with time zone.
	B.3.7	Transmission Confidentiality	Physical security measures such as tamper-	Fortification	Serialized void-if-removed labels: across chassis seams, drive bays, and module doors; scan serials during quarterly audits to detect swaps.

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
			evident seals on significant devices	Fortification, Access Control	1. Chassis-intrusion switch tied to SIEM: set up alarm capabilities in the event of opening the cover and timestamps the event in system logs. 2. Locking security screws: Utilize Torx-pin, Tri-wing screws plus colored epoxy on screw heads to show rotation or removal
	B.5.3	Changes to File System and Operating System Permissions	Limited functionality configuration to reduce vulnerabilities	Fortification	1. Hardened build images: Ensure OS uses required services only (ex. disable print spooler, SMB v1, legacy Bluetooth, IPv6 if unused) and for provisioning processes, deploy with configuration-as-code. 2. Enable Runtime controls: For Linux enforce SELinux/AppArmor or for Windows Exploit Guard rules that deny network or file access outside the defined need. 3. Continuous configuration drift monitoring: compare live device state to gold image with osquery/SCCM. Develop process to auto-remediate or quarantine if extra services appear.
	C.2.1	Personnel Security Policy and Procedures	Personnel security policies and procedures to ensure authorized access	N/A	Operational Control: N/A
	C.4.1	System Maintenance Policy and Procedures	System maintenance policy and procedures which cover assets located in all security boundaries (owner-controlled area, protected area, vital area)	N/A	Operational Control: N/A
	C.5.2	Third-Party/ Escorted Access	Screening and documenting security controls	N/A	Operational Control: N/A

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
			for third-party personnel		
	C.5.4	Physical Access Authorizations	Control and verify all entry/exit points to secure areas. Maintaining a list of, and issuing authorization credentials	N/A	Operational Control: N/A
	C.5.5	Physical Access Control	Access limited to authorized personnel only	N/A	Operational Control: N/A
3	B.3.2	Application Partitioning and Security Function Isolation	Configure CDAs to isolate critical security functions from non-security and other security functions while minimizing the inclusion of non-security functions within the isolation boundary.	Fortification	Function-specific hardware: run security logic controllers (e.g., SIS PLC, HSM) on their own chassis while hosting non-security apps elsewhere.
				Fortification, Access Control	Virtual or container isolation: separate VMs/containers with hypervisor or kernel-enforced boundaries; disable shared memory and inter-VM communication.
	B.3.3	Shared Resources	Use physically separate network devices to create and maintain logical separation of Levels 3 and 4 from each other and other levels	Access Control	Dedicated hardware per level: separate L3 switches, routers, and firewalls—no shared chassis, no cross-stack links.
				Fortification, Access Control	1. Uni-directional gateways: Utilize data diodes to allow one-way historian or syslog flows while blocking any path back into Level 3 assets. 2. Air-gapped or fiber-optic links: color-coded, separately routed cabling and patch panels. Ensure that VLAN trunking is disabled between security levels.

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
					3. Out-of-band management: a third, physically isolated network for switch/router console ports so production traffic can never traverse management paths.
	B.3.6	Transmission Integrity	Implement alternative controls and document the justification of countermeasures when a CDA cannot support transmission integrity and physically restrict access or sufficient monitoring to the CDA.	Fortification	Overlay encryption/tunneling: IPSec, TLS proxy, or MACsec applied at an upstream switch or firewall to protect data in transit.
				Fortification, Chokepoint	Anomaly detection: SPAN/TAP feeding an IDS that watches for protocol deviations from the CDA
				Fortification, Access Control	Continuous integrity verification: digital signatures or hashed sequence numbers checked by a guard device; alarm on mismatch. Strict physical safeguards: locked cages, tamper-evident seals, and CCTV covering the CDA; badge logs correlated with any config change.
	B.4.2	User Identification and Authentication	Implement identification and authentication technology to verify individuals, processes, and devices physically interacting with CDAs	Access Control	1. MFA at the door and the console: badge + PIN for rack access, then smart-card/FIDO2 for the CDA keyboard or KVM. 2. Device certificates & 802.1X: ports stay disabled until the CDA's TPM-issued X.509 cert successfully authenticates. 3. Secure-boot attestation: CDA refuses to execute code or accept field programming unless the signer's cert matches an internal trust store. 4. Signed maintenance tools: engineering laptops and USB media must present a valid code-signing cert before the CDA will enable its service port.
	C.5.5	Physical Access Control	Locked doors with multi-factor authentication and biometric access		Operational Control: No Example

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
	C.11.8	Least Functionality	Ensure CDAs have no unnecessary applications, functions, utilities, services, communication capabilities, interfaces, or peripherals beyond those needed for safety, security and emergency preparedness functions		Operational Control: No Example
4	B.1.1	Access Control Policy and Procedures	Access control policies and procedures for CDAs	Fortification	1. Credential hygiene requirements (≥12-character passwords, MFA for admin, unique vendor accounts) written into the policy and enforced by technical controls. 2. Mandatory training & acknowledgement: personnel must pass a CDA-specific security module and sign the policy before credentials are activated.
				Access Control	Standard operating procedures (SOPs): for request → approval → grant → review of access; require management + cybersecurity sign-off for any new privilege.
				Fortification, Chokepoint	1. Document a role-based access matrix that maps each CDA, function, and maintenance port to the minimum job roles allowed (operator, engineer, vendor). 2. Emergency access (“break-glass”) procedure with one-time passwords kept in a sealed envelope or password vault; every use must be justified and logged.
	B.1.15	Network Access Control	Network access control and monitoring for	Fortification, Access Control	1. 802.1X or MACsec on every switch port—devices must present a machine certificate; unrecognized hardware is placed in a quarantine VLAN with no east-west routes.

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
			unauthorized access		2. Port-security limits & automatic shutdown if a new MAC address appears or the MAC count exceeds one.
	B.4.4	Non-authenticated Human-Machine Interaction Security	Ensure physical security measures restricting access on CDAs to authorized personnel and ability to be tracked to specific individuals	Fortification, Chokepoint	1. Electronic badge + PIN or biometric: For rack doors or cages housing CDAs ensure authentication controller logs badge ID, time, and location. 2. Anti-tailgating portals: Install turnstiles or man-traps for high-value areas to guarantee single-person entry.
	B.4.5	Device Identification and Authentication	Ensure physical security measures restricting access on CDAs to authorized personnel and ability to be tracked to specific individuals	Fortification	Tamper-evident seals and chassis-intrusion switches: Install integrity measures for systems pertaining to physical-access. Alerts fire if opened without an authorized badge swipe.
	B.4.6	Identifier Management	Ensure physical security measures restricting access on CDAs to authorized personnel and ability to be tracked to specific individuals	Access Control	Real-time linkage to HR/AD so a terminated employee's badge and logical accounts disable simultaneously, blocking physical and console access.

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
	C.5.5	Physical Access Control	Confine all devices and networks to vital areas	N/A	Operational Control: N/A
	C.11.2	Configuration Management Policy and Procedures	Configuration management for controlling changes to CDAs	N/A	Operational Control: N/A

5.2. Wired Connectivity Cybersecurity Controls

Wired network connections in critical infrastructure present a potential attack pathway where adversaries can intercept, manipulate, or disrupt data communications essential to operational integrity. The adversary may exploit vulnerabilities within the wired network to gain unauthorized access, introduce malicious software, or reroute data, leading to disruptive failures in system operations.

The controls detailed in Table VIII focus on creating a secure network environment, establishing choke points to restrict unauthorized access, and enforcing stringent access controls. At Level 1, basic firewall configurations and secure password policies provide an initial layer of defense, preventing unauthorized traffic and ensuring that only trusted users can access the network. As security levels increase, measures such as VLAN segmentation, application whitelisting, and strict firewall filtering rules further fortify the network by isolating traffic and limiting the scope of potential attacks. At the highest security level, the implementation of strict network segmentation, data diodes for one-way data flows, and end-to-end encryption establishes multiple choke points, ensuring that even if one layer of defense is breached, subsequent layers continue to protect the system. Comprehensive wired restrictions create robust barriers that prevent unauthorized network access, ensuring secure data transmission and protecting critical systems.

Table VIII. Wired Connectivity Attack Pathway Cybersecurity Controls

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
1	B.1.12	Permitted Actions without Identification or Authentication	Document specific actions allowed without authentication under controlled conditions	Access Control	1. Pre-approved maintenance windows: authentication bypass (console logged-in session) allowed only during declared outage with change-ticket ID. 2. Physical presence requirement: unauthenticated console available solely via local serial port inside locked rack; door badge swipe + CCTV provide operator attribution.
	B.1.15	Network Access Control	Implement basic network access control using MAC address locking and physical isolation	Fortification, Access Control	1. Port-security on switches: Utilize Sticky MAC or static binding (max 1) per port. Log any violations and ensure the response action causes a port shutdown or restriction. 2. Unused ports administratively down: label & lock with port blockers to deter casual plug-ins. 3. Quarantine VLAN: A potential alternative to the port security on switches is to respond to any unknown MAC be moved automatically to an isolated network with no east-west routes and captive portal for IT ticketing. 4. Physical separation: color-coded patch panels and cables; dedicated switches for OT devices so IT endpoints cannot cross-connect.
	B.4.1	Identification and Authentication Policies and Procedures	Use of secure passwords and regular password changes for network devices	Fortification	1. Strong credential policy: Require 15 characters or greater, mixed type, no vendor defaults; enforce via TACACS+/RADIUS or device-local rules. 2. Disable plaintext protocols: turn off insecure protocols such as Telnet and HTTP. Enforce SSHv2 + strong ciphers with HTTPS and TLS 1.2+ only.

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
				Fortification, Chokepoint	1. Per-device unique secrets: auto-generate random passwords or key-strings during provisioning. Store the privileged credentials in a password vault (such as HashiCorp Vault, CyberArk). 2. Automated rotation: run vaulted API/CLI playbooks (such as Ansible, Nornir) that change device passwords every 90 days and update the vault entry. Can also be done through password management solutions.
	C.7	Defense-in-Depth Defensive Security Architecture	Basic firewall configurations to allow only necessary traffic	Chokepoint, Access Control	1. Default-deny rule set: drop all inbound/outbound packets except those explicitly permitted. Create a least-privilege baseline. 2. Stateful inspection with protocol validation: enable deep-packet inspection, allowing for permitting by service, and not port range. Commonly found protocols might consist of Modbus, DNP3, EtherNet/IP; reject malformed or unexpected command codes.
				Fortification, Access Control	Zone-based policy model: segment OT/ICS levels (L3, L2, L1) and IT networks into security zones; apply rules at each zone boundary.
	C.8.2	Incident Response Training	Simplified incident response plans focusing on wired network breaches	N/A	Operational Control: N/A
	C.10.2	Awareness Training	Establish and document awareness training for employees and contractors that address site-specific objectives, management	N/A	Operational Control: N/A

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
			expectations, roles, responsibilities, policies and procedures with the cybersecurity program		
	C.11.1	Configuration Management	Basic logging and monitoring of wired connections	N/A	Operational Control: N/A
2	B.1.20	Proprietary Protocol Visibility	Implement alternative controls for proprietary protocols lacking visibility	Fortification	Alternative Control is dependent on protocol
	B.2.2	Auditable Events	Defining list of auditable events and frequency of auditing for each identified auditable event	Fortification	Auditable Events are dependent on environment
	B.5.3	Changes to File System and Operating System Permissions	Application whitelisting to control software execution on networked devices	Fortification	1. OS-native application control enforcement: Using tools such as Applocker or Windows Defender Application Control for Windows, Gatekeeper or Configuration Profiles for macOS, SELinux/AppArmor allow-exec policies for Linux 2. Digital-signature enforcement: permit execution only when binaries or scripts are trusted internal or vendor certificates
	C.3.5	Security Alerts and Advisories	Implementation of automated tools for monitoring and logging network activity	N/A	Operational Control: N/A

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
	C.3.7	Software, Firmware, and Information Integrity	Ensure DA software, firmware, and data protected from unauthorized changes when employing hardware access controls	N/A	Operational Control: N/A
	C.7	Defense-in-Depth Defensive Security Architecture	Network intrusion detection and prevention systems (IDPS) deployed at key points	Chokepoint	Map critical choke-points – perimeter (north-south), data-center core, DMZ, VPN concentrators, cloud VPC/VNet ingress/egress, and inter-segment “east-west” paths; mandate an IDPS sensor (inline or passive) at each.
				Fortification, Chokepoint	1. Inline NGIPS at gateways – deploy high-availability (A/A or A/S) pairs behind the edge firewall so malicious traffic can be dropped in real time. 2. Passive IDS on aggregation links – use TAPs or switch SPAN sessions to mirror traffic from core/leaf switches and server VLAN trunks to out-of-band sensors.
3	C.13.1	Threat and Vulnerability Management	Routine network configuration reviews to identify and rectify vulnerabilities	N/A	Operational Control: N/A
	B.3.7	Transmission Confidentiality	End-to-end encryption of all data transmitted over wired connections	Fortification	Authenticated Encryption Protocols
	B.5.3	Changes to File System and Operating System Permissions	Restriction of network services to only those necessary for operations	Fortification	1. Service inventory & baselining — run automated port-scans / flow-analytics to map every listening service, then lock the “known-good” list in a Configuration Management Database (a centralized repository for storing configs)

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
					2. Host-based firewalls: Utilize host-based functionality such as Windows Defender FW, iptables, or pf to enforce a least-service rule set at the OS layer.
				Fortification, Chokepoint	Perimeter & internal firewall ACLs — explicit deny-all, allow-by-exception rulesets for inbound and outbound ports/protocols. Additionally apply this logic to all routers and switches.
	C.5.6	Access Control for Transmission Medium	Physical access control for network devices and conduits	N/A	Operational Control: N/A
	C.11.4	Configuration Change Control	Regular network audits to ensure compliance with security policies	N/A	Operational Control: N/A
	C.11.6	Access Restrictions for Change	Secure boot mechanisms to prevent unauthorized modifications to network devices	Fortification	Secure boot enabled BIOS and Operating System
	C.12.6	Licensee/Applicant Testing	Periodic testing and review of network security controls	N/A	Operational Control: N/A
4	B.3.4	Denial of Service Protection	Strict network segmentation and isolation for critical systems	Fortification	Dedicated VLAN + VRF instances — unique segments per critical zone; no route-leaking between VRFs except via controlled paths
				Fortification, Access Control	Physical or air-gapped separation — dedicated cabling, switches, and racks for ICS/OT or other crown-jewel assets; no shared uplinks with corporate LAN
	B.5.4	Hardware Configuration	Implementation of data diodes to	Fortification, Chokepoint	1. Certified hardware data-diode appliance – purpose-built chassis with physically

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
			enforce one-way data flows		separate TX / RX optics or photonic couplers that make reverse signaling impossible 2. Fiber pair cut-back (TX-only) – use single-strand transmit fibre on the “high-side” and receive only on the “low-side”; epoxy or cap the unused RX port to prevent reconnection
				Fortification, Access Control	1. Remove internal plug-in radios: Physically disable M.2 Key-E / mini-PCIe card capabilities by disconnecting antenna leads, removal of cards. Install a blank filler or EMI shield so the slot can’t be reused. Extract WiFi adapter cards, fit a vented slot cover, and apply tamper-evident measures. 2. TPM-measured boot of device tree – include absence of wireless adapters in PCR values; SIEM rules trigger if boot attestation deviates
	C.5.6	Access Control for Transmission Medium	Strict access controls and auditing for physical access to network devices	N/A	Operational Control: N/A
	C.11.2	Configuration Management Policy and Procedures	Rigorous change management procedures for network configurations	N/A	Operational Control: N/A
	C.13.1	Threat and Vulnerability Management	Regular security assessments and validation of wired network integrity	N/A	Operational Control: N/A

5.3. Wireless Connectivity Cybersecurity Controls

Wireless connectivity introduces significant vulnerabilities in critical infrastructure due to its inherent exposure to external threats. The adversary may exploit wireless networks to gain unauthorized access, intercept data, or introduce malicious traffic without needing direct physical access to the facility. Wireless networks, if not properly secured or restricted, can serve as an open gateway for cyber-attacks, allowing the adversary to bypass physical security measures and penetrate deeper into the network, potentially compromising CDAs.

The controls outlined in Table IX are designed to fortify the network environment, establish choke points, and enforce strict access control over wireless connectivity. At Level 1, the strategy begins with the basic restriction of wireless access, including disabling wireless interfaces by default and enforcing strong encryption and password policies on any wireless networks that are permitted in less critical areas. As the security level increases, more stringent controls are implemented, such as restricting wireless connectivity through group policies and device management software, and whitelisting devices with disabled wireless functionality. At the highest security level (Level 4), all wireless network interfaces on critical systems are completely disabled or physically removed, and RF shielding is implemented to prevent any unauthorized wireless communication. Outright restrictions and stringent controls on wireless connectivity effectively eliminate unauthorized access risks, safeguarding critical systems from wireless-based cyber threats.

Table IX. Wireless Connectivity Attack Pathway Cybersecurity Controls

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
1	B.4.2	User Identification and Authentication	Require strong passwords and encryption on any wireless networks that are permitted in less critical areas	Fortification	1. Mandate modern encryption: Configure all access points to allow WPA3-Personal (SAE) or WPA3/WPA2-Enterprise (AES-CCMP) exclusively; disable WEP, WPA, and TKIP ciphers at the controller or AP profile level. 2. Certificates: Certificate-based enterprise authentication or an individual/group-based PSKs as a fallback
				Chokepoint, Access Control	Wireless IDS/IPS monitoring: Run wireless intrusion prevention systems to detect rogue open or weakly encrypted SSIDs and alert or auto-contain offending access points.
	C.3.4	Monitoring Tools and Techniques	Establish procedures for monitoring wireless incidents	N/A	Operational Control: N/A
	C.5.5	Physical Access Control	General guidelines limiting the use of wireless devices in less critical areas	N/A	Operational Control: N/A
2	B.1.17	Wireless Access Restrictions	Treat wireless connections as outside security boundary and prohibit wireless for critical functions	Fortification	1. Define wireless as an “external zone”: When creating a network diagram, map the WLAN to its own DMZ-style VLAN / VRF, behind a firewall that treats it exactly like the public Internet. 2. Disable or remove wireless capability on critical hosts: Pull Wi-Fi/Bluetooth cards, disconnect antennas, or set BIOS/UEFI to Disable WLAN and lock firmware with an admin password. For managed endpoints, utilize GPO to restrict WLAN AutoConfig on Windows or blacklist modules (ex. Cfg80211, iwlwifi) on Linux

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
					3. Port-level network admission control: Enforce 802.1X or MAC-Auth on every wired port so a rogue AP plugged into Ethernet is placed in a quarantine VLAN or blocked outright.
				Chokepoint	Access-point engineering controls: Mount APs for non-critical areas so lobes point away from sensitive spaces; reduce transmit power and use directional antennas.
				Fortification, Access Control	RF containment for restricted zones: Line walls, ceilings, and doors with copper mesh or conductive paint. Apply RF-blocking window film to stop 2.4 / 5 GHz signals from leaking in or out.
	B.1.18	Insecure and Rogue Connections	Rogue Wireless Monitoring: Implement continuous monitoring or periodic scans to detect any unauthorized wireless devices or access points, allowing prompt removal of rogue connections.	Fortification	1. Continuous, automated monitoring: Deploy an enterprise-class Wireless IDS/IPS platform. Dedicate one radio per AP or use separate sensor APs to scan every 2.4 / 5 / 6 GHz channel around-the-clock. Enable background/Guard radio mode on dual- or tri-radio APs so infrastructure performs passive and active scans while still serving clients. 2. Baseline management & alerting: Maintain a signed, version-controlled list of authorized AP MACs/SSIDs; WIPS compares detections against this whitelist and raises Severity-1 alerts the SOC
	B.3.16	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	Restricting wireless connectivity through group policies or device management software	Fortification	Linux: Configure the NetworkManager keyfile (/etc/NetworkManager/system-connections/<ssid>.nmconnection) with autoconnect=yes; mark the interface unmanaged in nmcli or use polkit rules to deny non-root Wi-Fi edits.
				Fortification, Chokepoint	Windows - Active Directory: Create a GPO Wireless Network (IEEE 802.11) policy that lists

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
					only approved SSIDs, forces WPA2/3 + 802.1X, and checks “Prevent connections to ad-hoc and non-preferred networks.”
				Fortification, Access Control	Windows - Mobile Device Management: Deploy a Wi-Fi profile that auto-joins the corporate SSID which can be done by setting CSP WiFiBlockManualConfig = 1 to disable manual network creation and edits.
	B.4.5	Device Identification and Authentication	Whitelisting of devices and applications that are permitted to operate with wireless functionality disabled	Access Control	Authorative allow-list (CMDB – Configuration Management Database) - Maintain device IDs (serial, TPM EKpub, MACs) and approved app hashes/publishers certs for systems
	B.5.1	Removal of Unnecessary Services and Programs	Basic restriction of wireless access, including disabling wireless by default on all devices	Fortification	Endpoint “device-control” policies - Use endpoint detection response or antivirus platforms (such as CrowdStrike, Trellix, etc.), block all 802.11 and Bluetooth class devices unless a hardware ID is whitelisted.
				Access Control	1. Provisioning & automation hooks: Using tooling (such as SCCM, Intune, or Ansible) ensure “first-boot” tasks verify network adapters are disabled (ex. Get-NetAdapter | Where-Object {$_.InterfaceDescription -match 'Wireless'} | Disable-NetAdapter). 2. Removing the drivers at the host level of a windows/linux OS. Requires restriction of privileged accounts to truly function’
				Fortification, Access Control	Firmware / BIOS lockdown - Disable embedded Wi-Fi & Bluetooth radios in BIOS settings while setting a supervisor password, and push the setting fleet-wide with vendor management tools

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
					(such as Dell Command, Lenovo Commercial Vantage).
	C.5.4	Physical Access Authorizations	Strict procedures for approving and documenting any temporary wireless access	N/A	Operational Control: N/A
	C.10.2	Awareness Training	Awareness training for staff on the importance of wireless restrictions	N/A	Operational Control: N/A
	C.11.4	Configuration Change Control	Routine checks for unauthorized wireless devices or access points in the facility	N/A	Operational Control: N/A
	C.11.6	Access Restrictions for Change	Limit permission to change wireless devices or access points to authorized personnel	N/A	Operational Control: N/A
3	B.3.14	Mobile Code	Block all wireless protocols at the network level through firewalls and access points	Fortification, Chokepoint	Enable blocking of unauthorized communications at wireless access points and wireless gateways.
	B.3.15	Secure Name/Address Resolution Service (Authoritative/Trusted Source)	Use of firmware settings to permanently disable wireless capabilities	Fortification, Access Control	1. BIOS / UEFI “Radio Disable” options — turn off Wi-Fi, Bluetooth, WWAN in setup; lock BIOS with strong admin password 2. Firmware configuration lockdown — enable “write-protect” or “flash guard” so wireless-related NVRAM variables cannot be altered

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
					without physical jumper or cryptographic signed update 3. Tamper-evident seals & intrusion sensors on chassis covering any jumpers or card slots that could restore RF
	B.5.4	Hardware Configuration	Disabling wireless drivers and software in the operating system on critical systems	Fortification	1. Remove or block wireless NIC drivers in the base image – in Windows, strip *.inf / *.sys packages. For Linux, blacklist the kernel modules (/etc/modprobe.d/blacklist.conf) before system deployment 2. Application block-listing – WDAC or Carbon Black policies that block executables invoking WLAN APIs (such as netsh wlan, inSSIDer, Aircrack-ng) on critical systems (iii) Host-based intrusion prevention – Endpoint detection response rules that terminate processes opening RF device handles (such as \Device\NDMPump* or /dev/ath*) and generate an alert to the SOC
				Fortification, Access Control	GPO / MDM policy to disable WLAN service – set Windows “WlanSvc” startup type to Disabled and enforce via Group Policy → Security Settings → System Services; verify compliance through SCCM/Intune reports
	C.5.1	Physical Protection Policies and Procedures	Policy allowing wireless connectivity only with explicit, time-limited, and documented exceptions	N/A	Operational Control: N/A
	C.5.6	Access Control for Transmission Medium	Implementation of RF shielding in sensitive areas or CDAs to prevent	N/A	Operational Control: N/A

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Example
			any wireless communications		
4	B.5.4	Hardware Configuration	Physical removal of wireless hardware (e.g., Wi-Fi cards, Bluetooth modules) from critical systems	Fortification	Order RF-free hardware SKUs – specify “no-WLAN/Bluetooth” build options or industrial variants that ship without radio modules or embedded antennas
	C.5.2	Third-Party/Escorted Access	Policy enforcing a total ban on wireless devices in critical areas	N/A	Operational Control: N/A
	C.5.3	Physical Protection	Rigorous access control procedures ensuring no wireless-enabled devices enter secured areas	N/A	Operational Control: N/A
	C.11.4	Configuration Change Control	Regular security audits to ensure compliance with the no wireless policy	N/A	Operational Control: N/A

5.4. Portable Media and Mobile Devices Cybersecurity Controls

Portable media, such as USB drives and external hard drives, pose a significant attack pathway in cybersecurity. These devices can be used to introduce malware, exfiltrate sensitive data, or bypass network security controls. An adversary might gain physical access to a facility or deceive an employee into using a compromised device, thereby allowing malicious software to spread through the network or enabling unauthorized access to CDAs. Given the portability and general usefulness of portable media, controlling their use is essential to safeguarding the security and integrity of critical systems.

The controls detailed in Table X are focused on fortifying the environment against unauthorized use of portable media, establishing choke points through stringent controls, and enforcing strict access management. At Level 1, basic measures such as disabling USB ports by default and enforcing password protection on media devices serve as initial barriers, reducing the risk of unauthorized access. As security levels escalate, the controls include automated scanning for malware, the use of access control lists (ACLs) to limit access, and strict logging and monitoring of media use. At the highest security level, mandatory encryption, secure wiping tools, and the physical disabling or removal of media interfaces create designated choke points, ensuring that even if a portable device is introduced into the environment, its ability to compromise systems is significantly hindered. These measures collectively enhance access control, making it challenging for an adversary to leverage portable media as a pathway for cyber threats. Strict controls on portable media usage significantly reduce the risk of malware introduction and data exfiltration, reinforcing the security of CDAs.

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

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
1	B.1.19	Access Control for Portable Media and Mobile Devices	Establish usage restrictions for portable media and enforce mobile devices are only used in one security level and that mobile devices are not mobile between security levels	Fortification, Access Control	Restrict mobile devices to a single security zone: Define zones by hardware and network layers, issue zone specific X.509 certificates and bind them to the device TPM. 8021.X/NAC admits the device only to its home virtual local area network (VLAN).
				Fortification, Chokepoint	1. Physical segregation and access points: Utilize Faraday-caged cabinets at each zone boundary, enforcing personnel to deposit devices before crossing to another level. Apply tamper-evident seals 2. One-zone-only firmware settings: Lock BIOS to disable WiFi/Bluetooth adapters not used in the assigned zones. Use Mobile device management solutions to force geofencing or SSID fencing by locking the device if it associates with an unapproved access point.
	B.3.1	Critical Digital Asset and Communications Protection Policy and Procedures	Use of access control lists (ACLs) to restrict access to media contents	Fortification	Map VLANs to security zones: Assign a unique VLAN + IP subnet for each security level - zone (for example Level 2-Cell A, Level 3-DMZ, Level 4-Business); no device ports are members of more than one zone.
				Fortification, Access Control	Access-port hardening: Set every user/PLC port to switchport mode access, force the correct VLAN. Ensure DTP is disabled (with configuration switchport nonegotiate), and shut unused ports to block rogue trunking or VLAN hopping.
				Fortification, Chokepoint	Trunk pruning & tagged-native: On uplinks, explicitly list allowed VLANs (such as: switchport trunk allowed vlan 20,30) and move the native VLAN to an unused ID that is always tagged.

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
	B.3.8	Trusted Path	Application of anti-malware solutions to scan media automatically	Fortification	Enable “scan removable drives” in Endpoint AV: On Windows, utilize Group Policy to push (or manually set) registry key settings enforcing Microsoft Defender Antivirus to scan removable devices. On Linux, run clamd to scan /media paths and set rules to scan when USB devices are mounted.
				Fortification, Chokepoint	Inspect files at network choke points: Use DLP appliances or secure web gateways to scan any SMB/HTTP transfers originating from a USB-mounted path. Block if malware detected
	B.3.12	Transmission of Security Parameters	Require read-only access for non-authorized users	Fortification	1. Windows Group Policy: Apply “Removable Disk: Deny write access” and “Allow read access” which can be applied by a security group that contains only non-authorized users. 2. Endpoint-security / Data Loss Prevention Platforms: These tools can be configured to limit access to USB storage devices to read only. 3. Linux mount namespace: The file /etc/fstab can be configured to limit user’s capability to mount devices and assign read/write access to specific users.
				Fortification, Access Control	Windows Defender Device Control: Create a Device Control XML that grants Write rights for all processes and sets the default rule to Read-Only.
	B.4.2	User Identification and Authentication	Require use of passwords or PINs on media devices	Fortification, Access Control	1. Mandate OS-level encrypted volumes: Require passphrases. On Windows, enable Bitlocker on all removable drives via GPO. On Linux, provision removable media with LUKS2 full-disk encryption. 2. Password/PIN complexity and rotation: Require 8 or greater than digit numeric PINs

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
					or 12 or greater than character alphanumeric passwords with no dictionary words. In Windows, this can be enforced via the same GPO/MDM policy used to mandate encryption. 3. Built-in user-supplied authentication Media: Hardware-encrypted USB sticks or SSDs with an on-device keypad or integrated smartcard. Require mandatory PIN before device can unlock.
	B.5.1	Removal of Unnecessary Services and Programs	Basic restrictions on media use, such as disabling USB ports	Fortification, Access Control	1. Disable ports in firmware: Enter BIOS navigate to Integrated Peripherals set USB Ports = Disabled (or disable only "External USB"). 2. Block USB mass-storage drivers: Within Windows, set registry via group policy or WDAC / Device Control policy (deny UBSTOR.*). In Linux modify /etc/modprobe.d to blacklist usb storage. 3. Endpoint security / DLP device-control policies: Depending on endpoint security tooling used, create a policy to block removable storage (or Read-Only) and push to all endpoint groups.
	C.1.4	Media Storage	Detailed procedures for storing media	N/A	Operational Control: N/A
	C.1.5	Media Transport	General guidelines for proper handling and transport of portable media	N/A	Operational Control: N/A
	C.10.2	Awareness Training	Basic awareness training for personnel on the risks of portable media	N/A	Operational Control: N/A

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
2	B.1.18	Insecure and Rogue Connections	Routine checks for unauthorized media devices and connections	N/A	Operational Control: N/A
	B.1.20	Proprietary Protocol Visibility	Implement alternative controls for proprietary protocols on portable devices	Fortification, Chokepoint	1. Encapsulate the proprietary traffic: Force applications on mobile devices to connect only through a mutual-TLS VPN that authenticates the device certificate and encrypts all packets, regardless of protocols. 2. Utilize Application containerization: Run proprietary client inside a mobile device management deployed workspace container. Configure containers to enforce its own VPN, clipboard controls, and data-at-rest encryption separate from user space 3. Segmentation using strict ACLs: Assign the device to a dedicated VLAN or segmented overlay that permits egress only to the single IP and Port used by the proxy or server. Set all else to default deny.
	B.1.22	Use of External Systems	Prohibit external systems from accessing CDAs in level 3 and 4	Chokepoint	1. Network segmentation: Place all level 3 and 4 CDAs in dedicated VLANs that terminate on a firewall. Never route traffic directly from external zones such as internet, vendor networks or corporate WiFi into these segments 2. Unidirectional gateways for outbound-only flows: Utilize data diodes when reporting to cloud services is necessary, deploying transmit-only TCP relays that physically prevent any return traffic to CDA network 3. Firewalls and ACL posture to “Default-deny”: On perimeter firewalls, configure explicit rules that will drop all inbound sessions whose source is outside the site boundary. Only allow outbound traffic from

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
					the CDA required for patch or log uploads to pass through a screened DMZ proxy.
	B.2.2	Auditable Events	Defining list of auditable events and frequency of auditing for each identified auditable event	Fortification	1. Build an “audit-event catalog” as code: Ensure comprehensive logging is enabled with each object containing a set list of details (such as event-name, description, source, log location, severity, owner, etc) 2. Automate evidence collection: Use SOAR playbooks or cron jobs that snapshot the relevant log indices, hash/sign the data, and attach it to the audit ticket; reviewer only needs to validate rather than hunt.
	B.3.6	Transmission Integrity	Implement cryptographic-hashing checks (SHA-256 before/after file transfer) for integrity assurance	Fortification	Standardized FIPS compliant secure hash cryptosystem may be used.
	C.1.2	Media Access	Encrypt portable media containing sensitive information during transport outside controlled areas	N/A	Operational Control: N/A
	C.1.6	Media Sanitization and Disposal	Procedures for labeling and securing media when disposed or no longer in use	N/A	Operational Control: N/A
	C.3.6	Security Functionality Verification	Logging of all portable media usage	N/A	Operational Control: N/A
3	B.3.9	Cryptographic Key Establishment and Management	Implement secure key management practices for PMMD encryption keys	Fortification	1. Generate strong, unique keys: Use a FIPS-validated random number generator (RNG) to create AES-256 data-encryption key, unique for every portable-media / mobile-device instance. 2. Enforce strong access controls: Gate key-management APIs behind

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
					MFA-protected RBAC, a privileged access workstation, and/or Just-in-Time elevation. Log all operations to a SIEM for monitoring capabilities. 3. Protect root material in hardware: Store the master key encryption key in a secure vault such as a inside a Level3 HSM, cloud KMS, or on-device TPM. Never export a key in cleartext.
	B.3.14	Mobile Code	Disabling access to PMMD by default, enabling only when necessary	Fortification	Block portable media interfaces by default: Use Windows GPO to deny all access to removable disks and the WDAC Device-Control default rule = block for USB Mass-Storage
	B.3.18	Session Authenticity	Implementation of secure file transfer protocols for data moving to/from portable media	Fortification	Enforce encrypted transport protocols: when staging removable drives allow only secure protocols such as SFTP/SCP, rsyc + SSH, FTPS (TLS 1.2/1.3), HTTPS with mutual TLS or SMB3.x encryption.
				Access Control	Automate integrity checks: Generate SHA-256/512 hashes and a signed manifest at source. Verify the hashes on ingest.
				Fortification, Chokepoint	1. Mandate encryption at rest: On portable media, use tools such as BitLocker To Go, VeraCrypt/LUKS2, or FIPS-validated hardware-encrypted USBs. Enforce devices mount read-only until the controller confirms AES-256 encryption is active. 2. Cross-domain guards or data diodes: If portable media must traverse high to low security levels, enforce antivirus, content disarm-and-reconstruct, manual releasability review, then release to encrypted media through a one-way link

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
				Fortification, Access Control	Secure staging workstations: Air-gapped PC with smart-card MFA, hardened SFTP client, and Group-Policy-enforced BitLocker. Users can only copy to vetted USBs under monitored conditions.
	B.3.20	Protection of Information at Rest	Mandatory encryption of all data on PMMD	Fortification	Policy-enforced removable-media encryption: On Windows, utilize GPO's to "Deny write access to removable drives not protected by BitLocker". On Linux create a udev rule that triggers cryptsetup luksFormat and block write if dm-crypt mapper is absent.
	B.4.5	Device Identification and Authentication	Controlled use of media with whitelisted devices and systems	Fortification	1. Enforce OS-level device allowlists: On Windows, utilize GPOs to restrict installations to only matching device IDs and WDAC Device Control to deny everything else. On Linux, use USBGuard rulesets to only allow media from specific IDs. 2. Block physical ports on non-transfer systems: Within the BIOS disable mountable media, deploy lockable port blockers, or board-level power cutoff for hosts that should never use portable media
				Access Control	1. Require hardware or full-disk encryption before whitelist: Utilize encryption at rest tools (such as BitLockerToGo, FileVault, LUKS2) to enforce mandatory user PIN/paswords and escrow keys centrally 2. Apply read/write permissions by role: Through AD security groups, utilize device control policies to grant read only for standard users.
	C.2.1	Specialized Cybersecurity Training	Specialized training for personnel on secure handling	N/A	Operational Control: N/A

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
			of PMMD for Zones assigned L3 and L4		
4	B.3.2	Application Partitioning and Security Function Isolation	Isolate security functions on PMMD to prevent cross-contamination between segments	Fortification	1. Dual-partition scheme: Configure small, signed “security utilities” partition (read-only), separate encrypted data partition. Configure the OS so that mounts only one scheme at a time based on context. 2. Dedicated security tokens: Keep authentication keys or patch files on FIPS-validated smart cards/HSM-backed USBs; never mix with general data storage. 3. Label & color-code media: red = security-only, blue = general; inventory system rejects mis-categorized devices at check-in/out.
				Access Control	Virtualization containers: Run scanning/patching tools from a bootable, immutable image (e.g., Ventoy with write-protected ISO) so no residue persists across segments.
				Fortification, Chokepoint	1. Logical access controls: Configure file-system ACLs and application whitelists restrict the security partition to security software hashes; non-security apps cannot read or write there 2. Cross-domain data guards: when data must transit between security and non-security segments, pass through a detonation/sanitization gateway that strips executables and validates signatures.
	B.5.4	Hardware Configuration	Disabling auto-run features on systems to prevent	Fortification, Access Control	Windows Group Policy: “Turn off AutoPlay” = Enabled, “NoDriveTypeAutoRun” registry set to 0xFF; enforced via Intune/SCCM baselines.

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
			unauthorized execution from media		Linux/macOS: disable udev or udisks auto-mount rules; set /etc/fstab noexec for /media; configure launchctl to block autorun.inf. EDR/WDAC execution control: policy denies file:///removable/* unless signed and whitelisted.
				Chokepoint, Access Control	Kiosk/ICS HMIs: boot in “shell replacement” mode; USB mounted read-only and without execution permissions.
	C.1.1	Media Protection Policy and Procedures	Strict media control policies, including authorization and tracking of media usage	N/A	Operational Control: N/A
	C.1.3	Media Labeling and Marking	Regular audits and inventories of portable media	N/A	Operational Control: N/A
	C.1.6	Media Sanitization and Disposal	Use of secure wipe tools to sanitize media before reuse	Fortification	1. Data wiping tools: Use NIST 800-88–compliant tools such as nwipe (Linux), diskpart clean all or cipher /w (Windows), sg_format --sanitize (SCSI). These can be scripted into imaging workflow. 2. Cryptographic erase for SSDs & FIPS drives: Issue ATA Secure Erase or NVMe format –ses=1 commands. When dealing with self-encrypting media, rotate the encryption key to render prior data unreadable in seconds. 3. Automated kiosk “wipe station”: This essentially works as a kiosk where portable media can be inserted, a barcode scan work order is given for tracking, and a tool runs multi-pass wipe or crypto-erase, ending in a printed tamper-proof certificate, as well as logging the result to SIEM. 4. Sanitization verification: Tools such as badblocks –wsv or hash-verify random

Level	Control #	Control Name	Implementation Goal	Defensive Strategy	Implementation Examples
					sectors can be running post-wipe. Ensure the job fails if residual data is detected."
	C.7	Defense-in-Depth Defensive Security Architecture	Implementation of hardware-based write protection for media	Fortification	1. Forensic write-blockers – inline SATA/USB write-block bridges for laptops or kiosks that must ingest third-party drives. 2. Endpoint device-control enforcement – Endpoint detection response (EDR) policy sets external media to read-only unless the VID/PID matches an approved write-enabled list.
	C.11.7	Configuration Settings	Continuous monitoring and logging of media access and use	N/A	Operational Control: N/A
	C.12.1	System and Services Acquisition Policy and Procedures	Implementation of hardware-based write protection for media	Fortification, Chokepoint	1. Drives with physical read-only switch: Mandate USB sticks / SD cards that expose a mechanical lock. Draft a policy that forbids use of media lacking the switch. 2. UEFI/BIOS USB write-protect – some chipsets support port-level write disable. Access to the BIOS can be locked with admin password to prevent tampering.
				Fortification, Access Control	Keypad or biometric-auth encrypted drives: Utilizes encrypted portable media drives that offer a “read-only session” mode selectable at unlock time (ex., Apricorn, IronKey).

6. CONCLUSION

AR designers can consider cybersecurity from the start of the design process to avoid the wrap-around security measures often applied for the existing fleet. Designers are considering effective cybersecurity as a fundamental part of the design basis of the reactor. This provides an opportunity to potentially reduce costs and effort in establishing effective cybersecurity programs via integration of cybersecurity analysis with the design process.

This report presents the DCSA design for an SFR. This analysis approach is consistent with the TCA detailed in the U.S. NRC draft regulatory guide "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53" (DG-5075). The TCA approach presented in DG-5075 leverages the SeBD features of the plant as the foundation of cybersecurity analysis. A DCSA designed as part of the TCA approach is designed to deny the adversary access to the plant functions needed to cause an accident sequence that is unmitigated by the plant's physical design.

This report was written to demonstrate DCSA design approaches and to provide a template DCSA design for an SFR to be available for industry use. It is important to note that the DCSA design template and cybersecurity controls provided in this report are intended to serve as starting points for AR designers and are not prescriptive. Further optimization of the DCSA design and cybersecurity controls may be valuable given the unique design and performance requirements of the plant.

This report analyzed the technical and operational controls presented in U.S. NRC RG 5.71 and aligned them with the defensive strategies of fortification, chokepoints, and access control. The goal of the control was identified and examples of technical implementations of the controls were provided. These controls examples and the relationships between defensive strategies provide a useful basis for the development of a cybersecurity plan.

The application of technical controls to specific systems in addition to a base level of security requirements provided by the security level is likely to result in additional DCSA design improvements via the DG-5075 approach. Potential DCSA design improvements include the merging of zones and reassignment of lower security levels to certain zones as appropriate to the unique plant design.

This page left blank

REFERENCES

[1] International Atomic Energy Agency, "NSS 17-T: Computer Security Techniques for Nuclear Facilities," IAEA, Vienna, Austria, 2021.

[2] U.S. Nuclear Regulatory Commission, "Establishing Cybersecurity Programs for Commerical Nuclear Plants Licensed Under 10 CFR Part 53," U.S. NRC, Bethesda, MD, 2024.

[3] J. Redd, K. Fleming and A. Afzali, "SSC Safety Classification and Performance Requirements for Advanced Non-LWRs," in *2018 Probablistic Safety Assessment and Management*, Los Angeles, CA, 2018.

[4] Idaho National Laboratory, "Next Generation Nuclear Plant Structures, Systems, and Components Safety Classification White Paper," INL, Idaho Falls, ID, 2010.

[5] A. Campbell, "Non-Safety-Related with Special Treatment - Digital Considerations," in *U.S. Nuclear Regulatory Commision Regulatory Information Conference*, Bethesda, MD, 2024.

[6] L. T. Maccarone, M. T. Rowland, R. J. Brulles and A. S. Hahn, "Design of Defensive Cybersecurity Architectures for High Temperature, Gas-Cooled Reactors," Sandia National Laboratories, Albuquerque, NM, 2024.

[7] U.S. Nuclear Regulatory Commission, "Regulatory Guide 5.71 - Cyber Security Programs for Nuclear Facilities," Rockville, MD, 2010.

[8] U.S. Nuclear Regulatory Commission, "Part 53 – Risk Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors," 11 June 2024. [Online]. Available: https://www.nrc.gov/reactors/new-reactors/advanced/modernizing/rulemaking/part-53.html. [Accessed 2 August 2024].

[9] U.S. Nuclear Regulatory Commission, "Proposed Rule: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors," U.S. NRC, Bethesda, MD, 2023.

[10] L. T. Maccarone and M. T. Rowland, "The Sliding Scale of Cybersecurity Applied to the Cybersecurity Analysis of Advanced Reactors," in *American Nuclear Society 13th Nuclear Plant Instrumentation, Control, & Human-Machine Interface Technologies*, Knoxville, TN, 2023.

[11] J. Jauntirans, I. Garcia and M. Rowland, "U.S.A. Regulatory Efforts for Cyber Security of Small Modular Reactors/Advanced Reactors," in *IAEA Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors*, Vienna, Austria, 2021.

[12] J. James, J. Mohmand, L. Maccarone, D. R. Sandoval, A. Haddad, M. T. Rowland and A. J. Clark, "Consequence Modeling and Simulation of Hazardous Events for Advanced Reactors," Sandia National Laboratories, Albuquerque, NM, 2023.

[13] N. G. Leveson and J. P. Thomas, "STPA Handbook," 2018.

[14] L. Maccarone, A. Hahn and M. Rowland, "System-Level Design Analysis for Advanced Reactor Cybersecurity," Sandia National Laboratories, Albuquerque, NM, 2023.

[15] A. Hahn, L. Maccarone and M. Rowland, "Advanced Reactor Cyber Analysis and Development Environment (ARCADE) for System-Level Design Analysis," Sandia National Laboratories, Albuquerque, NM, 2023.

[16] A. Hahn, M. Higgins, L. Maccarone, M. Rowland and R. Valme, "Lessons Learned from Advanced Reactor Cyber Analysis and Development Environment (ARCADE)," in *NPIC&HMIT 2023*, Knoxville, TN, 2023.

[17] A. Hahn, L. Maccarone and M. Rowland, "Simulation Based Analytical Approaches to Cyber Risk Mitigation in Advanced Nuclear Reactors," in *2024 ANS Annual Conference*, Las Vegas, NV, 2024.

[18] L. Maccarone, A. Hahn and M. Rowland, "Design of Defensive Cyber Security Architectures Using Event Trees," in *2024 ANS Annual Conference*, Las Vegas, NV, 2024.

[19] World Nuclear Association, "Design Maturity and Regulatory Expectations for Small Modular Reactors," London, UK, 2021.

[20] L. Maccarone, S. Eggers, M. Rowland and J. deCastro, "Advances in Cybersecurity-by-Design Leveraging Complementary Frameworks of CIE and TCA," in *INMM Annual Meeting*, Washington, D.C., 2025.

[21] International Atomic Energy Agency, "IAEA Nuclear Safety and Security Glossary," IAEA, Vienna, Austria, 2022.

[22] K. Biba, "Integrity Considerations for Secure Computer Systems," The Mitre Corporation, Bedford, MA, 1975.

[23] G. Landine, "M-51 Defensive Computer Security Architectures (DCSA)," in *Protecting Computer Based Systems in Nuclear Security Regimes*, Vienna, Austria, 2018.

[24] L. Maccarone, J. deCastro and M. Rowland, "Implementing Complementary Defensive Strategies in Defensive Cybersecurity Architectures," in *American Nuclear Society 14th Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT)*, Chicago, IL, 2025.

[25] Nuclear Energy Institute, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," NEI, Washington, D.C., 2019.

[26] NSA, "NSA's Top Ten Cybersecurity Mitigation Strategies," March 2018. [Online]. Available: https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf.

[27] S. C. Fitch and M. Muckin, "Defendable Architectures: Achieving Cyber Security by Designing Intelligence Driven Defense," Lockheed Martin Corporation, 2019.

[28] A. A. Mughal, "The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection," *International Journal of Intelligent Automation and Computing,* vol. 1, no. 1, 2018.

[29] EPRI, "Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation, Revision 1," EPRI, 2018.

[30] K. S. Long, "Cybersecurity Network Monitoring Challenge in Commercial Service Provider Clouds," MITRE Corporation, Annapolis Junction, MD, USA, 2021.

[31] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communications Review,* vol. 34, no. 2, 2004.

[32] XM Cyber, "Navigating the Paths of Risk: The State of Exposure Management in 2024," Cyentia Institute, 2024.

[33] W. Baker, "Visualizing the Value of Attack Path Choke Points for Prioritization," Cyentia Institute, 25 May 2023. [Online]. Available: https://www.cyentia.com/value-of-choke-points/#:~:text=Choke%20Points%3A%20From%20Concept%20to%20Data&text=About%202%25%20(~200)%20of,that%20distinction%20in%20a%20moment)..

[34] ORS, "Cybersecurity Best Practices for Users of Radioactive Sources," ORS, 2022.

[35] D. Kuipers and M. Fabro, "Control Systems Cyber Security: Defense in Depth Strategies," Idaho National Laboratory, Idaho Falls, 2006.

[36] A. Valenzano, "Industrial Cybersecurity: Improving Security Through Access Control Policy Models," *IEEE Industrial Electronics Magazine,* vol. 8, no. 2, June 2014.

[37] B. Leander, A. Čaušević, H. Hansson and T. Lindström, "Toward an Ideal Access Control Strategy for Industry 4.0 Manufacturing System," *IEEE Access,* vol. 9, pp. 114037-114050, 2021.

[38] Fortinet, "Deception Technology Definition," Fortinet, [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-deception-technology#:~:text=Threat%20deception%20technology%20works%20by,not%20damage%20business%2Dcritical%20systems..

[39] J. Pawlick, E. Colbert and Q. Zhu, "A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy," *ACM Computing Surveys (CSUR),* pp. 1-28, 30 August 2019.

[40] L. Zhang and V. L. L. Thing, "Three Decades of Deception Techniques in Active Cyber Defense - Retrospect and Outlook," *Computers and Security,* vol. 106, 2021.

[41] H. Ohshima and S. Kubo, "Sodium-Cooled Fast Reactor," in *Handbook of Generation IV Nuclear Reactors*, I. Pioro, Ed., Cambridge, UK, Woodhead Publishing, 2023, pp. 1-1.

[42] R. Michal, "Fifty Years Ago in December: Atomic Reactor EBR-I Produced First Electricity," *Nuclear News,* pp. 28-29, November 2001.

[43] K. Henry and A. Edwards, "The Operation of the Dourneay Fast Reactor," in *Proceedings of the London Conference on Fast Breeder Reactors Organized by the British Nuclear Energy Society*, London, UK, 1966.

[44] U.S. Nuclear Regulatory Commission, "Fermi - Unit 1," U.S. NRC, 12 July 2024. [Online]. Available: https://www.nrc.gov/info-finder/decommissioning/power-reactor/enrico-fermi-atomic-power-plant-unit-1.html. [Accessed 2 September 2025].

[45] C. Westfall, "Vision and Reality: The EBR-II Story," *Nuclear News,* pp. 25-32, February 2004.

[46] M. Schneider, "Fast Breeder Reactors in France," in *Fast Breeder Reactor Programs: History and Status*, Princeton, NJ, International Panel on Fissile Materials, 2010, pp. 17-35.

[47] J. Arterburn, G. Billuris and G. Kruger, "SEFOR Operating Experience," American Society of Mechanical Engineers, New York, NY, 1971.

[48] A. Izhutov, A. Burukin, Y. Krasheninnikov, I. Zhemkov, A. Varivtcev and Y. Naboishchikov, "BOR-60 Reactor Operational Experience and Experimental Capabilities," in *IAEA International Conference on Fast Reactors and Related Fuel Cycles*, Yekaterinburg, Russia, 2017.

[49] J. Guidez, P. Chaucheprat, B. Fontaine, E. Brunon, L. Martin, D. Warin, A. Zaetta and F. Sudreau, "Phenix: The Irradiation Program for Transmutation Experiments," in *NEA Actinide and Fission Product Partitioning & Transmutation, Eighth Information Exchange Meeting*, Las Vegas, NV, 2004.

[50] V. Troyanov and A. Kamaev, "Evolution of Fast Reactors: The Role of a BN-350 Reactor," *Atomic Energy,* vol. 136, no. 5-6, pp. 222-232, 2024.

[51] S. Jensen and P. Olgaard, "Description of the Prototype Fast Reactor at Dounreay," Riso National Laboratory, Roskilde, Denmark, 1995.

[52] W. Marth, H. Andrae, K. Busch, E. Guthmann and G. Hendl, "KNK II - Construction and Aseismic Design," in *International Symposium on Design, Construction, and Operating Experience of Demosntration Liquid Metal Fast Breeder Reactors*, Bologna, Italy, 1978.

[53] T. Ashida, Y. Gondai and e. al., "Experimental Reactor Joyo," *Sodium-Cooled Fast Reactors: JSME Series in Thermal and Nuclear Power Generation,* vol. 3, pp. 9-85, 2022.

[54] N. Oshkanov, O. Saraev, M. Bakanov, P. Govorov, O. Potapov, Y. Ashurko, V. Poplavskii, B. Vasil'ev, Y. Kamanin and V. Ershov, "30 Years of Experience in Operating the BN-600 Sodium-Cooled Fast Reactor," *Atomic Energy,* vol. 108, no. 4, pp. 234-239, 2010.

[55] C. C.P., "A Summary Description of the Fast Flux Test Facility," Hanford Engineering Development Laboratory, Richland, WA, 1980.

[56] G. Srinivasan, K. Suresh Kumar, B. Ragendran and P. Ramalingam, "The Fast Breeder Test Reactor - Design and Operating Experiences," *Nuclear Engineering and Design,* vol. 236, pp. 796-811, 2006.

[57] Compagnie d'Ingenierie pour les Reacteurs a Sodium (CIRNA), "Super Phenix Breeder Reactor," Science Applications, Inc., Rolling Meadows, IL, 1976.

[58] G. Karsten, "Between Science and Technology - Results and Reflections on the Status of Fuel Element Development for Fast Reactors," Kernforschungszentrum Karlsruhe, Karlsruhe, Germany, 1973.

[59] T. Hazama, "Prototype Reactor Monju," *Sodium-Cooled Fast Reactors: JSME Series in Thermal and Nuclear Power Generation,* vol. 3, pp. 87-161, 2022.

[60] D. Zhang, Y. Yang and J. Zhao, "Main Technical Innovation and Engineering Experience of China Experimental Fast Reactor," *Atomic Energy Science and Technology,* vol. 54, pp. 194-198, 2020.

[61] V. Popllavskii, A. Chebeskov and V. Matveev, "BN-800 as a New Stage in the Development of Fast Sodium-Cooled Reactors," *Atomic Energy,* vol. 96, no. 6, pp. 386-90, 2004.

[62] S. Chetal, V. Balasubramaniyan, P. Chellapandi, P. Mohanakrishnan, P. Puthiyavinayagam, C. Pillai, S. Raghupathy, T. Shanmugham and C. Sivathanu Pillai, "The Design of the Prototype Fast Breeder Reactor," *Nuclear Engineering and Design,* vol. 236, no. 7-8, pp. 852-860, 2006.

[63] ARC Clean Technology, "ARC-100 Technical Summary," ARC Clean Technology, Saint John, Canada, 2023.

[64] Oklo, "Principal Design Criteria for the Aurora Powerhouse," Oklo, Santa Clara, CA, 2025.

[65] Oklo, "Final Safety Analysis Report," U.S. NRC, Rockville, MD, 2020.

[66] TerraPower, LLC, "Regulatory Management of Natrium Nuclear Island and Energy Island Design Interfaces," U.S. NRC, Rockville, MD, 2022.

[67] TerraPower, LLC, "Instrumentation and Control Architecture and Design Basis Topical Report," U.S. NRC, Rockville, MD, 2024.

[68] H. Trellue, "Safety and Neutronics: A Comparison of MOX vs UO2 Fuel," *Progress in Nuclear Energy,* vol. 48, pp. 135-145, 2006.

[69] World Nuclear Association, "Mixed Oxide (MOX) Fuel," WNA, 10 October 2017. [Online]. Available: https://world-nuclear.org/information-library/nuclear-fuel-cycle/fuel-recycling/mixed-oxide-fuel-mox. [Accessed 1 August 2025].

[70] D. Blanchet, L. Buiron, N. Stauff, T. Kim and T. Taiwo, "Sodium Fast Reactor Core Definitions," Nuclear Energy Agency, Boulogne-Billancourt, France, 2011.

[71] R. Nakai and D. Hahn, "Sodium-Cooled Fast Reactor (SFR) Risk and Safety Assessment White Paper," Generation IV International Forum, 2016.

[72] T. Sofu, "Fast Reactor Fuels," in *Fast Reactor Technology Training*, Rockville, MD, 2019.

[73] H. Ohshima and S. Kubo, "Sodium-Cooled Fast Reactors (SFRs)," in *Handbook of Generation IV Nuclear Reactors*, Cambridge, MA, Woodhead Publishing, 2023, pp. 173-194.

[74] TerraPower, Inc., "Natrium Topical Report: Fuel and Control Assembly Qualification," U.S. NRC, Rockville, MD, 2023.

[75] U.S. Department of Energy, Office of Nuclear Energy, "Sodium-Cooled Fast Reactor (SFR) Technology and Safety Overview," Washington, DC, 2015.

[76] Generation IV International Forum, "2019 Annual Report," GIF, 2019.

[77] K. Kim, J. Kim and C. Park, "Conceptual Designs and Characteristic of the Fuel Handling and Transfer System for 150 MWe PGSFR and 1400 MWe SFR Burner Reactor," *Nuclear Engineering and Technology,* vol. 54, pp. 4125-4133, 2022.

[78] X-energy, "Xe-100 Spent Fuel Management Licensing Approach White Paper," U.S. Nuclear Regulatory Commission, Bethesda, MD, 2023.

[79] H. Guo, L. Buiron, P. Sciora and T. Kooyman, "Optimization of Reactivity Control in a Small Modular Sodium-Cooled Fast Reactor," *Nuclear Engineering and Technology,* vol. 52, pp. 1367-1379, 2020.

[80] A. Maioli, H. Detar, R. Haessler, B. Friedman, C. Belovesick, J. Scobel, S. Kinna, M. Smith, J. van Wyk and K. Fleming, "Westinghouse eVinci Micro-Reactor Licensing Modernization Project Demonstration," Southern Company, Atlanta, GA, 2019.

[81] MARVEL RCS Development Team, "MARVEL Technology Review: Reactivity Control System (RCS)," U.S. DOE, Washington, D.C., 2022.

[82] H. Lee, T. Han, H. Lim and J. Noh, "An Accident-Tolerant Control Drum System for a Small Space Reactor," *Annals of Nuclear Energy,* vol. 79, pp. 143-151, 2015.

[83] P. Venter, "Pebble Bed HTGR Thermal-Fluid Behavior," in *HTGR Technology Course for the Nuclear Regulatory Commission*, Idaho Falls, ID, 2010.

[84] GE Hitachi Nuclear Energy, "Demonstration of Sodium-Cooled Fast Reactor GE-PRISM," GE Hitachi, Wilmington, NC, 2016.

[85] T. Sofu, "SFR Technology Overview," in *Fast Reactor Technology Training*, Rockville, MD, 2019.

[86] W. Zhihua, "Evaluation of Neutron Nuclear Data of Sodium," *Communication of Nuclear Data Progress,* vol. 6, pp. 17-23, 1992.

[87] J. Ruggieri, L. Ren, J. Glatz, I. Ashurko, H. Hayafune, Y. Kim and R. Hill, "Sodium-Cooled Fast Reactor (SFR) System Safety Assessment," GIF, Paris, France, 2017.

[88] T. Sofu, "Fast Reactor Safety," in *Fast Reactor Technology Training*, Rockville, MD, 2019.

[89] U.S. Department of Energy Nuclear Energy Research Advisory Committee and the Generation IV International Forum, "A Technology Roadmap for Generation IV Nuclear Energy Systems," U.S. DOE and GIF, Washington, D.C., 2002.

[90] Generation IV International Forum, "Sodium Fast Reactor," GIF, [Online]. Available: https://www.gen-4.org/generation-iv-criteria-and-technologies/sodium-fast-reactor-sfr. [Accessed 2 August 2025].

[91] Y. Jeong, M. Weathered, L. Ibarra, D. O'Grady, A. Brunett, R. Thomas and R. Hu, "Experimental Validation of Thermal Hydraulic Behavior in Sodium Fast Reactors (SFR) with the Thermal Hydraulic Experimental Test Article (THETA)," Argonne National Laboratory, Lemont, IL, 2024.

[92] World Nuclear News, "Oklo and Argonne Complete Second THETA Testing Campaign," WNN, 14 March 2024. [Online]. Available: https://www.world-nuclear-news.org/Articles/Oklo-and-Argonne-complete-second-THETA-testing-cam. [Accessed 3 August 2025].

[93] D. Grabaskas, "Operational Considerations," in *Fast Reactor Technology Training*, Rockville, MD, 2019.

[94] F. Kozlov, A. Sorokin and M. Konovalov, "Sodium Purification Systems for NPP with Fast Reactors (Retrospective and Perspective Views)," *Nuclear Energy and Technology,* vol. 2, pp. 5-13, 2016.

[95] J. Courouau, F. Masse, G. Rodriguez, C. Latge and B. Redon, "The Various Sodium Purification Techniques," in *Proceedings of the Technical Committee Meeting on Sodium Removal and Disposal from LMFRs in Normal Operation and in the Framework of Decommissioning*, Aix-en-Provence, France, 1997.

[96] D. Hanson, "Helium Inventory and Purification System," in *HTGR Technology Course for the Nuclear Regulatory Commission*, Idaho Falls, ID, 2010.

[97] V. Ivanenko and V. Zybin, "Fast Reactor Sodium Systems Operation Experience and "Leak-Before-Break" Criterion," in *Technical Committee Meeting on Evaluation of Radioactive Materials Release and Sodium Fires in Fast Reactors*, Oarai, Japan, 1996.

[98] Y. Bagdasarov, A. Vinogradov, A. Drobyshev, A. Kamaev, V. Poplavskii, I. Yagodkin, D. Kardash and I. Pakhomov, "Sodium Fires and Fast Reactor Safety," *Atomic Energy,* vol. 119, no. 1, pp. 25-31, 2015.

[99] D. Lisowski, Q. Lv, B. Alexandreanu, Y. Chen, R. Hu and T. Sofu, "Technical Letter Report: An Overview of Non-LWR Vessel Cooling Systems for Passive Decay Heat Removal," U.S. NRC, Rockville, MD, 2021.

[100] W. Li, J. Liu, Y. Bai, Y. Li, M. Jin, T. Li and C. Li, "Design and Analysis of a Direct Reactor Auxiliary Cooling System for a Pool-Type Small Modular Lead-Based Reactor," *Annals of Nuclear Energy,* vol. 207, no. 110678, pp. 1-9, 2024.

[101] M. Lee, J. Hwang, K. Choi, D. Jerng and I. Bang, "Application of Two Different Similarity Laws for the RVACS Design," *Nuclear Engineering and Technology,* vol. 54, pp. 4759-4775, 2022.

[102] TerraPower, Inc., "The Next Generation of Power is Here - The Natrium Reactor and Energy Storage System," 2024. [Online]. Available: https://www.terrapower.com/downloads/Natrium_Technology.pdf. [Accessed 2 August 2025].

[103] E. Mulder, "X-energy," in *NRC-DOE Workshop on Advanced Non-LWRs*, Bethesda, MD, 2015.

[104] L. Lommers, "Steam Cycle Power Conversion System," in *HTGR Technology Course for the Nuclear Regulatory Commission*, Idaho Falls, ID, 2010.

[105] J. Lamarsh and A. Baratta, Introduction to Nuclear Engineering, Upper Saddle River, NJ: Prentice Hall, 2001.

[106] R. Knief, Nuclear Engineering: Theory and Technology of Commerical Nuclear Power, La Grange Park, IL: American Nuclear Society, 2008.

[107] N. Todreas and M. Kazimi, Nuclear System Volume I: Thermal Hydraulic Fundamentals, Boca Raton, FL: CRC Press, 2011.

[108] C. Borgnakke and R. Sonntag, Fundamentals of Thermodynamics, Hoboken, NJ: John Wiley & Sons, 2013.

[109] U.S. Department of Energy, "SCO2 Power Cycles," US DOE, [Online]. Available: https://www.energy.gov/sco2-power-cycles. [Accessed 2 September 2025].

[110] G. Musgrove and S. Wright, "Introduction and Background," in *Fundamentals and Applications of Supercritical Carbon Dioxide (sCO2) Based Power Cycles*, K. Brun, P. Friedman and R. Dennis, Eds., Cambridge, MA, Woodhead Publishing, 2017, pp. 1-22.

[111] S. Wright and W. Scammell, "Economics," in *Fundamentals and Applications of Supercritical Carbon Dioxide (sCO2) Based Power Cycles*, K. Brun, P. Friedman and R. Dennis, Eds., Cambridge, MA, Woodhead Publishing, 2017, pp. 127-146.

[112] P. Wu, Y. Ma, C. Gao, W. Liu, J. Shan, Y. Huang, J. Wang, D. Zhang and X. Ran, "A Review of Research and Development of Supercritical Carbon Dioxide Brayton Cycle Technology in Nuclear Engineering Applications," *Nuclear Engineering and Design,* vol. 368, no. 110767, pp. 1-23, 2020.

[113] Y. Ahn, S. Bae, M. Kim, S. Cho, S. Baik, J. Lee and J. Cha, "Review of Supercritical CO2 Power Cycle Technology and Current Status of Research and Development," *Nuclear Engineering and Technology,* vol. 47, pp. 647-661, 2015.

[114] L. Maccarone, A. Hahn, R. Valme, M. Rowland, A. Kapuria, Y. Zhang and D. Cole, "Advanced Reactor Cyber Analysis and Development Environment (ARCADE) for University Research," in *TRTR Annual Meeting*, College Park, MD, 2023.

[115] U.S. Department of Energy, "Thermal Energy Storage," U.S. DOE, [Online]. Available: https://www.energy.gov/eere/buildings/thermal-energy-storage. [Accessed 2 September 2025].

[116] M. Faizan, A. Alkaabi, B. Nie and I. Afgan, "Thermal Energy Storage Integration with Nuclear Power: A Critical Review," *Journal of Energy Storage,* vol. 96, no. 112577, pp. 1-16, 2024.

[117] TerraPower, Inc., "Energy Island Decoupling Strategy," U.S. NRC, Rockville, MD, 2022.

[118] TerraPower, Inc,, "Natrium Decoupling Strategy," U.S. NRC, Rockville, MD, 2021.

[119] U.S. Nuclear Regulatory Commission, "Exemption Request for Construction of Energy Island for Kemmerer Unit 1," 7 May 2025. [Online]. Available: https://www.nrc.gov/docs/ML2511/ML25119A329.html. [Accessed 23 August 2025].

[120] X-energy, "Plant Control and Data Acquisition White Paper," U.S. Nuclear Regulatory Commission, Bethesda, MD, 2023.

[121] U.S. Nuclear Regulatory Commission, "10 CFR Part 50, Appendix A,Criterion 20: Protection System Functions," U.S. Nuclear Regulatory Commission, Bethesda, MD, 1971.

[122] R. Stattel and D. Taneja, "U.S. Nuclear Regulatory Commission Staff Safety Evaluation for Topical Report 2016-RPC003-TR-001 RadICS Safety System Digital Platform," U.S. NRC, Rockville, MD, 2016.

[123] IEEE Standards Association, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (IEEE Std 603-2018)," IEEE, New York, NY, 2018.

[124] U.S. Nuclear Regulatory Commission, "10 CFR Part 50, Appendix A,Criterion 21: Protection System Reliability and Testability," U.S. Nuclear Regulatory Commission, Bethesda, MD, 1971.

[125] U.S. Nuclear Regulatory Commission, "10 CFR Part 50, Appendix A,Criterion 22: Protection System Independence," U.S. Nuclear Regulatory Commission, Bethesda, MD, 1971.

[126] Westinghouse, "Section 12.1: Reactor Protection System," in *Westinghouse Technology Systems Manual*, Bethesda, MD, U.S. Nuclear Regulatory Commission, 2016.

[127] G. Simmons, "Symmetric and Asymmetric Encryption," *Computing Surveys,* vol. 11, no. 4, pp. 305-330, 1979.

[128] S. Hachana, F. Cuppens and N. Cuppens-Boulahia, "Towards a New Generation of Industrial Firewalls: Operational-Process Aware Filtering," in *14th Annual Conference on Privacy, Security, and Trust (PST)*, Auckland, New Zealand, 2016.

[129] T. Kampa, C. Muller and D. Grossman, "Interlocking IT/OT Security for Edge Cloud-Enabled Manufacturing," *Ad Hoc Networks,* vol. 154, no. 103384, pp. 1-11, 2024.

[130] M. Garcia, The Design and Evaluation of Physical Protection Systems, Burlington, MA: Butterworth-Heinemann, 2008.

[131] L. Maccarone, A. Hahn, B. Liu and F. Oppel, "Defensive Cybersecurity Design Using Force-on-Force Cyber-Physical Modeling," Sandia National Laboratories, Albuquerque, NM, 2025.

[132] B. Triplett, E. Loewen and B. Dooies, "PRISM: A Competitive Small Modular Sodium-Cooled Reactor," *Nuclear Technology,* vol. 178, pp. 186-200, 2012.

APPENDIX A. SFR FUNDAMENTAL SENSORS AND ACTUATORS

This appendix contains the tables of fundamental sensors and actuators necessary for operation of the SFR systems described in Section 3. In many cases, there is a diverse set of devices that could be implemented to achieve the required function. For generalizability of these results and to avoid prescriptive engineering implementations, the actuators and sensors are described in terms of their subfunctions to be performed, rather than describing specific technologies to be implemented.

Table XI. FHS Sensors

Sensor ID	Sensor Purpose
FHS.S.1	Measures position of fuel assembly manipulator (loading/unloading)
FHS.S.2	Measures position of fuel assembly manipulator (in-vessel storage)
FHS.S.3	Fuel assembly proximity sensors

Table XII. FHS Actuators

Actuator ID	Actuator Purpose
FHS.A.1	Loads fuel assemblies into reactor core
FHS.A.2	Unloads fuel assemblies from the reactor core
FHS.A.3	Moves fuel assemblies from reactor core to in-vessel storage
FHS.A.4	Moves fuel assemblies from in-vessel storage to SFSS

Table XIII. SFSS Sensors

Sensor ID	Sensor Purpose
SFSS.S.1	Measures radiation levels
SFSS.S.2	Measures fuel cask temperature

Table XIV. SFSS Actuators

Actuator ID	Actuator Purpose
SFSS.A.1	Manipulate position of spent fuel storage cask

Table XV. RCS Sensors

Sensor ID	Sensor Purpose
RCS.S.1-6	Measures control rod position
RCS.S.7-12	Measures position of control rod release actuator
RCS.S.13	Measures neutron flux across core
RCS.S.14	Measures hot leg temperature
RCS.S.15	Measures cold leg temperature
RCS.S.16	Measures sodium flow rate

Table XVI. RCS Actuators

Actuator ID	Actuator Purpose
RCS.A.1-6	Manipulates position of control rods
RCS.A.7-12	Releases control rods

Table XVII. RSS Sensors

Sensor ID	Sensor Purpose
RSS.S.1-3	Measures reserve shutdown rod position
RSS.S.4-6	Measures position of reserve shutdown rod release actuator

Table XVIII. RSS Actuators

Actuator ID	Actuator Purpose
RSS.A.1-3	Releases reserve shutdown rods

Table XIX. PHTS Sensors

Sensor ID	Sensor Purpose
PHTS.S.1	Measures sodium temperature at reactor core inlet (cold plenum)
PHTS.S.2	Measures sodium temperature at reactor core outlet (hot plenum)
PHTS.S.3	Measures sodium flow rate
PHTS.S.4-7	Measures speed of primary sodium pumps
PHTS.S.8-11	Measures vibration of sodium pumps

Table XX. PHTS Actuators

Actuator ID	Actuator Purpose
PHTS.A.1-4	Primary sodium pumps

Table XXI. IHTS Sensors

Sensor ID	Sensor Purpose
IHTS.S.1	Measures sodium temperature at heat exchanger inlet
IHTS.S.2	Measures sodium temperature at heat exchanger outlet
IHTS.S.3	Measures sodium flow rate
IHTS.S.4-5	Measures speed of sodium pumps
IHTS.S.6-7	Measures vibration of sodium pumps

Table XXII. IHTS Actuators

Actuator ID	Actuator Purpose
IHTS.A.1-2	Secondary sodium pumps

Table XXIII. SPS Sensors

Sensor ID	Sensor Purpose
SPS.S.1	Measures chemical contaminants in sodium
SPS.S.2	Measures radionuclide contaminants in sodium
SPS.S.3	Measures cold trap sodium pump speed
SPS.S.4	Measures cold trap sodium pump vibration
SPS.S.5	Measures cesium trap sodium pump speed
SPS.S.6	Measures cesium trap sodium pump vibration
SPS.S.7	Measures sodium temperature at cold trap
SPS.S.8	Measures wall temperature in cold trap
SPS.S.9	Measures differential pressure across cold trap
SPS.S.10	Measures sodium flow rate through cold trap
SPS.S.11	Measures sodium level in cold trap
SPS.S.12	Measures sodium level in cold trap drain tanks
SPS.S.13	Measures sodium temperature at cesium trap
SPS.S.14	Measures differential pressure across cesium trap
SPS.S.15	Measures sodium flow rate through cesium trap

Table XXIV. SPS Actuators

Actuator ID	Actuator Purpose
SPS.A.1	Control sodium pathway through cold trap
SPS.A.2	Control sodium pathway through cesium trap
SPS.A.3	Cold trap sodium pump
SPS.A.4	Cesium trap sodium pump
SPS.A.5	Cold trap cooling system
SPS.A.6	Heaters on cold trap
SPS.A.7	Heaters on cesium trap

Table XXV. SLM Sensors

Sensor ID	Sensor Purpose
SLM.S.1	Sodium leak detectors
SLM.S.2	Measures temperatures in areas where sodium may leak
SLM.S.3	Smoke detectors
SLM.S.4	Measures sodium pressure
SLM.S.5	Measures cover gas composition

Table XXVI. SLM Actuators

Actuator ID	Actuator Purpose
SLM.A.1	Sodium isolation valves in PHTS
SLM.A.2	Sodium isolation valves in IHTS
SLM.A.3	Sodium drain valves
SLM.A.4	Sodium cooling system actuators

Table XXVII. SFP Sensors

Sensor ID	Sensor Purpose
SFP.S.1	Flame detectors
SFP.S.2	Measures temperatures in areas where sodium may leak
SFP.S.3	Smoke detectors
SFP.S.4	Gas composition sensors
SFP.S.5	Measures pressure in areas where sodium may leak

Table XXVIII. SFP Actuators

Actuator ID	Actuator Purpose
SFP.A.1	Sodium isolation valves in PHTS
SFP.A.2	Sodium isolation valves in IHTS
SFP.A.3	Inert gas injection valves
SFP.A.4	Ventilation dampers
SFP.A.5	Interlock actuators

Table XXIX. CGS Sensors

Sensor ID	Sensor Purpose
CGS.S.1	Measures gas pressure
CGS.S.2	Measures gas temperature
CGS.S.3	Measures gas oxygen content
CGS.S.4	Measures gas humidity
CGS.S.5	Measures gas isolation valve position
CGS.S.6	Measures gas purge valve position

Table XXX. CGS Actuators

Actuator ID	Actuator Purpose
CGS.A.1	Control gas supply pathway
CGS.A.2	Gas isolation valve
CGS.A.3	Gas purge valve
CGS.A.4	Gas pressure regulator

Table XXXI. DRACS Sensors

Sensor ID	Sensor Purpose
DRACS.S.1-3	Measures temperature of air at inlet
DRACS.S.4-6	Measures temperature of air at outlet
DRACS.S.7-9	Measures air flow rate
DRACS.S.10-12	Measures cold-side sodium temperature
DRACS.S.13-15	Measures hot-side sodium temperature
DRACS.S.16-18	Measures sodium flow rate
DRACS.S.19-21	Natural draft heat exchanger air fan speed

Table XXXII. DRACS Actuators

Actuator ID	Actuator Purpose
DRACS.A.1-3	Natural draft heat exchanger air fan

Table XXXIII. RVACS Sensors

Sensor ID	Sensor Purpose
RVACS.S.1-4	Measures temperature of air at inlet
RVACS.S.5-8	Measures temperature of air at outlet
RVACS.S.9-12	Measures air flow rate

Table XXXIV. IRACS Sensors

Sensor ID	Sensor Purpose
IRACS.S.1-2	Measures temperature of air at inlet
IRACS.S.3-4	Measures temperature of air at outlet
IRACS.S.5-6	Measures air flow rate
IRACS.S.7-8	Measures sodium-air heat exchanger fan speeds

Table XXXV. IRACS Actuators

Actuator ID	Actuator Purpose
IRACS.A.1-2	Sodium-air heat exchanger fans

Table XXXVI. SCPCS Sensors

Sensor ID	Sensor Purpose
SCPCS.S.1	Measures steam temperature in the steam generator
SCPCS.S.2	Measures steam temperature at the turbine inlet
SCPCS.S.3	Measures steam temperature at the turbine exhaust
SCPCS.S.4	Measures water temperature in the condenser
SCPCS.S.5	Measures water temperature at feedwater pump discharge

Sensor ID	Sensor Purpose
SCPCS.S.6	Measures steam pressure in the steam generator
SCPCS.S.7	Measures steam pressure in the turbine
SCPCS.S.8	Measures steam pressure in the condenser
SCPCS.S.9	Measures water pressure at feedwater pump discharge
SCPCS.S.10	Measures steam flow rate at the steam generator outlet
SCPCS.S.11	Measures steam flow rate at the turbine exhaust
SCPCS.S.12	Measures water flow rate at condenser outlet
SCPCS.S.13	Measures water flow rate into steam generator
SCPCS.S.14	Measures water level in the steam generator
SCPCS.S.15	Measures water level in the condenser
SCPCS.S.16	Measures steam quality at turbine inlet
SCPCS.S.17	Measures turbine speed
SCPCS.S.18	Measures feedwater pump speed
SCPCS.S.19	Measures main steam isolation valve position
SCPCS.S.20	Measures feedwater isolation valve position
SCPCS.S.21	Measures feedwater control valve position
SCPCS.S.22	Measures turbine throttle valve position
SCPCS.S.23	Measure turbine bypass valve position
SCPCS.S.24	Measures vibration of turbine
SCPCS.S.25	Measures vibration of feedwater pump
SCPCS.S.26	Measures steam generator dump valve position

Table XXXVII. SCPCS Actuators

Actuator ID	Actuator Purpose
SCPCS.A.1	Main steam isolation valve
SCPCS.A.2	Feedwater isolation valve
SCPCS.A.3	Feedwater control valve
SCPCS.A.4	Turbine throttle valve
SCPCS.A.5	Turbine bypass valve
SCPCS.A.6	Feedwater pump
SCPCS.A.7	Condenser pump
SCPCS.A.8	Steam generator dump valve

Table XXXVIII. SCDPCS Sensors

Sensor ID	Sensor Purpose
SCDPCS.S.1	Measures CO_2 temperature in the heater

Sensor ID	Sensor Purpose
SCDPCS.S.2	Measures CO_2 temperature at the turbine inlet
SCDPCS.S.3	Measures CO_2 temperature at the turbine exhaust
SCDPCS.S.4	Measures CO_2 temperature in the recuperator cold side
SCDPCS.S.5	Measures CO_2 temperature in the recuperator hot side
SCDPCS.S.6	Measures CO_2 temperature in the precooler
SCDPCS.S.7	Measures CO_2 temperature in the recuperator cold side
SCDPCS.S.8	Measures CO_2 temperature in the compressor inlet
SCDPCS.S.9	Measures CO_2 temperature in the compressor outlet
SCDPCS.S.10	Measures CO_2 pressure in the heater
SCDPCS.S.11	Measures CO_2 pressure in the turbine
SCDPCS.S.12	Measures CO_2 pressure in the recuperator cold side
SCDPCS.S.13	Measures CO_2 pressure in the recuperator hot side
SCDPCS.S.14	Measures CO_2 pressure at precooler
SCDPCS.S.15	Measures CO_2 pressure at compressor outlet
SCDPCS.S.16	Measures CO_2 flow rate at the heater outlet
SCDPCS.S.17	Measures CO_2 flow rate at the turbine exhaust
SCDPCS.S.18	Measures CO_2 flow rate at recuperator cold side inlet
SCDPCS.S.19	Measures CO_2 flow rate at recuperator hot side inlet
SCDPCS.S.20	Measures CO_2 flow rate into heater
SCDPCS.S.21	Measures CO_2 quality at turbine inlet
SCDPCS.S.22	Measures turbine speed
SCDPCS.S.23	Measures compressor speed
SCDPCS.S.24	Measures main CO_2 isolation valve position
SCDPCS.S.25	Measures CO_2 isolation valve position
SCDPCS.S.26	Measures CO_2 control valve position
SCDPCS.S.27	Measures turbine throttle valve position
SCDPCS.S.28	Measure turbine bypass valve position
SCDPCS.S.29	Measures vibration of turbine
SCDPCS.S.30	Measures vibration of compressor
SCDPCS.S.31	Measures CO_2 dump valve position
SCDPCS.S.32	Measures precooler pump speed
SCDPCS.S.33	Measures precooler pump vibration

Table XXXIX. SCDPCS Actuators

Actuator ID	Actuator Purpose
SCDPCS.A.1	Main CO_2 isolation valve
SCDPCS.A.2	CO_2 isolation valve
SCDPCS.A.3	CO_2 control valve
SCDPCS.A.4	Turbine throttle valve
SCDPCS.A.5	Turbine bypass valve
SCDPCS.A.6	Compressor
SCDPCS.A.7	Precooler pump
SCDPCS.A.8	CO_2 dump valve

Table XL. TESS Sensors

Sensor ID	Sensor Purpose
TESS.S.1	Measures hot tank sodium level
TESS.S.2	Measures hot tank sodium temperature
TESS.S.3	Measures hot tank wall temperature
TESS.S.4	Measures cold tank sodium level
TESS.S.5	Measures cold tank sodium temperature
TESS.S.6	Measures cold tank wall temperature
TESS.S.7	Measure hot tank sodium pump speed
TESS.S.8	Measures hot tank sodium pump vibration
TESS.S.9	Measure cold tank sodium pump speed
TESS.S.10	Measures cold tank sodium pump vibration
TESS.S.11	Measure attemperation sodium pump speed
TESS.S.12	Measures attemperation sodium pump vibration
TESS.S.13	Measures feedwater pump speed
TESS.S.14	Measures feedwater pump vibration
TESS.S.15	Measures sodium flowrate through superheater
TESS.S.16	Measures sodium flowrate through reheater
TESS.S.17	Measures sodium flowrate through evaporator
TESS.S.18	Measures sodium flowrate through preheater
TESS.S.19	Measures sodium flowrate to attemperation
TESS.S.20	Measures sodium flowrate into hot tank
TESS.S.21	Measures sodium flowrate into cold tank
TESS.S.22	Measures steam flowrate through superheater
TESS.S.23	Measures steam flowrate through evaporator
TESS.S.24	Measures feedwater flowrate through reheater

Sensor ID	Sensor Purpose
TESS.S.25	Measures feedwater flowrate through preheater
TESS.S.26	Measures pressure in steam drum
TESS.S.27	Measures steam temperature at inlet and outlet of superheater
TESS.S.28	Measures steam temperature at inlet and outlet of evaporator
TESS.S.29	Measures feedwater temperature at inlet and outlet of reheater
TESS.S.30	Measures feedwater temperature at inlet and outlet of preheater

Table XLI. TESS Actuators

Actuator ID	Actuator Purpose
TESS.A.1	Hot tank sodium pump
TESS.A.2	Cold tank sodium pump
TESS.A.3	Attemperation sodium pump
TESS.A.4	Feedwater pump

Table XLII. DCS Sensors

Sensor ID	Sensor Purpose
DCS.S.1	Measures sodium temperature at steam generator inlet
DCS.S.2	Measures main steam pressure
DCS.S.3	Measures main steam temperature
DCS.S.4	Measures electrical load
DCS.S.5-11	Measures control rod position
DCS.S.12-15	Measures speed of primary sodium pumps
DCS.S.16-18	Measures vibration of primary sodium pumps
DCS.S.19-20	Measures speed of intermediate sodium pumps
DCS.S.21-22	Measures vibration of intermediate sodium pumps
DCS.S.23	Measures feedwater pump speed
DCS.S.24	Measures vibration of feedwater pump
DCS.S.25	Measures feedwater isolation valve position
DCS.S.26	Measures feedwater control valve position
DCS.S.27	Measures turbine throttle valve position

Table XLIII. DCS Actuators

Actuator ID	Actuator Purpose
DCS.A.1-6	Manipulates position of control rods (RCS.A.1-6)
DCS.A.10-12	Primary sodium pumps (PHTS.A.1-3)
DCS.A.13-14	Secondary sodium pumps (IHTS.A.1-2)

Actuator ID	Actuator Purpose
DCS.A.15	Feedwater pump (SCPCS.A.6)
DCS.A.16	Feedwater isolation valve (SCPCS.A.2)
DCS.A.17	Feedwater control valve (SCPCS.A.3)
DCS.A.18	Turbine throttle valve (SCPCS.A.4)

Table XLIV. RPS Sensors

Sensor ID	Sensor Purpose
RPS.S.1-4	Measures neutron flux
RPS.S.5-8	Measure sodium level in hot pool
RPS.S.9-12	Measures primary sodium level
RPS.S.13-16	Measures hot sodium temperature
RPS.S.17-20	Measures cold sodium temperature
RPS.S.21-24	Measures primary sodium flow rate
RPS.S.25-28	Measures neutron flux rate
RPS.S.29-32	Measures control rod position
RPS.S.33-41	Measures position of control rod release actuator
RPS.S.42-50	Measures reserve shutdown rod position
RPS.S.51-59	Measures position of reserve shutdown rod release actuator

Table XLV. RPS Actuators

Actuator ID	Actuator Purpose
RPS.A.1-3	Releases reserve shutdown rods (RSS.A.1-3)
RPS.A.4-9	Releases control rods (RCS.A.7-12)
RPS.A.10-13	Primary sodium pumps (PHTS.A.1-4)
RPS.A.14-15	Intermediate sodium pumps (IHTS.A.1-2)
RPS.A.16	Main steam isolation valve (SCPCS.A.1)
RPS.A.17	Feedwater isolation valve (SCPCS.A.2)

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Ben B. Cipiti	8845	bbcipit@sandia.gov
Robert J. Brulles	8851	rjbrulle@sandia.gov
Lon A. Dawson	8851	ladawso@sandia.gov
Jenna deCastro	8851	jdecast@sandia.gov
Lee T. Maccarone	8851	lmaccar@sandia.gov
Michael T. Rowland	8851	mtrowla@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Daniel Warner	daniel.warner@nuclear.energy.gov	DOE-NE

This page left blank

This page left blank

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.