Advanced Reactor Safeguards & Security

Design of Defensive Cybersecurity Architectures for High Temperature, Gas-Cooled Reactors

Prepared for
US Department of Energy

Lee Maccarone, Michael Rowland, Robert Brulles, Andrew Hahn

Sandia National Laboratories

August 2024
SAND2024-11449R

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 High Temperature, Gas-Cooled Reactors (HTGRs). 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 HTGR and describes a DCSA design process using event tree analysis so that the template may be optimized for a given HTGR 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 M2CT-24SN1102039. The authors would like to acknowledge the program leadership provided by Dan Warner (DOE-NE), Ben Cipiti (Sandia National Laboratories), and Katya Le Blanc (Idaho National Laboratory). The authors would also like to acknowledge J. Connor Grady (Sandia National Laboratories) for producing several figures in this report.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

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 probabilistic risk assessment (PRA) of an HTGR 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.

Design constraints for the assignment of systems to zones can be obtained using event tree analysis. Event tree analysis is a top-down analysis approach that assesses the probability outcomes given an initiating event [6]. For the purpose of DCSA design, we consider only the manipulation of functions performed by control systems (i.e., not passive safety features or random events). Given this scope, event trees can be iteratively analyzed to identify the impact of an adversary compromising combinations of facility functions. If an adversary compromises a function, it is assumed that the event can be caused by the adversary at will rather than at the event frequency that is used in the event tree. If compromising a set of functions causes the event sequence frequency (ESF) to rise to an unacceptable licensing basis event (LBE) category (e.g., a beyond design basis event (BDBE) becomes a design basis event (DBE)), then the systems must be placed in separate DCSA zones as part of denial of access analysis.

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), Investment Protection System (IPS), 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 to 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 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 HTGR 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.

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.

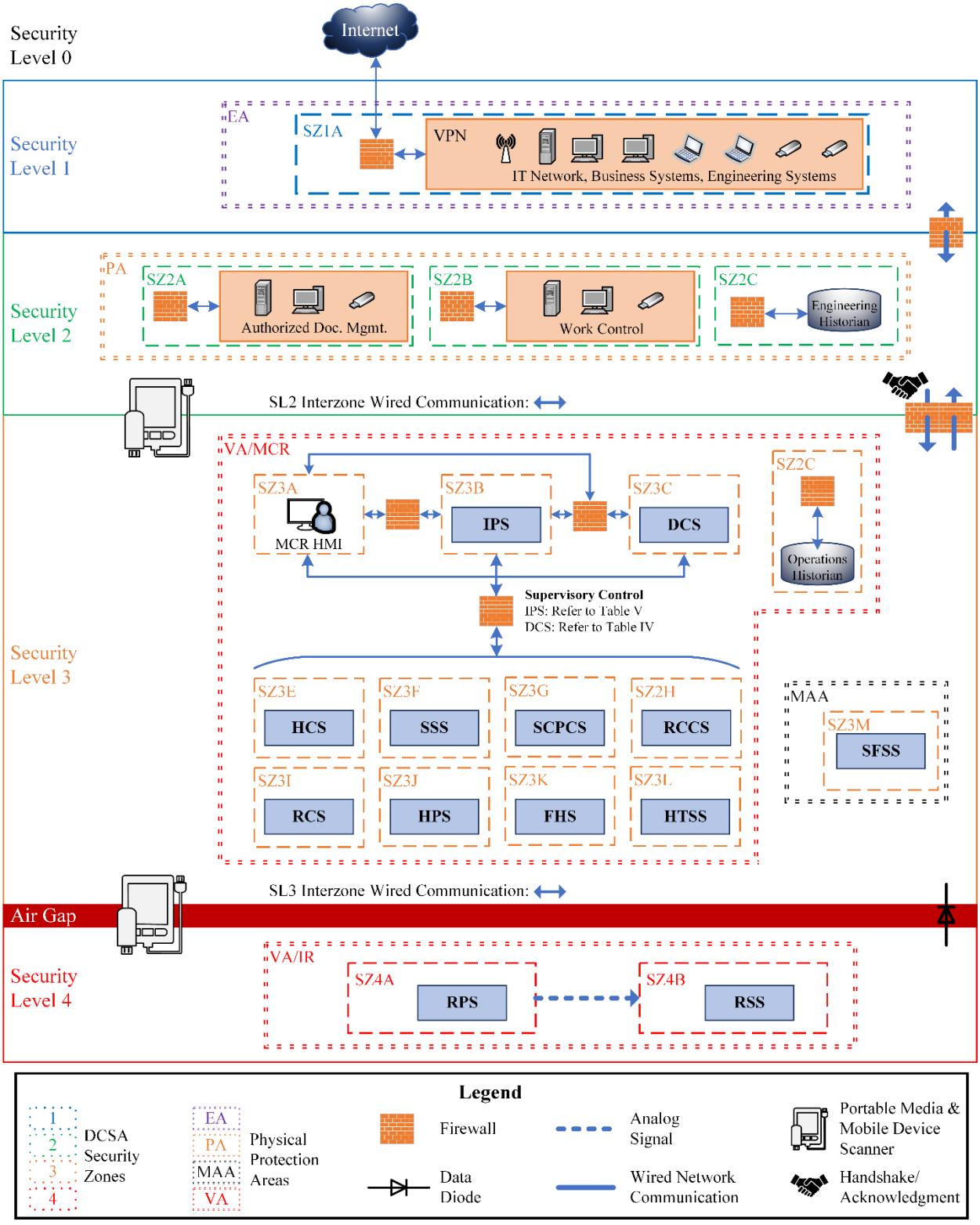

Figure 1. HTGR DCSA Template

This page left blank

ACRONYMS AND TERMS

Acronym/Term	Definition
ACL	Access control list
AFSA	Adversary Functional Scenario Analysis
AOO	Anticipated operational occurrence
AR	Advanced reactor
AVR	Arbeitsgemeinschaft Versuchsreaktor
BDBE	Beyond design basis event
BISO	Bistructural-isotropic
CDA	Critical digital asset
CEAS	Cyber Extension to Safety Accident Scenario Analysis
CFR	Code of Federal Regulations
CSP	Cybersecurity plan
DBA	Design basis accident
DBE	Design basis event
DBT	Design basis threat
DCS	Distributed Control System
DCSA	Defensive cybersecurity architecture
DG	Draft guide
DiD	Defense-in-depth
EA	Exclusion area
ESF	Event sequence frequency
F-C	Frequency-consequence
FHS	Fuel Handling System
FHSS	Fuel Handling and Storage System
HCS	Helium Circulator System
HMI	Human-machine interface
HPB	Helium pressure boundary
HPS	Helium Purification System
HSS	Helium Service System
HTGR	High temperature, gas-cooled reactor
HTR-10	High-Temperature Reactor - 10
HTR-PM	High-Temperature Reactor Pebble-Bed Module
HTSS	Helium Transfer and Storage System
HTTR	High-Temperature Engineering Test Reactor
HVAC	Heating, ventilation, and air conditioning

Acronym/Term	Definition
IAEA	International Atomic Energy Agency
I&C	Instrumentation and control
IDPS	Intrusion detection and prevention systems
IE	Incredible event
IP	Internet Protocol
IPL	Independent protection layer
IPS	Investment Protection System
IR	Instrumentation room
IT	Information technology
LAA	Limited access area
LMP	Licensing Modernization Project
LWR	Light water reactor
MAA	Material accountability area
MCR	Main Control Room
ML	Main line
NPP	Nuclear power plant
NRC	Nuclear Regulatory Commission
NSRST	Non-safety related with special treatment
NSS	Nuclear Security Series
NST	Non-safety related with no special treatment
OCS	Operator Control System
PA	Protected area
PMMD	Portable media and mobile devices
PRA	Probabilistic risk assessment
RB	Reactor building
RCCS	Reactor Cavity Cooling System
RCS	Reactivity Control System
RCSS	Reactivity Control and Shutdown System
RF	Radio frequency
RPS	Reactor Protection System
RSS	Reserve Shutdown System
RG	Regulatory guide
SCPCS	Steam Cycle Power Conversion System
SeBD	Security-by-design
SFSS	Spent Fuel Storage System

Acronym/Term	Definition
SG	Steam generator
SL	Security level
SMR	Small modular reactor
SR	Safety-related
SSCs	Systems, structures, and components
SSS	Start-Up and Shutdown System
STPA	Systems-Theoretic Process Analysis
SZ	Security zone
TCA	Tiered Cybersecurity Analysis
TCP	Transmission Control Protocol
THTR	Thorium High-Temperature Reactor
TRISO	Tristructural-isotropic
VA	Vital area
VLAN	Virtual local area network
WNA	World Nuclear Association

This page left blank

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 high temperature, gas-cooled reactor (HTGR) 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 probabilistic risk assessment (PRA) of an HTGR 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 aims to develop requirements for passive DCSA measures by:

- Identifying significant functions performed via PRA.
- Identifying the sensitivity of PRA to cyber compromise of specific systems that implement these functions.

- Indicating the stringency of the requirements (i.e., security level) for each function and its associated system.
- Assigning applicable technical and operational cybersecurity controls to each security level.

2. BACKGROUND

This section provides a conceptual overview of advanced reactor SeBD considerations, DCSAs, and defensive cybersecurity strategies.

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.

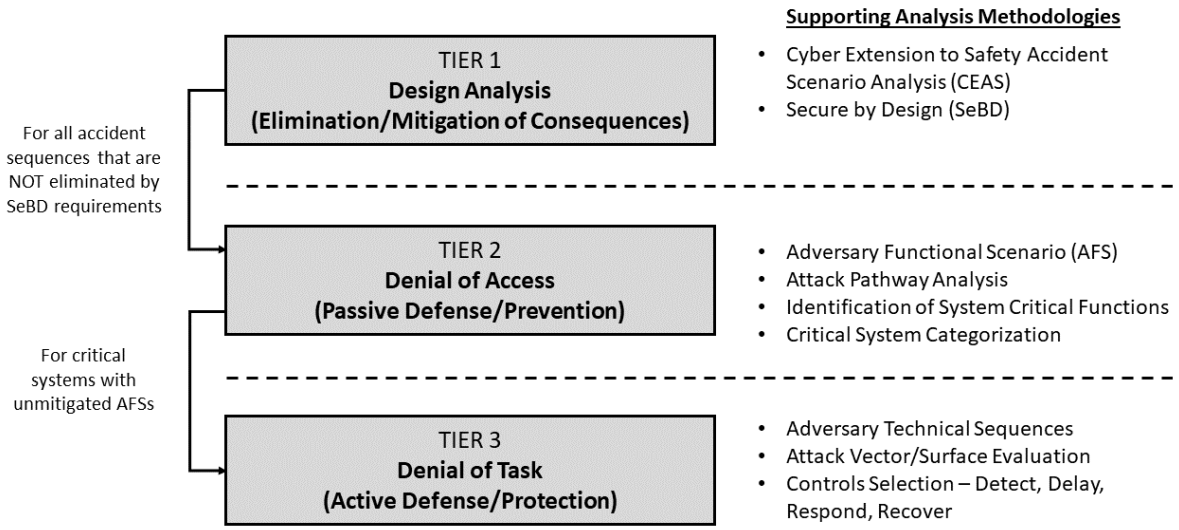

Figure 2: Tiered Cybersecurity Analysis (TCA) [12]

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.

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-

[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).

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 first phase of design maturity is the conceptual phase where the reactor concept is developed. In Phase 1 critical questions are asked and major risks are identified. The second phase of design maturity is plant-level design. In Phase 2 the requirements and design parameters of key systems, structures, and components (SSCs) are defined. Key outputs of Phase 2 include process flow diagrams and a preliminary I&C architecture. The third phase of design maturity is system-level design. In Phase 3 the requirements and design parameters of key SSCs are further refined and other plant systems are defined. Key outputs of Phase 3 include piping and instrumentation diagrams, I&C systems design, and a refined I&C architecture. Finally, the fourth phase of design maturity is component-level design. In Phase 4 the engineering details are finalized for SSCs to allow for manufacturing to begin [19].

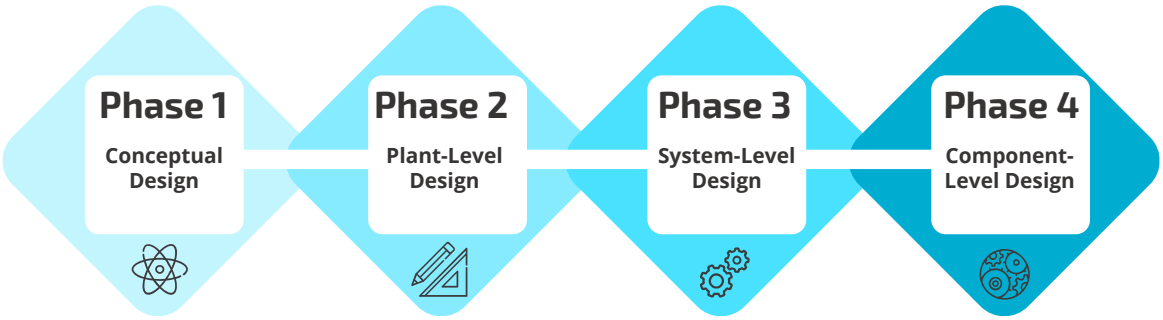

Figure 3: Plant Design Phases of Maturity [19]

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.

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)

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].

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" [20].
- 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.

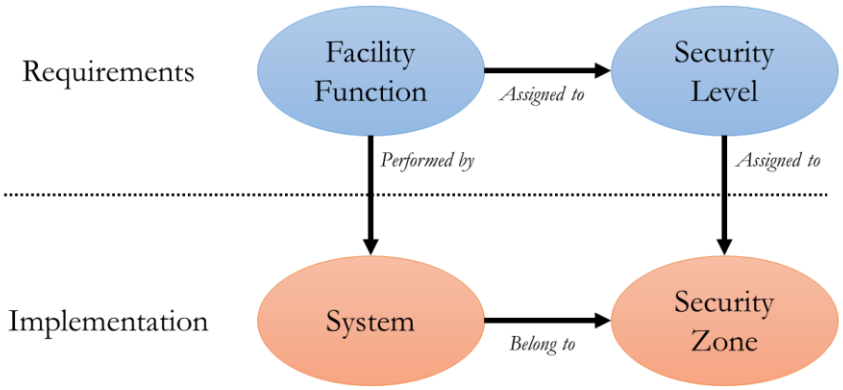

Figure 4. Relationship Between DCSA Elements (Adapted from [1])

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 defense in depth (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.

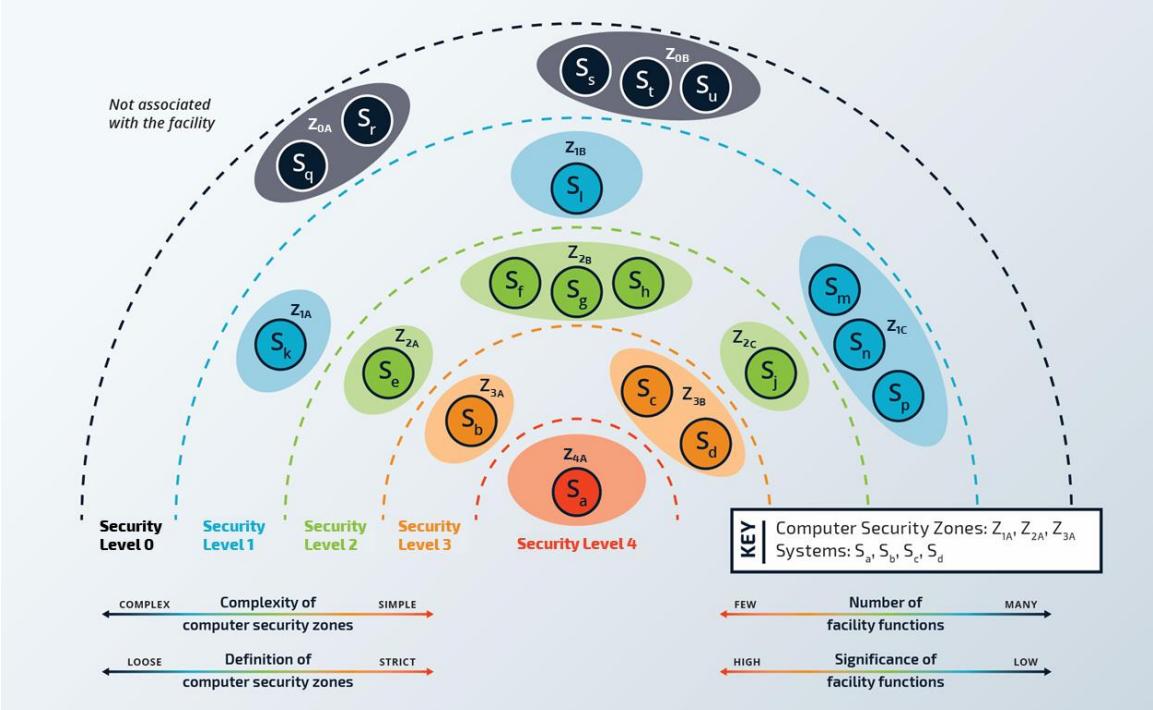

Figure 5. Conceptual DCSA Model [1]

2.3.1. Facility Functions

A mature process is used to categorize safety functions and classify safety systems. I&C systems important to safety are identified on the basis of their necessary safety functions and the definition of systems that perform certain combinations of these functions [21]. The systems important to safety are based on the following fundamental safety functions that are required for all plant states:

- Control of reactivity;
- Removal of heat from the reactor and from the fuel store;
- Confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

These functions need to be considered within the plant state context. For example, control of reactivity during normal operations is less significant, when associated with the consequences of accident conditions, than during Anticipated Operational Occurrences (AOOs) and Design Basis Accidents (DBAs). Figure 6 identifies plant states associated with NPPs, consequence severity increases from normal operations being the lowest, to design extension conditions with core melting being associated with the most severe consequences [20].

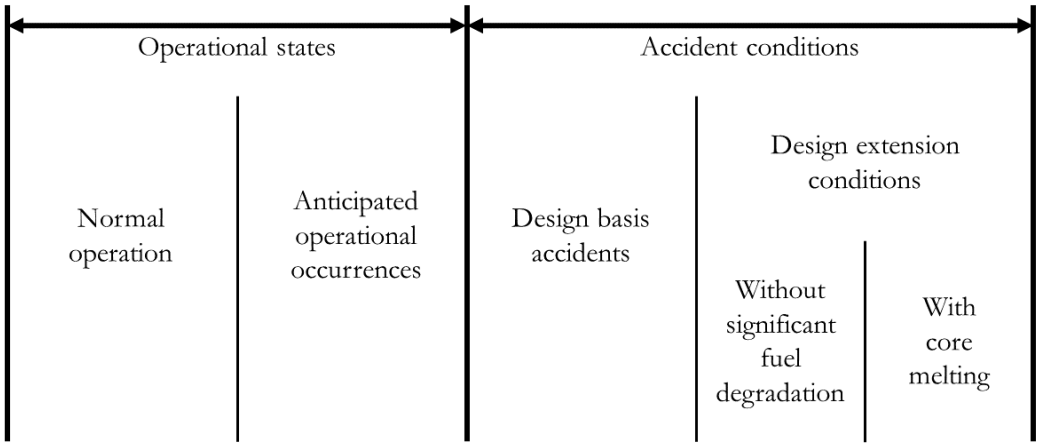

Figure 6. Plant States Considered in Design for a Nuclear Power Plant [20]

Para 5.34 of [22] specifies that the method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:

1. The safety function(s) to be performed by the item.
2. The consequences arising from failure of the item to perform its safety function.
3. The frequency with which the item will be called upon to perform a safety function
4. The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function

The identification of the functions performed by an item is a critical element in determining its safety classification. This approach is generalized by [20] as follows:

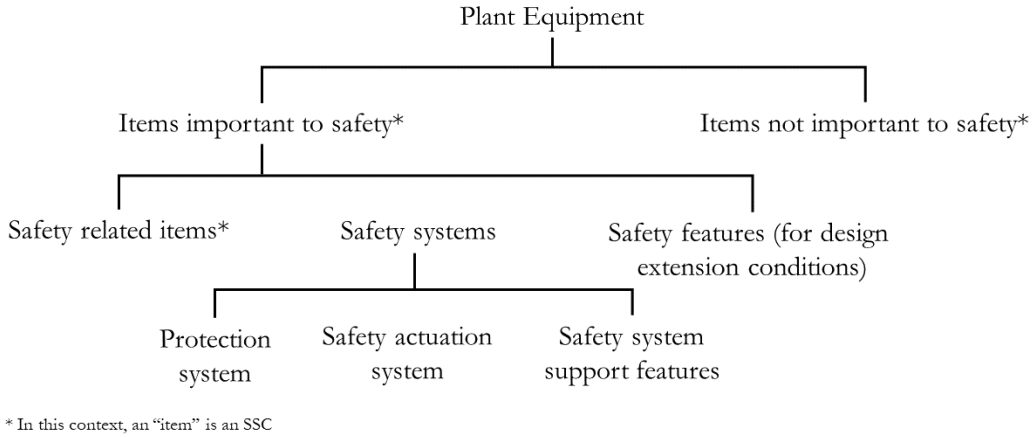

Figure 7. Plant Equipment for a Nuclear Power Plant [20]

ARs leverage the above attributes to generate a frequency-consequence evaluation criteria (referred to as the F-C Target). This aims to establish license conditions for ARs based on risk. This F-C target is shown in Figure 8 [23]. The F-C target categorization is based upon a safety analysis, likely included within PRA models and event trees. This report extends the PRA model and F-C target evaluation to consider Cyber-Extension to Safety Accident Scenario (CEAS) Analysis and associated Adversary Functional Scenario Analysis (AFSA) to evaluate the significance of a function and the associated system, assign the function to a security level within the DCSA, and specify requirements.

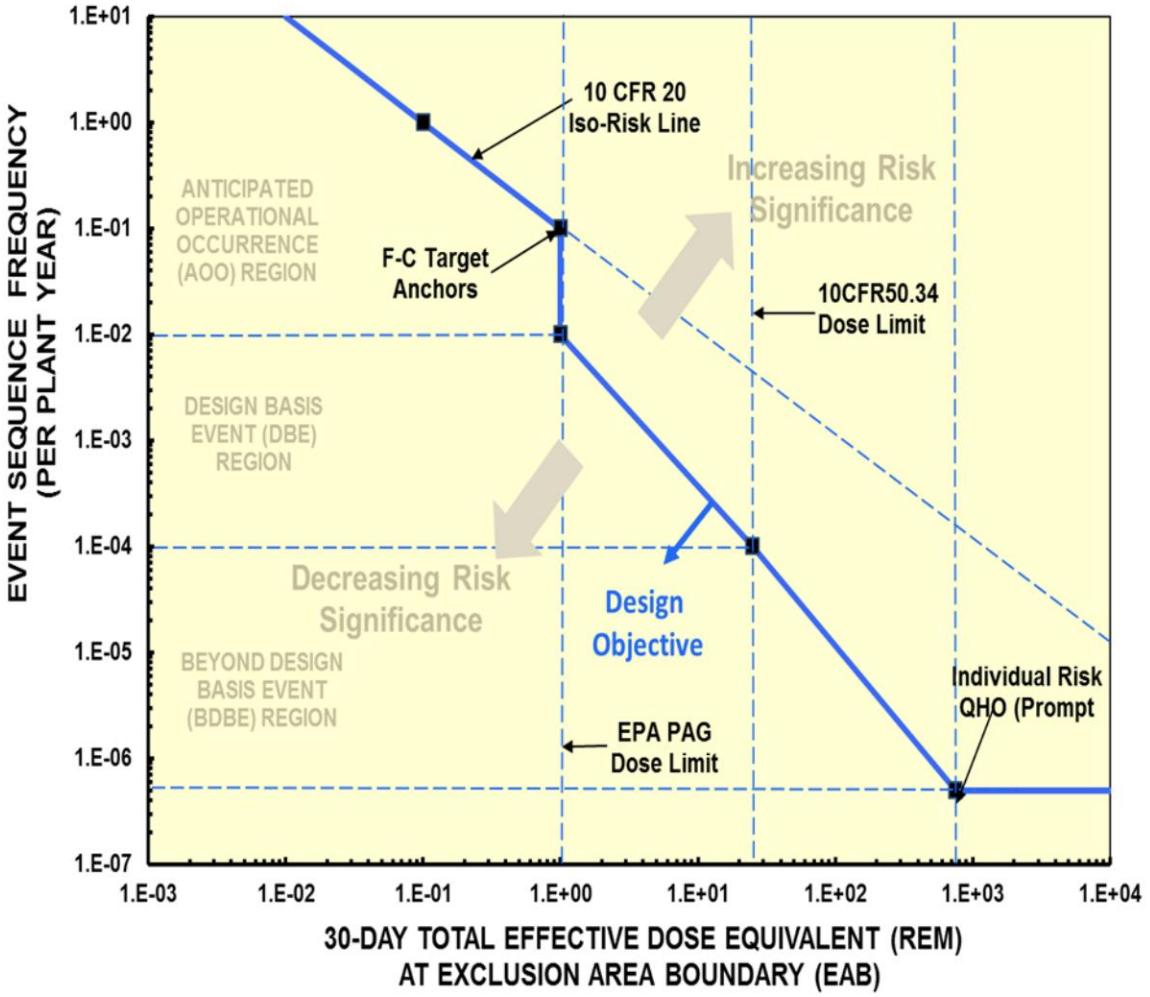

Figure 8. Frequency-Consequence (F-C) Target [23]

2.3.2. Security Levels

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 9. DCSAs implemented within the existing fleet and the example provided in are based upon the Biba trust model [24]. 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.

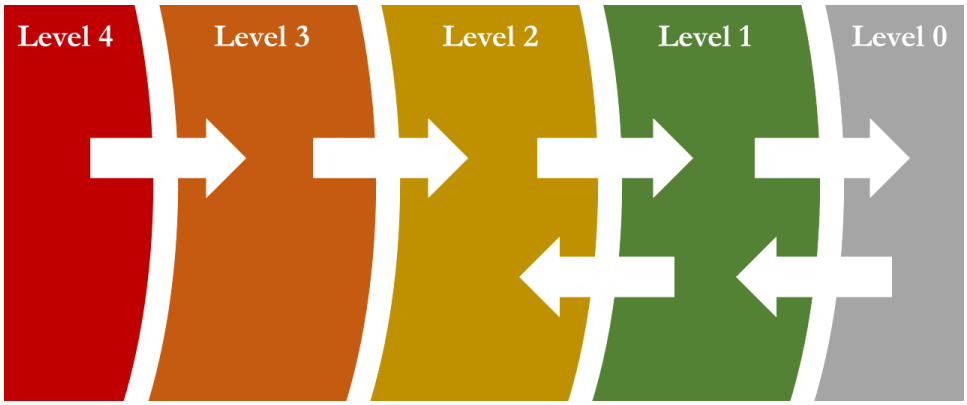

Figure 9. Simplified Defensive Cybersecurity Architecture [7]

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.

These requirements are informed by current application of the security level and zones concepts and the design basis of the existing fleet, with its reliance on many isolated and air-gapped system. These wrap-around requirements, that in practice result in controls at the logical and physical boundaries supported by management controls and robust physical protection, eliminate many of the use cases that are likely necessary for ARs to achieve cost-competitiveness with the legacy fleet or other

technologies for electricity generation (e.g., remote management and control, offsite physical protection).

2.3.3. Systems

Digital systems require cybersecurity. As detailed in the preceding section, security levels and security zones are fundamental concepts used to apply a graded approach and implement defense in depth. However, current practice is to implement cybersecurity measures that meet the set of requirements of a specific security level. Operating experience has demonstrated that this is an effective approach but relies upon the design bases of the existing fleet.

ARs are currently in various stages of design maturity. Application of the DG-5075 TCA during the earliest stages of design has the potential to integrate security requirements and their associated cybersecurity controls within facility, DCSA, and system design. These multiple layers of defense would enable use cases necessary for ARs. For example, requirements 1-3 from Section 2.3.2 could be modified to directly apply to system design as follows:

1. Only networked flow of data is allowed from level 3 to level 2 systems that meets security requirements of the systems. For example, configurable settings that are limited by non-cyber independent protection layers (IPLs) to only those values validated to be within safe operational limits.
2. Command and control communications are tightly restricted to minimize exposure to exploitation. For example, these communications may be passed to a proxy or gateway that then transmits these commands via relay logic. This deterministically limits the types of communications to the operational computer.
3. Remote maintenance is permitted, so long as there is real-time strict detection and alerting on unauthorized attempts and independent concurrent verification of all remote maintenance activities. The independent concurrent verification may be provided by a separate system immune to network connectivity attack pathways (i.e., wired and wireless) due to protection offered by a unidirectional deterministic gateway device (e.g., data diode).

Modified requirements 1 and 2 impose demands on system design that will, if implemented, significantly impact the system's interfaces, operation modes, and limits. Whereas, modified requirement 3 imposes external demands on DCSA and licensee activities. Improved system designs aim to both eliminate or control access through passive DCSA requirements, that may be implemented within the systems of the zone; but also provides key elements for protective functions (i.e., detect, delay, respond, recover) necessary to meet Tier 3 TCA (i.e., active defense) requirements.

2.3.4. Security Zones

A key element of DCSA is the grouping and placement of systems that have similar cybersecurity demands (or requirements) into cybersecurity zones. Ideally, these zones have hardened or fortified boundaries and conduits or entry control points that control access to the zone. For this report, there are two types of zone boundaries applicable to cybersecurity: physical and logical.

A physical boundary is a boundary that protects against entities that occupy volume and have mass. These entities include people, drones, robots, portable media, and mobile devices. Typical physical boundary elements include hardened walls or fences, doors or entry points, ceilings, locked cabinets or safes, secure conduits for network cabling, and secure rooms or enclosures for switches and routers. Installation of rogue devices which enable new unauthorized wired or wireless connectivity

are also defended by physical boundaries. Physical boundaries prevent unauthorized access for the physical access and portable media attack pathways.

Logical boundaries are boundaries that protect against entities interacting with the information associated with a zone. These entities do not occupy volume and do not have mass. These entities include malware such as, bots, trojans, worms, and viruses. Logical boundaries are used to separate zones and are typically decoupled from one another via a technical measure such as a firewall or data diode. Logical boundaries prevent unauthorized access for the wired network connectivity and wireless network connectivity attack pathways.

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:

6. Physical Access
7. Wired Network Connectivity
8. Wireless Network Connectivity
9. Portable Media and Mobile Device
10. 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 [25].

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 modules, data diodes, and network segmentation. Approaches that enhance fortification are system hardening such as the removal of unnecessary ports and services from a computer system. Unnecessary system services must be disabled or removed from devices to remove vulnerabilities that are present in these services.
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 provides 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.
3. **Area or Access Control:** The selective restriction of either access or denial to a place or other resource. Access control aims to prevent adversarial access to the to either an internal area or digital components of zones and systems. Access control can be passive, such as physical USB port blockers, walls, locked doors, and network traffic filtering or active, such as intrusion protection systems, or transition to more defensive modes of operations.

Typically, these types of defensive strategies are combined into an overall plan for defense-in-depth 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 implemented detection, protection and response 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 defense-in-depth concept is shown in Figure 10. The three defensive strategies are shown within this concept in Appendix A.

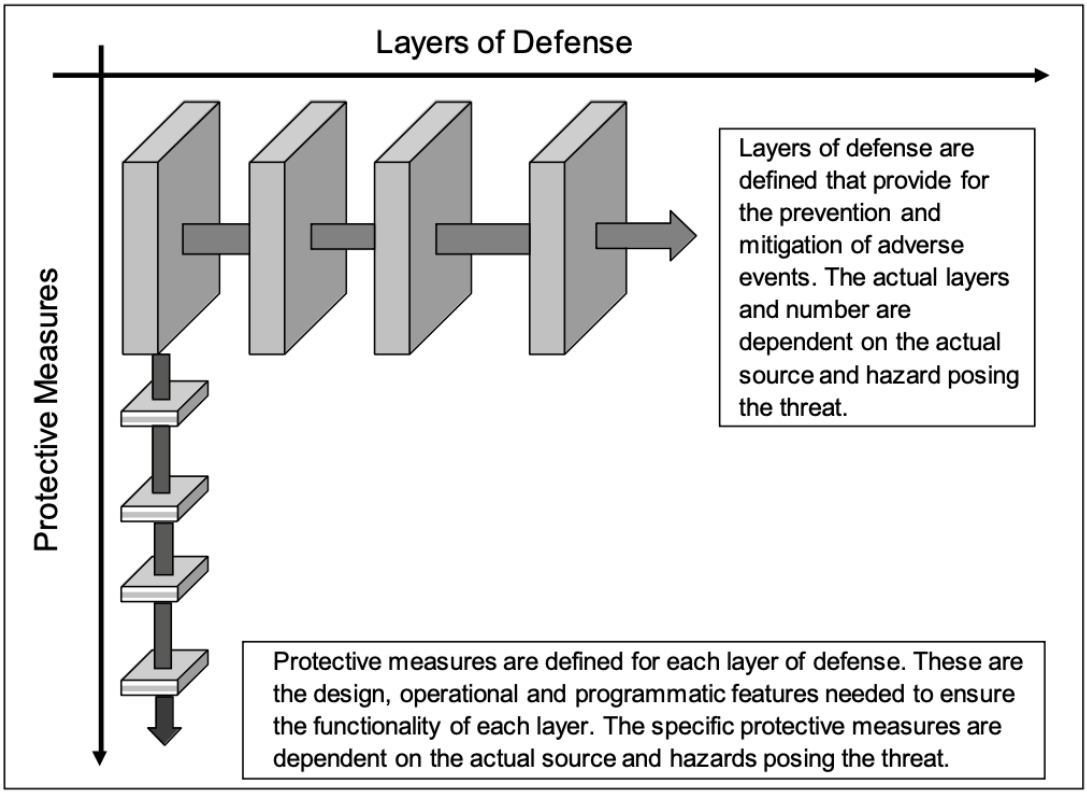

Figure 10. U.S. NRC's Defense-in-Depth Concept [23]

This page left blank

3. HIGH TEMPERATURE, GAS-COOLED REACTORS

This section contains descriptions of the systems generally found in both constructed and conceptual HTGRs. A list of constructed HTGRs is provided in Table II. The designs of these reactors and publicly available conceptual designs were used to inform the HTGR description in this section. Dragon Reactor, Peach Bottom, Arbeitsgemeinschaft Versuchsreaktor (AVR), Fort Saint Vrain, and Thorium High-Temperature Reactor (THTR) have been decommissioned, but the High-Temperature Engineering Test Reactor (HTTR), High-Temperature Reactor – 10 (HTR-10), and High-Temperature Reactor Pebble-Bed Module (HTR-PM) are currently operating.

Table II. Constructed HTGRs [26]

Facility	Country	Purpose	Commissioned	Shutdown
Dragon Reactor [27]	United Kingdom	Testing fuel, fuel elements, and structural materials	1964	1975
Peach Bottom [28]	United States	Experimental reactor; commercial	1967	1974
AVR [29, 30]	Germany	Experimental reactor; fuel testing	1967	1988
Fort Saint Vrain [31, 32]	United States	Commercial; testing	1974	1989
THTR-300 [33]	Germany	Commercial; fuel testing	1985	1988
HTTR [34, 35]	Japan	Experimental reactor	1999	--
HTR-10 [36, 37, 38, 39, 40]	China	Test and demonstration reactor	2000	--
HTR-PM [41, 42]	China	Demonstration reactor	2021	--

The HTGR DCSA analysis and design presented in Sections 4 and 5 are 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 B 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, HTGRs have used either bistructural-isotropic (BISO) fuel (Peach Bottom and THTR) or tristructural-isotropic (TRISO) fuel (all other HTGRs). Both X-energy and Kairos Power have submitted fuel qualification methodology reports to the US NRC for their reactors [43, 44]. Both topical reports specify that a UCO fuel kernel is to be used within the TRISO pellet [43, 44]. Based on the historical use of TRISO and pre-application activities with US NRC, our plant design assumptions are:

A.1. The nuclear fuel is contained in TRISO particles

A.2. The TRISO particles contain UCO fuel kernels

The TRISO fuel particle is composed of five layers as shown in Figure 11. The layers and their functions are summarized below, starting with the innermost layer.

- Fuel Kernel: This layer provides fission energy, retains fission products, and controls the particle oxygen potential [45].
- Buffer Carbon: This layer attenuates fission recoils, provides void volume for fission gases, and accommodates fuel kernel swelling [45].
- Inner Pyrolytic Carbon: This layer prevent chlorine attack of the fuel kernel during manufacturing, provides structural support, and retains gaseous fission products [45].
- Silicon Carbide: This layer is the primary load-bearing layer of the particle and retains fission products [45].
- Outer Pyrolytic Carbon: This layer provides structural support and provides a fission product barrier [45].

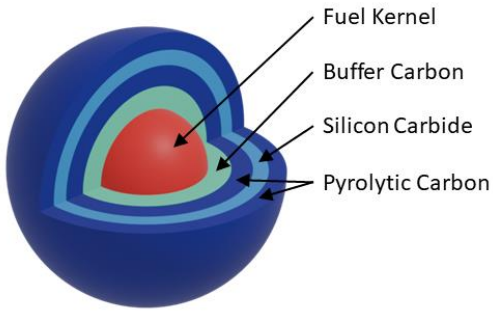

Figure 11. TRISO Fuel Particle [46]

Assumptions A.1 and A.2 are important for the design of a DCSA within the context of the TCA because the use of TRISO particles with a UCO fuel kernel may act as a physical robustness factor that eliminates or mitigates the effects of a cyber-attack. UCO fuel is designed to provide improved fuel performance at high burnup, thereby enabling longer fuel cycles [45]. UCO also eliminates CO formation and reduces internal gas pressure [45]. Modern TRISO particles retain fission products well under extreme temperature conditions, enabling coolant output temperatures near 1000 °C [47].

3.1.2. Nuclear Fuel Configuration

The TRISO fuel particles may be formed into either spherical fuel pebbles as part of a pebble-bed reactor configuration, or into cylindrical fuel compacts as part of a prismatic block configuration [47]. The first constructed HTGRs leveraged the prismatic block configuration [26]. Of the currently operating reactors, the HTTR leverages the prismatic block configuration, and the HTR-10 and HTR-PM leverage the pebble-bed configuration [34, 36, 41]. X-energy's Xe-100 reactor is designed with a pebble-bed configuration [48, 49]. The Xe-100 active core volume will accommodate approximately 224,000 fuel spheres in a cylindrical pebble-bed [49]. Based on current industry trends, our plant design assumptions are:

A.3. The HTGR has a pebble-bed configuration

A.4. The pebble-bed volume is cylindrical and not annular

A.5. The HTGR utilizes on-line refueling

A pebble-bed reactor configuration is shown in Figure 12. The core shape is typically tall with a relatively small diameter, providing three key design advantages:

1. Optimized temperature distribution across the fuel [50]
2. Reduced external heat rejection pathway for decay heat [50]
3. Improved reactivity control via control rods in the reflectors [50]

Fuel spheres are typically loaded through the top of the core barrel and unloaded through the bottom of the core barrel [50]. The pebble bed fuel core is surrounded by graphite reflectors to reduce neutron escape [50]. An annular core configuration would utilize either central graphite spheres, stacked graphite blocks, or dynamic center column configurations [50]. The control rods and their operation will be discussed in later sections.

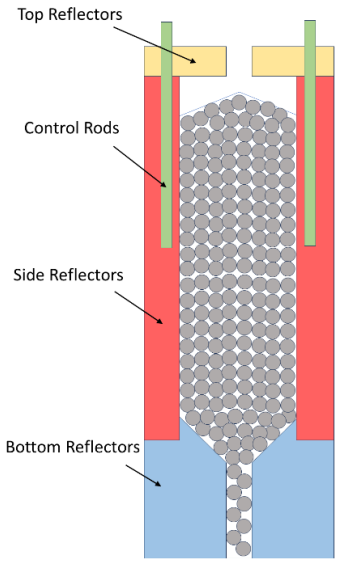

Figure 12. HTGR Pebble Bed [50]

Assumptions A.3 - A.5 are important for the design of a DCSA because they affect the requirements for systems to handle and store the fuel spheres. These systems will be discussed in greater detail in Section 3.2.

3.1.3. Reactor Operating Modes

Based on HTGR training documentation [50], it is assumed that the reactor has three operating modes:

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. Full helium coolant flow through the core via the primary circulators is establish and the core is transitioned to energy production [50].
2. Energy Production (Normal Operations): In this mode of operation, power is adjusted by changing the coolant mass flow rate through the core via the coolant pressure or the circulator speed control. The reactor outlet temperature is manipulated using the control rods and the reactor is refueled on-line [50].

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 with residual heat removal systems [50].

These modes are documented in the following assumption:

A.6. The reactor has three operating modes: start-up, energy production, and shutdown

Assumption A.6 is important for DCSA design because it informs the interdependencies between plant systems required to achieve the functions performed during each operating mode. 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.7. 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.7 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)

An overview of the FHS is shown in Figure 2. The FHS functions are:

F.FHS.1. Charge fresh fuel from storage [51]
F.FHS.2. Load fuel into the reactor [51]
F.FHS.3. Re-circulate used fuel through the reactor [51]
F.FHS.4. Unload spent fuel from the reactor [51]
F.FHS.5. Maintain operation [51]

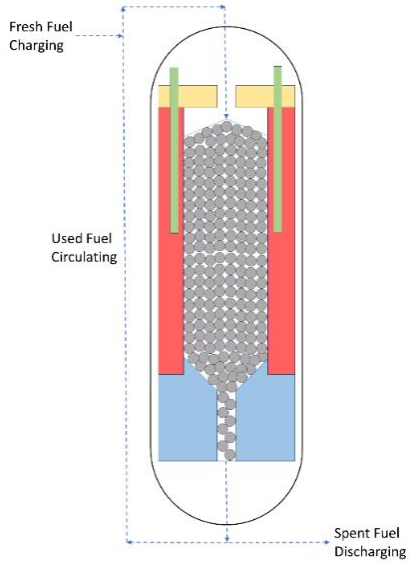

Figure 13. Fuel Handling System (FHS) [51]

The fuel charging operation supplies the circulating circuit with fuel from on-site storage drums to replace spent fuel. Fuel drums are stored on-site which enables approximately 180 days of continuous operation [51].

The fuel loading operation loads both new and used fuel spheres into the top of the reactor. New replace used spheres depending on burnup and sphere mechanical conditions [51].

The fuel circulation operation extracts fuel from the bottom of the core, separates fuel that is damaged or spent, and returns intact fuel below the burnup limit to the top of the reactor. Spheres may pass through the core 1-15 times before reaching their burnup limit [51].

Extracted spheres that have reached their burnup limit are discharged to spent fuel storage [51]. The SFSS is discussed in greater detail in the following section.

The fundamental sensors and actuators necessary for FHS operation are summarized in Table XIV and Table XV, respectively. Fuel spheres must be tracked in transit through the FHS [52]. Actuators transit the spheres throughout the FHS.

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 [51]

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 [51, 53]. Based on the X-energy spent fuel management plan [54], the SFSS assumptions are:

A.8. The Spent Fuel Storage System (SFSS) is passively air-cooled via natural convection

A.9. The Spent Fuel Storage System (SFSS) operates independently of other plant systems

Assumption A.8 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.9 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 XVI and Table XVII, respectively [54].

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 [50]. Based on documentation of the historical pebble-bed reactors (AVR, THTR, HTR-10, and HTR-PM) and X-energy's licensing topical reports [30, 33, 36, 41, 49], it is assumed that the RCCS consists of two subsystems:

A.10. The Reactivity Control and Shutdown System (RCSS) consists of two subsystems: the Reactivity Control System (RCS) and Reserve Shutdown System (RSS).

Assumption A.10 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 [50]

F.RCS.2. Achieve hot shutdown state by inserting control rods [55, 36]

F.RCS.3. Achieve cold shutdown state by inserting control rods in conjunction with the RSS [55, 36]

F.RCS.4. Drop control rods during a reactor trip [22]

The RCS manipulates the reactivity of the core by inserting or withdrawing control rods to absorb neutrons [50]. The Xe-100 RCS design has nine control rods [56]. The control rods typically remain partially inserted and are manipulated incrementally to meet operational needs [56]. During a reactor trip, the control rods are quickly fully inserted to achieve safe shutdown [22, 56].

With the exception of AVR, all previous pebble-bed HTGRs have had control rods that insert from the top of the reactor [30, 33, 36, 41], and Xe-100 licensing topical reports indicate that the control rods will insert from the top of the reactor [56], therefore it is assumed that:

A.11. The Reactivity Control System (RCS) control rods insert from the top of the reactor.

A.12. 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.11 and A.12 are important for DCSA design because they inform the actuation requirements of the RCS control rods during a reactor trip.

Both the HTR-10 and HTR-PM reactors use their primary control rods for routine reactivity control and hot shutdown (i.e., subcritical reactor with core and coolant at high temperatures) [55, 36], therefore it is assumed that:

A.13. The insertion of the Reactivity Control System (RCS) control rods provides sufficient neutron absorption for hot shutdown.

To achieve cold shutdown, the HTR-10 and HTR-PM reactors must use both their primary control rods and RSS [55, 36], therefore it is assumed that:

A.14. The insertion of both the Reactivity Control System (RCS) control rods and the Reserve Shutdown System (RSS) control rods are necessary to provide sufficient neutron absorption for cold shutdown.

Assumptions A.13 and A.14 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 XVIII and Table XIX, respectively [56].

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 [55, 36]

F.RSS.2. Drop shutdown rods during a reactor trip [56]

The RSS manipulates the reactivity of the core by inserting shutdown rods to absorb neutrons [50]. The Xe-100 RSS design has nine shutdown rods [56]. Unlike the RCS control rods, the RSS shutdown rods are fully withdrawn when not in use, and are rapidly inserted when needed [56].

Following the same logic as applied to Assumptions A.11 and A.12, it is assumed that:

A.15. The Reserve Shutdown System (RSS) shutdown rods insert from the top of the reactor.

A.16. 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 XX and Table XXI, respectively [56].

3.4. Helium Circulator System (HCS)

The primary functions of the Helium Circulator System (HCS) are:

F.HCS.1. Provide cooling to the reactor core [57]

F.HCS.2. Transport thermal energy to the secondary loop [57]

Early designs of HCSs featured a main circulator to transfer heat to the secondary loop and a smaller shutdown cooling circulator for rapid cooling of the reactor system [58]. A comparison of HCS design features is shown in Table III. As shown in Table III, there is significant variability in the HCS design parameters across existing and proposed designs. Considering the variability in design features, we place emphasis on the most modern designs and make the following assumptions:

A.17. The Helium Circulator System (HCS) uses two circulators

Assumption A.17 is important for DCSA design because it informs interdependencies required for the HCS to perform its functions.

Table III. HCS Design Features [26, 59, 55, 60]

Design Feature	Dragon	Peach Bottom	AVR	Fort St. Vrain	THTR	HTTR	HTR-10	HTR-PM	Xe-100
Helium Pressure (MPa)	2	2.3	1.1	4.8	4	4	3	7	5.82
Helium Flow Rate (kg/s)	9.62	60	13	110	51.2	10.2-12.4	3.2-4.3	96	78.5
Reactor Inlet Temperature (°C)	350	327	275	404	250	395	250	250	259
Reactor Outlet Temperature (°C)	750	700-726	950	777	750	850-950	700	750	750
Circulator Size (kWe)	75	1,417	220	3,954	2,300	260 x 2, 190 x 1	165	1,500	--
Circulator Quantity	6	2	2	4	6	3	1	2	2

The fundamental sensors and actuators necessary for HCS operation are summarized in Table XXII and Table XXIII, respectively [57, 61, 59].

3.5. Helium Service System (HSS)

The purpose of the Helium Service System (HSS) is to provide clean, high-pressure helium to be circulated by the HCS [62]. Based on documentation of the historical pebble-bed reactors [62], it is assumed that the HSS consists of two subsystems:

A.18. The Helium Service System (HSS) consists of two subsystems: the Helium Purification System (HPS) and Helium Transfer and Storage System (HTSS).

Assumption A.18 is important for DCSA design because it informs the interdependencies between plant systems required to achieve their functions. The following sections describe the HPS and HTSS in greater detail.

3.5.1. Helium Purification System (HPS)

The primary functions of the Helium Purification System (HPS) are:

F.HPS.1. Remove chemical impurities from the helium [62]
F.HPS.2. Remove radionuclide impurities from the helium [62]
F.HPS.3. Provide purified helium for purges and buffers [62]
F.HPS.4. Purify helium that is pumped to storage [62]
F.HPS.5. Remove water from the helium circuit following a water ingress event [62]

The HPS often consists of a filter to remove dust-like impurities, a copper oxide bed to oxidize hydrogen and carbon monoxide impurities, and a charcoal absorber to absorb impurities including methane, oxygen, and nitrogen [37, 63, 64]. Many of these components are passive, modularized, and have high reliability and availability [62].

The fundamental sensors and actuators necessary for HPS operation are summarized in Table XXIV and Table XXV, respectively [62].

3.5.2. Helium Transfer and Storage System (HTSS)

The primary functions of the Helium Transfer and Storage System (HTSS) are [62]:

F.HTSS.1. Provide storage capacity for helium inventory exchanges [62]
F.HTSS.2. Pressurize the primary coolant inventory [62]
F.HTSS.3. Depressurize the primary coolant inventory [62]
F.HTSS.4. Control the primary coolant inventory [62]
F.HTSS.5. Maintain helium circuit at sub-atmospheric pressures during maintenance [62]

The HTSS receives purified helium from the HPS and stores it in a series of tanks with various pressures or recirculates it to the primary loop [62]. The helium from the high pressure supply tanks is used by auxiliary plant services [62].

The fundamental sensors and actuators necessary for HTSS operation are summarized in Table XXVI and Table XXVII, respectively [62].

3.6. Reactor Cavity Cooling System (RCCS)

The primary functions of the Reactor Cavity Cooling System (RCCS) are:

F.RCCS.1. Control reactor cavity concrete temperatures in normal operation [65]
F.RCCS.2. Cool the reactor vessel [65]

F.RCCS.3. Control reactor cavity concrete temperature in accident conditions [65]

F.RCCS.4. Control reactor vessel temperatures in accident conditions [65]

F.RCCS.5. Residual/decay heat removal in accident conditions [65]

The RCCS may be implemented with a passive and/or active cooling design and the coolant may be air or water [65]. Air cooling allows for an unlimited coping period and requires no other support systems but has a reduced capacity when compared to water. Of the existing HTGRs, Fort Saint Vrain implemented an active, water-cooled RCCS [66], and HTTR, HTR-10, and HTR-PM implemented passive, air-cooled RCCSs [67, 68, 69]. Demonstrations for the Licensing Modernization Project using a pebble-bed HTGR have also implemented a passive air-cooled RCCS [70]. Therefore we assume:

A.19. The Reactor Cavity Cooling System (RCCS) is a passive, air-cooled design

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

An overview of an air-cooled RCCS is shown in Figure 14. Cool air enters the inlet duct, is heated inside the reactor cavity, rises, then exits via the outlet stack [65].

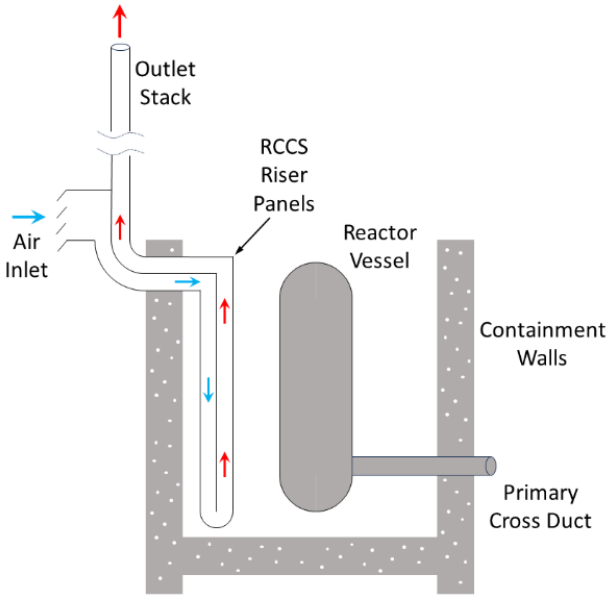

Figure 14. Air-Cooled RCCS [65]

The fundamental sensors necessary for RCCS operation are summarized in Table XXVIII [65, 67, 68, 69]. Although the RCCS is designed to utilize passive cooling, actuators may still be implemented for auxiliary functions and safety.

3.7. Steam Cycle Power Conversion System (SCPCS)

The primary functions of the Steam Cycle Power Conversion System (SCPCS) are:

F.SCPCS.1. Transfer heat from the primary loop to the secondary loop [71]

F.SCPCS.2. Residual heat removal during off-normal operation [71]

F.SCPCS.3. Generate electricity [71]

With the exception of HTTR, all previous HTGRs have used an SCPCS with steam as the secondary coolant [26]. Peach Bottom, Fort Saint Vrain, HTR-10, and HTR-PM all used Rankine cycles as their SCPCSs [72, 66, 36, 41]. The Xe-100 design plan also implement a Rankine cycle [73]. Therefore we assume:

A.20. The Steam Cycle Power Conversion System (SCPCS) implements 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 15. Thermal energy is transferred from the helium in the primary loop to the feedwater in the secondary 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.

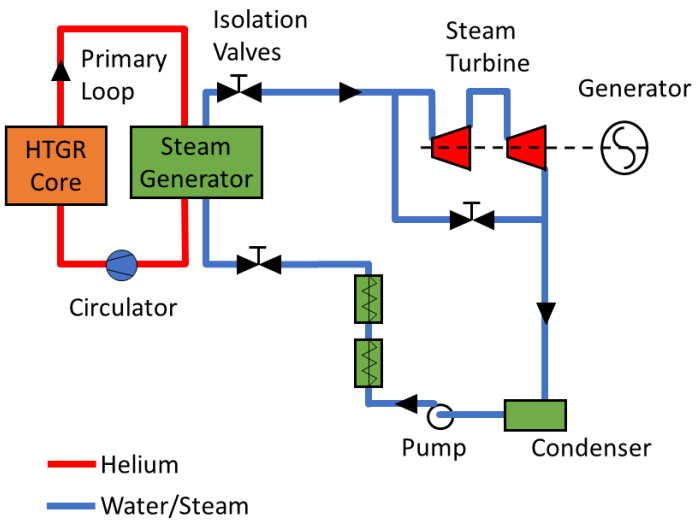

Figure 15. SCPCS Overview [71]

The fundamental sensors and actuators necessary for SCPCS operation are summarized in Table XXIX and Table XXX, respectively [74, 75, 76, 77].

3.8. Start-Up and Shutdown System (SSS)

The primary functions of the Start-Up and Shutdown System (SSS) are:

F.SSS.1. Provide forced cooling during plant start-up [78, 70]

F.SSS.2. Provide forced cooling during plant shut-down [78, 70]

F.SSS.3. Provide forced cooling in response to design basis events [78, 70]

There is little literature available to describe modern designs or implementations of the SSS. The functions described above and the remainder of this section were obtained using contextual evidence from Xe-100 tabletop exercises and Licensing Modernization Project (LMP) documentation [78, 70]. The fundamental sensors and actuators necessary for SSS operation are summarized in Table XXXI and Table XXXII, respectively.

3.9. Distributed Control System (DCS)

The primary function of the Distributed Control System (DCS) is:

F.DCS.1. Coordinate control actions between plant systems to maintain operations [56, 79]

F.DCS.2. Coordinate control actions between plant systems to transition the plant between states [56, 79]

The DCS is a supervisory control system that utilizes sensor data from multiple plant systems to coordinate actuation among those systems [79]. The high-level control approach planned for the Xe-100 plant is shown in Table IV. The fundamental sensors and actuators required for DCS operation are shown in Table XXXIII and Table XXXIV, respectively [56]. It is assumed that:

A.21. 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.21 is important for DCSA design because it informs the interdependencies between the DCS and other plant systems.

Table IV. DCS Control Approach [56]

Controlled Variable	Controlled Variable System	Manipulated Variable	Manipulated Variable System
SG Inlet Temperature	SCPCS	Control Rod Position	RCS
Main Steam Pressure	SCPCS	Helium Circulator Speed	HCS
Main Steam Temperature	SCPCS	Feed Pump Speed	SCPCS
Electrical Load	SCPCS	Turbine Throttle Valve Position	SCPCS

3.10. Investment Protection System (IPS)

The primary functions of the Investment Protection System (IPS) are:

F.IPS.1. Sense conditions that jeopardize the plant investment [56, 80, 79]

F.IPS.2. Protect the plant investment [56, 80, 79]

Although investment protection is a consideration in historical HTGR designs, the implementation of dedicated IPSs is relatively new [80, 79]. The IPS is intended to prevent the plant from reaching conditions necessary for Reactor Protection System (RPS) actuation [56]. Based on the Xe-100 design plan [56], it is assumed that:

A.22. The Investment Protection System (IPS) will take corrective action if a corrective action threshold is exceeded.

A.23. The Investment Protection System (IPS) will take protective action if a protective action threshold is exceeded.

There are several events which necessitate IPS corrective or protective action. The design basis events (DBEs) given in [56] are:

1. Turbine trip
2. Reactor trip
3. Single circulator shutdown
4. Loss of both circulators
5. Loss of steam generator feedwater flow
6. Loss of offsite power
7. Control rod withdrawal
8. Small HPB breach

9. Medium HPB breach
10. Steam generator tube rupture
11. Loss of nuclear island cooling water system
12. Feedwater and steam line breaks

These DBEs require monitoring of the plant parameters given in Table V [56]. The IPS trip criteria in Table V include the RPS trip criteria in Table VI. Table V also provides the corresponding IPS protective action for each plant parameter (Table 6 in [56]). The corrective IPS action for all trip criteria except high intermediate range start-up rate is to reduce reactor power (Table 2 in [56]). The IPS corrective action for high intermediate range start-up rate is to prevent control rod withdrawal (Table 2 in [56]).

Table V. IPS Trip Parameters and Response [56]

Plant Parameter to be Monitored	Parameter Origin	IPS – Feedwater & Main Steam Isolation and SG Dump	IPS – Turbine Bypass	IPS – Circulator Run Down	IPS – Power Reduction & Controlled Steam Dump
High helium pressure boundary pressure	HCS	X		X	X
Low helium pressure boundary pressure	HCS	X (isolation only)			X
High neutron flux	RCS				X
High intermediate range start-up rate	SSS				X
High helium pressure boundary humidity	HCS	X		X	X
High hot helium temperature	HCS				X
High cold helium temperature	HCS			X	X
High mass flow rate ratio of helium to water	HCS & SCPCS			X	X
Main breaker open	SCPCS		X		X
High turbine speed	SCPCS		X		X
High auxiliary bus frequency	SCPCS		X		X
Low auxiliary bus frequency	SCPCS		X		X
Manual trip	MCR	X	X	X	X

The fundamental sensors and actuators necessary for IPS operation are summarized in Table XXXV and Table XXXVI, respectively. Sensors IPS.S.1-15 either provide trip parameters to the IPS or are

used by the IPS to calculate trip parameters. Sensors IPS.S.16-30 are used to monitor actuation of plant systems by the IPS trip. It is assumed that:

A.24. The Investment Protection System (IPS) does not have independent actuators. The IPS provides signals to other plant systems that then respond by actuating.

Assumption A.24 is important for DCSA design because it informs the interdependencies between the IPS and other plant systems.

3.11. Reactor Protection System (RPS)

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

F.RPS.1. Sense design basis accident conditions [81, 82]

F.RPS.2. Prevent release of radionuclides in response to design basis accidents [81, 82]

To perform its functions, the RPS must detect an event that requires intervention and initiate the appropriate intervene [81]. The DBEs for RPS trip are identical to those for IPS action, with the exception of DBEs 1, 2, and 6. By definition, the thresholds for RPS trip are more extreme than those for IPS protective action [56]. The corresponding plant parameters to be monitored and the RPS responses are adopted from the Xe-100 design plan and are summarized in Table VI [56].

Table VI. RPS Trip Parameters and Response [56]

Trip Parameters to be Monitored	Parameter Origin	RPS – Control Rod Trip	RPS – Circulator Shutdown	RPS – Feedwater & Main Steam Isolation
High helium pressure boundary pressure	HCS	X		X
Low helium pressure boundary pressure	HCS	X		
High neutron flux	RCS	X		
High intermediate range start-up rate	SSS	X		
High helium pressure boundary humidity	HCS	X	X	X
High hot helium temperature	HCS	X		
High cold helium temperature	HCS	X	X	
High mass flow rate ratio of helium to water	HCS & SCPCS	X	X	
Manual trip	MCR	X	X	X

To comply with requirements for RPS reliability, redundancy, and independence [83, 84, 85, 86], the following requirements/assumptions are applied to each of the trip criteria in Table VI. These requirements are not exhaustive, but are a fundamental list pertinent to DCSA design [86, 56].

A.25. Four independent measurement channels are provided for each Reactor Protection System (RPS) trip criterion.

A.26. The Reactor Protection System (RPS) shall trip the reactor if two-out-of-four measurement channels exceed the allowable threshold.

A.27. No single failure will prevent the Reactor Protection System (RPS) from tripping the reactor.

A.28. 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 XXXVII and Table XXXVIII, respectively [81, 82, 56]. 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.29. The Reactor Protection System (RPS) has independent actuators to drop the control rods and the reserve shutdown rods.

A.30. The Reactor Protection System (RPS) provides trip signals to other plant systems that then respond by actuating.

Assumptions A.25 - A.30 are important for DCSA design because they inform the interdependencies between the RPS and other plant systems.

4. DCSA DESIGN PROCESS

This section describes the design process implemented for the HTGR DCSA. 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. Event trees are used as the basis for design constraints for the placement of systems into separate zones. These constraints are necessary to deny the adversary access to systems needed to cause scenarios that are unmitigated by plant SeBD features [18].

4.1. Security Levels

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 VII. Note that these SSC classifications may vary depending on the requirements of the specific HTGR design.

Table VII. HTGR 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	• SCPCS • HCS • FHS • SSS • SFSS • HTSS • Operations historian
	Non-safety related with special treatment	• IPS • DCS • RCCS • RCS • HPS
4	Safety-related	• RPS • RSS

4.2. Security Zones

This section describes how security zones are assigned to systems. First, event trees were used to examine the effects of the adversary compromising different combinations of functions along each event sequence of each event tree. This analysis was used to derive design constraints for separation of systems into different zones.

4.2.1. Event Tree Analysis

Event tree analysis is a top-down analysis approach that assesses the probability outcomes given an initiating event [6]. Figure 16 shows an HTGR small pressure boundary break event tree which describes the response systems, their probabilities of success/failure, and the corresponding licensing basis event (LBE) category for each event sequence. The LBE category is defined by the event sequence frequency (ESF) according to the values defined by the Licensing Modernization Project (LMP) given in The LBE categories and their ESF ranges are summarized in Table VIII. The ESF is measured in occurrences per plant-year and each LBE has a range of approximately two orders of magnitude.

Table VIII. The initiating event is a small break in the Helium Pressure Boundary (HPB) of less than or equal to 10mm in size. There is a 50% chance the break is in an isolable area of the system. The Operator Control System (OCS) can only maintain power operation if the break is isolable and trip conditions are not exceeded. It is highly likely that the reactor will then trip, though a small 0.001% chance of failure exists. The exemplar analysis provided for this event tree is quoted from a conference paper produced over the course of this research [18]. The additional analyses provided in Appendix C were not included in the conference paper.

The event tree follows that forced cooling will be more difficult to maintain if the break is not isolable. If the break is isolated, cooling system pump down is assured which will significantly limit the release of the radionucleotides in the coolant, otherwise there is an estimated 10% chance of failure to pump down the system. The last line of heat removal is the RCCS which has an exceptionally low estimated chance of failure. Finally, the event tree ends with the Reactor Building (RB) heating, ventilation, and air conditioning (HVAC) filtration which is the last line of defense against some of the radionucleotides escape to the environment.

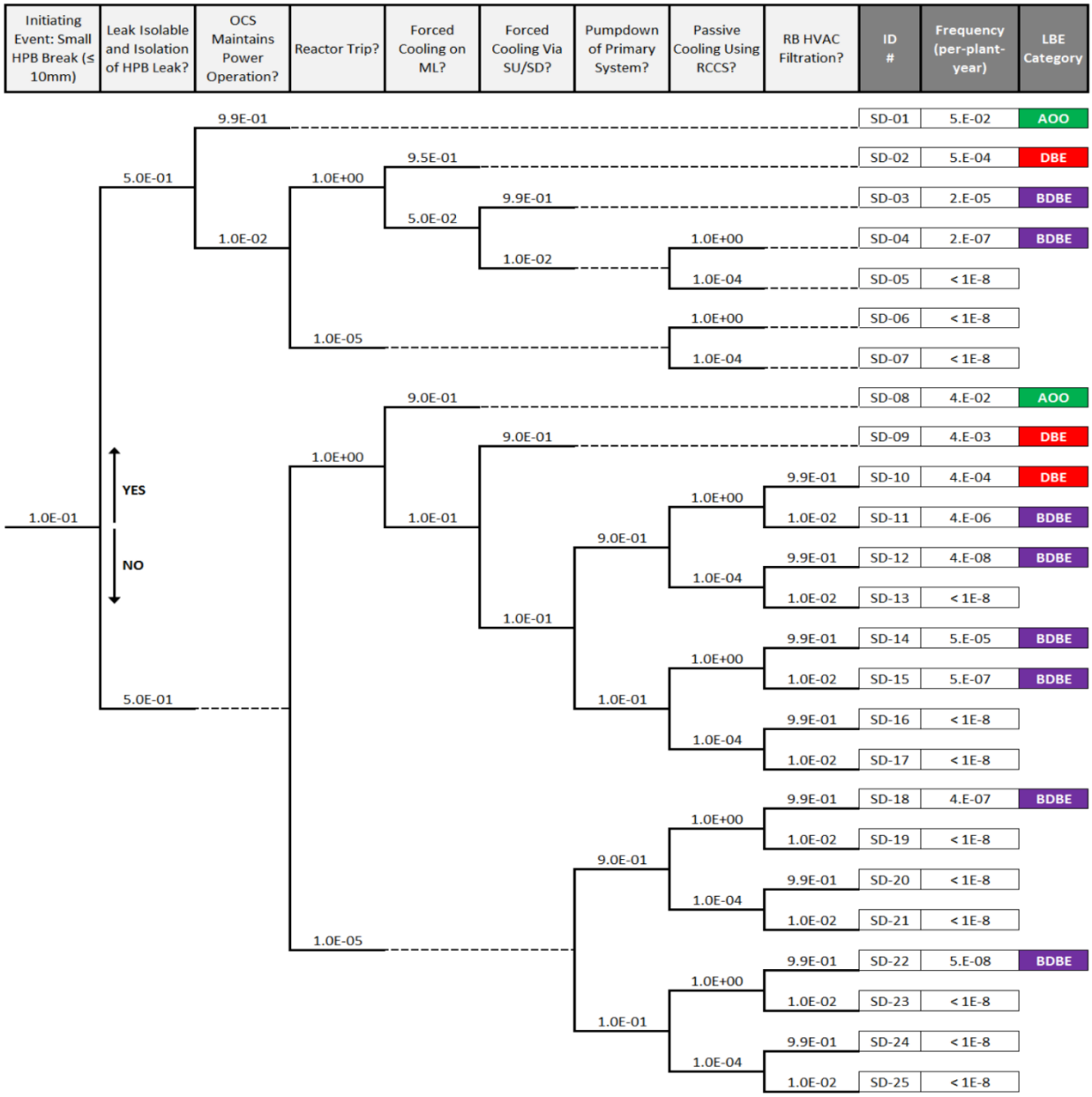

Figure 16. Small Helium Depressurization Event Tree with Associated LBEs [70]

The LBE categories and their ESF ranges are summarized in Table VIII. The ESF is measured in occurrences per plant-year and each LBE has a range of approximately two orders of magnitude.

Table VIII. LBE Category Definitions [23]

LBE Category	ESF Range
Anticipated Operational Occurrence (AOO)	ESF ≥ 1×10^{-2}/plant-year
Design Basis Event (DBE)	1×10^{-4}/plant-year ≤ ESF < 1×10^{-2}/plant-year
Beyond Design Basis Event (BDBE)	5×10^{-7}/plant-year ≤ ESF < 1×10^{-4}/plant-year
Incredible Event (IE)	ESF < 5×10^{-7}/plant-year

To identify how systems should be separated into DCSA zones, we first consider the impact of the adversary manipulating functions represented on the event tree in Figure 16. If the adversary has compromised the system performing a certain function, it is assumed that the adversary can cause the function to fail on-demand, therefore the probability of that function failing is changed to one. It is assumed that the adversary's manipulation of these functions does not affect the dose calculation for each of the event sequences, only the event sequence frequencies ESFs. For example, consider the manipulation of three functions:

1. **Reactor trip: changes ESF of SD-18**
   The RPS is responsible for monitoring the condition of the plant and initiating a shutdown if parameters exceed safe conditions. The system monitors sensors that may indicate power excursions, helium leaks, water ingress, fuel overheating, system over pressure, and loss of heat sink. When the RPS detects unsafe conditions, it releases the safety control rods into the core and sends a trip signal to other systems to correctly respond to the safe shutdown of the plant.
2. **Forced cooling via SU/SD: changes ESF of SD-14**
   The Start Up/Shut Down (SU/SD) system is a helium circulator and heat exchanger that is separate from the main circulator and steam generators. The purpose of the SU/SD system is to allow the reactor to slowly come to or down from operating temperatures to reduce thermal stresses in the fuel and structures of the core. Engaging the main circulators and steam generators at start up and shutdown would cause too great of a temperature differential on the inlet and outlet for the power level. This system also allows an emergency source of forced cooling for the core to manage decay heat.
3. **Passive cooling via the RCCS: changes ESF of SD-12**
   The RCCS is a passive cooling system that operates using natural convection to remove heat from the reactor cavity. The RCCS can be either air cooled, or water cooled. Air cooling allows for an unlimited coping period and requires no other support systems but has a reduced capacity when compared to water. Water cooling allows a greater heat rejection capacity, but the coping period is limited by the volume of water and the cooling support provided to the water tank by an auxiliary system.

The changes to the ESF of each event sequence are shown in Figure 17. Figure 17 shows the LMP frequency-consequence (F-C) target and the regions corresponding to AOOs, DBEs, and BDBEs as defined in The LBE categories and their ESF ranges are summarized in Table VIII. The ESF is measured in occurrences per plant-year and each LBE has a range of approximately two orders of magnitude.

Table VIII. The ESF of SD-14 increased by one order of magnitude when the forced cooling function performed by SU/SD was compromised. This increase in ESF moved SD-14 from the BDBE region to the DBE region. The ESF of SD-12 increased by four orders of magnitude when the passive cooling via RCCS was compromised. This increase in ESF moved SD-12 from below the BDBE region to the DBE region. Finally, the ESF of SD-18 was increased by five orders of magnitude when the reactor trip function was compromised. This increase in ESF moved SD-18 from below the BDBE region to the AOO region. The changes in ESF did not cause the LMP F-C target to be exceeded in any of the cases considered here, but still demonstrate the risk implications of a cyber-attack compromising certain system functions.

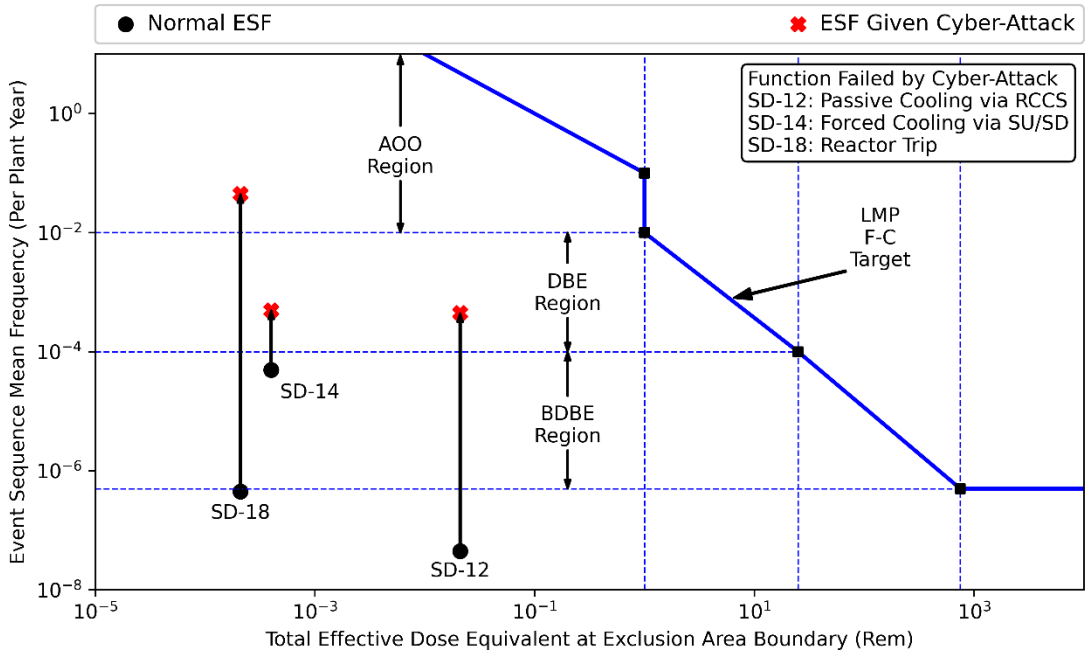

Figure 17. Event Sequences Plotted Against the LMP F-C Target [18]

For the purpose of DCSA design, we will consider only the manipulation of functions performed by control systems (i.e., not passive safety features or random events). Given this scope, an event tree was iteratively analyzed to identify the impact of an adversary compromising combinations of facility functions. If an adversary compromises a function, it is assumed that the event can be caused by the adversary at will rather than at the event frequency that is used in the event tree. The combinations of functions considered and the corresponding event sequences are given in Table IX. The final column of Table IX will be explained later in this section.

Table IX. Function Combination, Applicable Event Sequence IDs, and Greatest Change in Event Classification [18]

Function 1	Function 2	Event Sequence IDs	Greatest LBE Change
OCS Maintains Power	Forced Cooling on ML	SD-03	BDBE→AOO
Forced Cooling on ML	Forced Cooling Via SU/SD	SD-10, SD-11, SD-14, SD-15	DBE→AOO
Forced Cooling on ML	RB HVAC Filtration	SD-11, SD-15	BDBE→DBE
Forced Cooling Via SU/SD	RB HVAC Filtration	SD-11, SD-15	BDBE→DBE
Forced Cooling on ML	Pumpdown of Primary System	SD-14, SD-15	BDBE→DBE
Forced Cooling Via SU/SD	Pumpdown of Primary System	SD-14, SD-15	BDBE→DBE
RB HVAC Filtration	Pumpdown of Primary System	SD-15	BDBE→DBE

An example analysis is shown in Figure 18 for the combination of forced cooling on the main line and forced cooling via start-up/shut-down. The event sequences SD-10 and SD-11 have the same total effective dose equivalent of 2×10^{-4} Rem and the sequences SD-14 and SD-15 have the same total effective dose equivalent of 4×10^{-4} Rem, but are separated slightly along the horizontal axis for ease of viewing. For all four event sequences, the adversary's compromise of both forced cooling functions does not cause the LMP F-C target to be exceeded, however two BDBEs became as frequent as DBEs, and one DBE became as frequent as an AOO (and one sequence remained in the BDBE region). Similar figures for each of the function combinations in Table IX are provided in Appendix C.

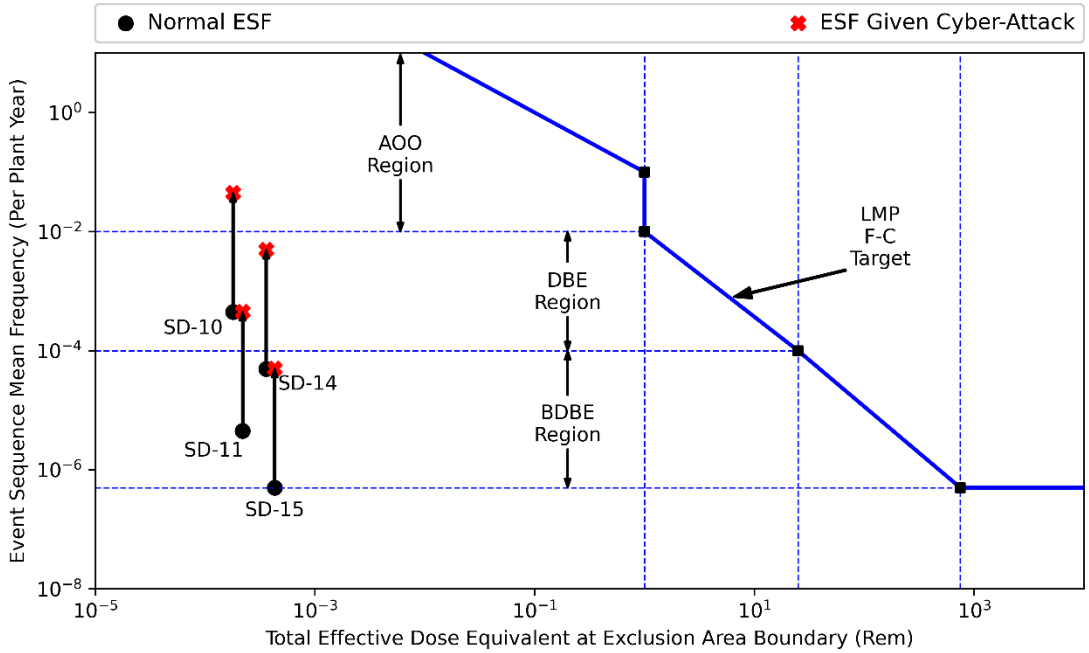

Figure 18. Event Sequences Plotted Against the LMP F-C Target for Forced Cooling on the Main Line and Via Start-Up/Shut-Down [18]

Analysis of the combinations of functions (and applicable event sequences) given in Table IX resulted in the outcomes given in the final column of Table IX. If the design objective is to not exceed the LMP F-C target, then this analysis indicates that the systems performing the pairs of function in Table IX may be grouped in the same DCSA zones without violating the design constraint. Further analysis would need to be performed for combinations of three functions to determine whether trios of systems could be placed in the same zones without violating the design constraint. If, instead, the design objective is to prevent event sequences categorized as DBEs or BDBEs from becoming as frequent as AOOs, then the results indicate that the OCS and forced cooling on the main line systems must be placed in separate zones and the forced cooling on the main line and forced cooling via start-up/shut-down must be placed in separate zones. Further iterations with more event sequences may result in additional design constraints.

5. HTGR DCSA DESIGN

This section provides the HTGR 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.

5.1. DCSA Template

The HTGR DCSA template is shown in Figure 19. 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), IPS, and DCS serve as supervisory controllers. Operators in the MCR may interface with the IPS and DCS. The IPS may also interface with the DCS. The relationships between the IPS, DCS, and their subordinate systems are discussed in Section 3. An architecture for a typical system is given in Figure 20. 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.

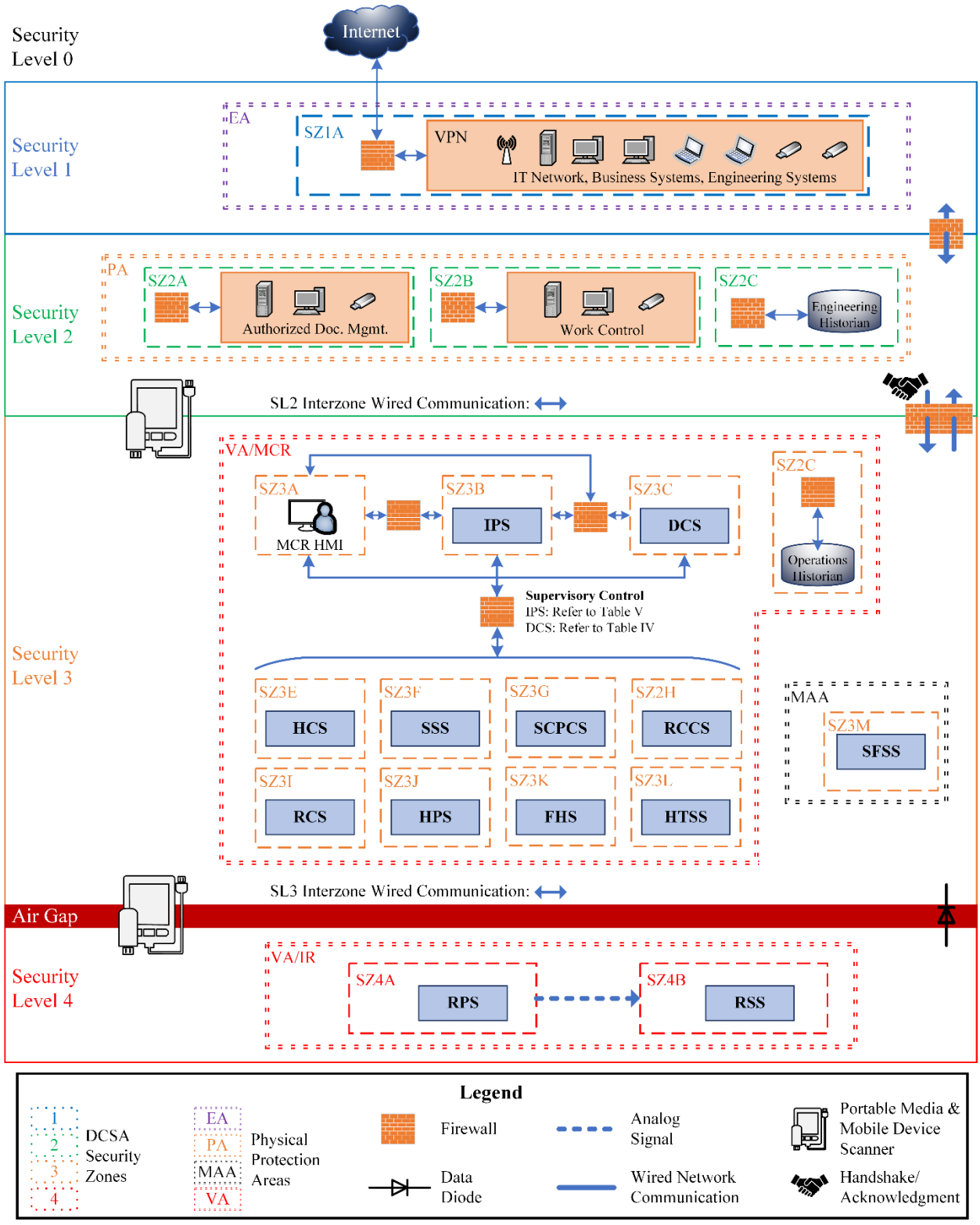

Figure 19. HTGR DCSA Template

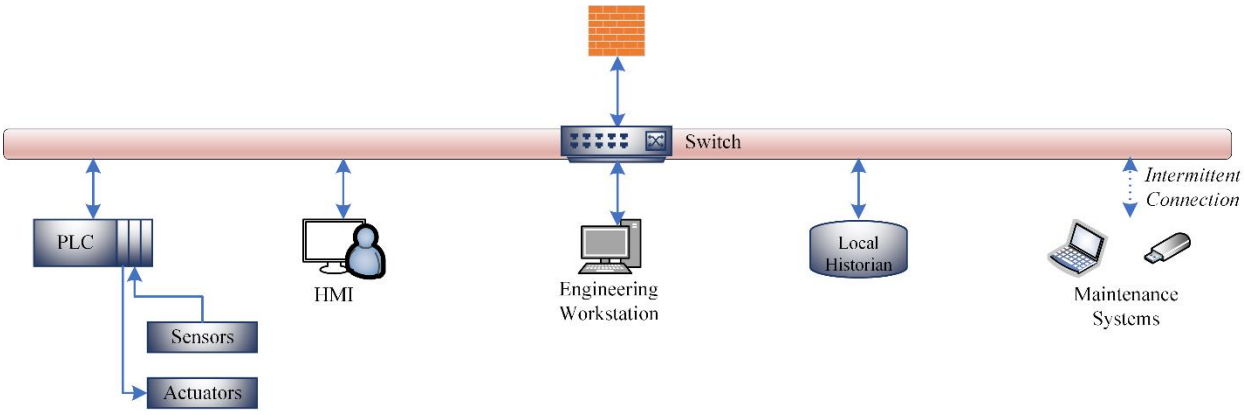

Figure 20. Example System Architecture

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

5.1.1. 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 SCPCS to command the RCS (Table IV). Without considering information dependencies, the SCPCS would belong to security level 2 and the DCS and RPS 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 SCPCS 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., SCPCS) in security level 2 rather than security level 3 [87, 88, 89]. 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.

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

Section 4.2 described a method for identifying DCSA zone design constraints using event trees. If all DBEs are analyzed in this manner, systems may be placed in the same zone if there is not an unacceptable change in 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 BDBE to DBE or 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.

5.2. Passive Cybersecurity Controls

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 and support a comprehensive cybersecurity framework designed to detect, prevent, and respond to cyber attacks.

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 connectivity, 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. 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.

5.2.1. 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 physical access requirements for 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: Restricted**
  Enforce strict technical controls that restrict access to only essential personnel through the use of multi-factor authentication and physical barriers. Eliminate unauthorized access possibilities by ensuring all systems are secure and monitored in real-time.

The controls outlined in Table X 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 X. Physical Access Attack Pathway Cybersecurity Controls

SL	Technical Controls	Operational Controls
Level 1	• Basic access control mechanisms such as user ID and password [B.1.5] • Logging of access to systems [B.2.2] • Limited physical access controls, such as keycard access [B.3.9]	• General awareness training on physical security and cybersecurity [C.2.4]
Level 2	• Limited functionality configuration to reduce vulnerabilities [B.5.3] • Physical security measures such as tamper-evident seals on significant devices [B.3.7] • Procedures to promptly identify and remove or disable any unauthorized physical connections or interfaces [B.1.18] • Use of automated labeling for information classification and protection [B.1.14] • Capability to compile audit records of physical access with correlated timestamps [B.2.12] • Secure session management and enforcement of session authenticity [B.3.18]	• Access limited to authorized personnel only [C.2.18] • Personnel security policies and procedures to ensure authorized access [C.2.1] • Screening and documenting security controls for third-party personnel [C.5.2] • Control and verify all entry/exit points to secure areas. Maintaining a list of, and issuing authorization credentials [C.5.4] • System maintenance policy and procedures which cover assets located in all security boundaries (owner-controlled area, protected area, vital area) [C.4.1]
Level 3	• Use physically separate network devices to create and maintain logical separation of Levels 3 and 4 from each other and other levels [B.3.3] • 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. [B.3.2]	• Regular personnel training and awareness programs on security protocols [C.2.1] • Locked doors with multi-factor authentication and biometric access [C.5.5] • Ensure CDAs have no unnecessary applications, functions, utilities, services, communication

SL	Technical Controls	Operational Controls
	• 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. [B.3.6] • Implement identification and authentication technology to verify individuals, processes, and devices physically interacting with CDAs [B.4.2]	capabilities, interfaces, or peripherals beyond those needed for safety, security and emergency preparedness functions [C.11.8]
Level 4	• Access control policies and procedures for CDAs [B.1.1] • Ensure physical security measures restricting access on CDAs to authorized personnel and ability to be tracked to specific individuals [B.4.4] • Network access control and monitoring for unauthorized access [B.1.15] • Enable ability to audit and account for access events [B.2.1]	• Configuration management for controlling changes to CDAs [C.11.2] • Confine all devices and networks to vital areas [C.5.5]

5.2.2. 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 wired connectivity requirements for each security level are specified below:

- **Security Level 1: Available**
  Implement policies to ensure that all wired connections are identified, documented, and monitored to provide basic connectivity for authorized systems. Ensure that any changes to wired connections are controlled and approved according to established policies.
- **Security Level 2: Controlled**
  Combine policy and technical controls to manage and monitor wired connections, ensuring only authorized devices are connected. Implement technical measures to log and alert on unauthorized connection attempts while maintaining oversight through established policies.
- **Security Level 3: Mitigated**
  Deploy advanced technical controls to actively prevent unauthorized connections, including network segmentation, encryption, and real-time monitoring. Ensure automatic detection and response mechanisms are in place to isolate and mitigate any security risks associated with wired connections.
- **Security Level 4: Restricted**
  Enforce stringent technical controls to restrict wired connectivity to essential systems only, using techniques like port security, intrusion detection, and strict access control lists.

Eliminate unauthorized wired connections by ensuring all systems are secured and continuously monitored.

The controls detailed in Table XI 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 XI. Wired Connectivity Attack Pathway Cybersecurity Controls

SL	Technical Controls	Operational Controls
Level 1	• Basic firewall configurations to allow only necessary traffic [B.3.9] • Implement basic network access control using MAC address locking and physical isolation [B.1.15] • Use of secure passwords and regular password changes for network devices [B.4.1] • Document specific actions allowed without authentication under controlled conditions [B.1.12] • Enforcing physical security measures for wiring closets and network hardware [B.3.7]	• Basic logging and monitoring of wired connections [C.11.1] • Establish and document awareness training for employees and contractors that address site-specific objectives, management expectations, roles, responsibilities, policies and procedures with the cybersecurity program [C.10.2] • Simplified incident response plans focusing on wired network breaches [C.8.2]
Level 2	• Use of VLANs to separate and control traffic between different network zones [B.3.13] • Application whitelisting to control software execution on networked devices [B.3.2] • Implementation of firewalls with strict filtering rules [B.3.9] • Implement alternative controls for proprietary protocols lacking visibility [B.1.20] • Defining list of auditable events and frequency of auditing for each identified auditable event [B.2.2]	• Routine network configuration reviews to identify and rectify vulnerabilities [C.11.3] • Implementation of automated tools for monitoring and logging network activity [C.3.5] • Scheduled training for personnel on secure network practices [C.2.1] • Ensure CDA software, firmware, and data protected from unauthorized changes when employing hardware access controls [C.3.7]
Level 3	• Network intrusion detection and prevention systems (IDPS) deployed at key points [B.3.5] • Restriction of network services to only those necessary for operations [B.5.3]	• Periodic testing and review of network security controls [C.6.2] • Implementation of least privilege principle for network access [C.2.2] • Regular network audits to ensure compliance with security policies [C.11.4]

SL	Technical Controls	Operational Controls
	• Secure boot mechanisms to prevent unauthorized modifications to network devices [B.5.7] • End-to-end encryption of all data transmitted over wired connections [B.3.7]	• Physical access control for network devices [C.5.6]
Level 4	• Strict network segmentation and isolation for critical systems [B.3.4] • Implementation of data diodes to enforce one-way data flows [B.3.11] • Use of secure communication protocols with mutual authentication [B.3.10]	• Rigorous change management procedures for network configurations [C.11.2] • Regular security assessments and validation of wired network integrity [C.13.1] • Strict access controls and auditing for physical access to network devices [C.5.6]

5.2.3. 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 wireless connectivity requirements for each security level are specified below:

- **Security Level 1: Available**
  Implement policies to ensure that all wireless connections are identified, documented, and monitored to provide basic connectivity where necessary. Ensure that wireless connectivity is only used where essential, with minimal security features to allow basic functionality.
- **Security Level 2: Controlled**
  Combine policy-driven and technical controls to manage and monitor wireless connections, ensuring only authorized devices can connect. Implement technical measures to secure wireless communications, such as encryption and authentication, while policies enforce strict usage guidelines.
- **Security Level 3: Mitigated**
  Wireless connectivity should be entirely prohibited to mitigate security risks. Any previous wireless infrastructure must be decommissioned, and all wireless communication capabilities must be removed or disabled.
- **Security Level 4: Eliminated**
  Enforce strict technical measures to eliminate all wireless connectivity options entirely. Ensure that no devices capable of wireless communication are present in critical areas, and implement continuous monitoring to detect and prevent any attempts to establish wireless connections.

The controls outlined in Table XII are designed to fortify the network environment, establish choke points, and enforcing 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 XII. Wireless Connectivity Attack Pathway Cybersecurity Controls

SL	Technical Controls	Operational Controls
Level 1	• Basic restriction of wireless access, including disabling wireless by default on all devices [B.3.6] • Require strong passwords and encryption on any wireless networks that are permitted in less critical areas [B.4.2]	• General guidelines limiting the use of wireless devices in less critical areas [C.5.5] • Establish procedures for monitoring wireless incidents [C.3.4]
Level 2	• Restricting wireless connectivity through group policies or device management software [B.3.16] • Whitelisting of devices and applications that are permitted to operate with wireless functionality disabled [B.3.18] • Treat wireless connections as outside security boundary and prohibit wireless for critical functions [B.1.17] • Implementation of physical and software barriers to ensure compliance with wireless restrictions [B.3.20]	• Routine checks for unauthorized wireless devices or access points in the facility [C.11.4] • Strict procedures for approving and documenting any temporary wireless access [C.5.4] • Limit permission to change wireless devices or access points to authorized personnel [C.11.6] • Awareness training for staff on the importance of wireless restrictions [C.2.4]
Level 3	• Disabling wireless drivers and software in the operating system on critical systems [B.5.4] • Use of firmware settings to permanently disable wireless capabilities [B.3.15] • Block all wireless protocols at the network level through firewalls and access points [B.3.14]	• Policy allowing wireless connectivity only with explicit, time-limited, and documented exceptions [C.5.1] • Training and awareness programs highlighting the risks and restrictions of wireless connectivity [C.2.1] • Implementation of RF shielding in sensitive areas or CDAs to prevent any wireless communications [C.5.6]
Level 4	• Physical removal of wireless hardware (e.g., Wi-Fi cards, Bluetooth modules) from critical systems [B.5.6]	• Policy enforcing a total ban on wireless devices in critical areas [C.5.2] • Rigorous access control procedures ensuring no wireless-enabled devices enter secured areas [C.5.3] • Regular security audits to ensure compliance with the no wireless policy [C.11.4]

5.2.4. 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 portable media requirements for each security level are specified below:

- **Security Level 1: Available**
  Implement policies to ensure that portable media usage is identified, documented, and monitored to allow basic functionality while minimizing risks. Establish guidelines for the acceptable use and handling of portable media, ensuring that data integrity and confidentiality are maintained.
- **Security Level 2: Controlled**
  Combine policy-driven and technical controls to manage and monitor the use of portable media, ensuring that only authorized devices are utilized and that all activities are logged. Implement technical measures such as encryption, malware scanning, and access control to secure data transferred via portable media.
- **Security Level 3: Mitigated**
  Prohibit the use of portable media to eliminate the associated security risks. Configure systems to prevent the connection or use of any portable media devices, effectively removing this as a potential attack vector.
- **Security Level 4: Restricted**
  Enforce strict technical measures to eliminate all possibilities of portable media usage. Disable all ports and interfaces that could allow portable media connections, ensuring continuous monitoring and preventing any attempts to re-enable these functions.

The controls detailed in Table XIII 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 XIII. Portable Media and Mobile Devices (PMMD) Attack Pathway Cybersecurity Controls

SL	Technical Controls	Operational Controls
Level 1	• Basic restrictions on media use, such as disabling USB ports [B.3.6] • Require use of passwords or PINs on media devices [B.4.2] • Require read-only access for non-authorized users [B.3.12] • Application of anti-malware solutions to scan media automatically [B.3.8] • Use of access control lists (ACLs) to restrict access to media contents [B.3.1] • 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 [B.1.19]	• General guidelines for proper handling and storage of portable media [C.1.7] • Basic awareness training for personnel on the risks of portable media [C.2.4] • Detailed procedures for handling, transporting, and disposing of portable media [C.1.4]
Level 2	• Implement alternative controls for proprietary protocols on portable devices [B.1.20] • Prohibit external systems from accessing CDAs in level 3 and 4 [B.1.22] • Defining list of auditable events and frequency of auditing for each identified auditable event [B.2.2]	• Routine checks for unauthorized media devices and connections [C.11.5] • Logging of all portable media usage [C.3.6] • Procedures for labeling and securing media when not in use [C.1.6] • Encrypt portable media containing sensitive information during transport outside controlled areas [C.1.2]
Level 3	• Controlled use of media with whitelisted devices and systems [B.3.16] • Implementation of secure file transfer protocols for data moving to/from portable media [B.3.19] • Implement secure key management practices for PMMD encryption keys [B.3.9] • Disabling access to PMMD by default, enabling only when necessary [B.3.14] • Mandatory encryption of all data on PMMD [B.3.20]	• Regular training for personnel on secure handling of PMMD [C.2.1] • Media handling procedures that include specific steps for sanitization and disposal [C.1.5]
Level 4	• Use of secure wipe tools to sanitize media before reuse [B.3.15] • Implementation of hardware-based write protection for media [B.3.17] • Disabling auto-run features on systems to prevent unauthorized execution from media [B.5.4] • Isolate security functions on PMMD to prevent cross-contamination between segments [B.5.6]	• Strict media control policies, including authorization and tracking of media usage [C.1.1] • Regular audits and inventories of portable media [C.1.3] • Continuous monitoring and logging of media access and use [C.11.7]

This page left blank

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 demonstrates the use of event trees to develop a DCSA design for an HTGR. 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 a high temperature, gas-cooled reactor (HTGR) 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.

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.

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] U.S. Nuclear Regulatory Commission, "Tutorial on Probabilistic Risk Assessment," in *P-101: Risk Informed Regulation for Tehcnical Staff*, Bethesda, MD.

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

[21] World Nuclear Association, "Safety Classification for I&C Systems in Nuclear Power Plants - Current Status and Difficulties," WNA, London, UK, 2020.

[22] International Atomic Energy Agency, "Safety of Nuclear Power Plants: Design," IAEA, Vienna, Austria, 2016.

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

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

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

[26] J. Beck and L. Pincock, "High Temperature Gas-Cooled Reactors Lessons Learned Applicable to the Next Generation Nuclear Power Plant," Idaho National Laboratory, Idaho Falls, ID, 2011.

[27] R. Simon and P. Capp, "Operating Experience with the DRAGON High Temperature Reactor Experiment," in *Proceedings of the Conference on High Temperature Reactors*, Vienna, Austria, 2002.

[28] J. Everett III and E. Kohler, "Peach Bottom Unit No. 1: A High Performance Helium Cooled Nuclear Power Plant," *Annals of Nuclear Energy,* vol. 5, no. 8-10, pp. 321-335, 1978.

[29] C. Marnet, M. Wimmers and U. Birkhold, "Decommissioning of the AVR Reactor, Concept for the Total Dismantling," in *Technical Committee Meeting on Technologies for Gas Cooled Reactor Decommissioning, Fuel Storage, and Waste Disposal*, Vienna, Austria, 1998.

[30] P. Pohl, "The Importance of the AVR Pebble-Bed Reactor for the Future of Nuclear Power," in *PHYSOR-2006*, Vancouver, Canada, 2006.

[31] D. Copinger and D. Moses, "Fort Saint Vrain Gas Cooled Reactor Operational Experience," U.S. Nuclear Regulatory Commission, Washington, DC, 2003.

[32] C. Fuller, "Fort Saint Vrain Operational Experience," in *Technical Committee Meeting on Design Requirements, Operation, and Maintenance of Gas-Cooled Reactors*, San Diego, CA, 1988.

[33] International Atomic Energy Agency (IAEA), "Current Status and Future Development of Modular High Temperature Gas Cooled Reactor Technology," International Atomic Energy Agency (IAEA), Vienna, Austria, 2001.

[34] S. Shiozawa, S. Fujikawa, T. Iyoku, K. Kunitomi and Y. Tachibana, "Overview of HTTR Design Features," *Nuclear Engineering and Design,* vol. 223, pp. 11-21, 2004.

[35] M. Ogawa and T. Nishihara, "Present Status of Energy in Japan and HTTR Project," *Nuclear Engineering and Design,* vol. 233, pp. 5-10, 2004.

[36] Z. Wu, D. Lin and D. Zhong, "The Design Features of the HTR-10," *Nuclear Engineering and Design,* vol. 218, pp. 25-32, 2002.

[37] M. Yao, R. Wang, Z. Liu, X. He and J. Li, "The Helium Purification System of the HTR-10," *Nuclear Engineering and Design,* vol. 218, pp. 163-167, 2002.

[38] W. Yuanqiang, D. Xingzhong, Z. Huizhong and H. Zhiyong, "Design and Tests for the HTR-10 Control Rod System," *Nuclear Engineering and Design,* vol. 218, pp. 147-154, 2002.

[39] H. Zhao, T. Liang, J. Zhang, J. He, Y. Zou and C. Tang, "Manufacture and Characteristics of Spherical Fuel Elements for the HTR-10," *Nuclear Engineering and Design,* vol. 236, pp. 643-647, 2006.

[40] Z. Zhang and S. Yu, "Future HTGR Developments in China After the Criticality of the HTR-10," *Nuclear Engineering and Design,* vol. 218, pp. 249-257, 2002.

[41] Z. Zhang, W. Z., Y. Sun and F. Li, "Design Aspects of the Chinese Modular High-Temperature Gas-Cooled Reactor HTR-PM," *Nuclear Engineering and Design,* vol. 236, pp. 485-490, 2006.

[42] Z. Zhang, Z. Wu, D. Wang, Y. Xu, Y. Sun, F. Li and Y. Dong, "Current Status and Technical Description of Chinese 2 x 250 MWth HTR-PM Demonstration Plant," *Nuclear Engineering and Design,* vol. 239, pp. 1212-1219, 2009.

[43] X-energy, "X-energy, LLC Xe-100 Topical Report: TRISO-X Pebble Fuel Qualification Methodology," US Nuclear Regulatory Commission, Rockville, MD, 2021.

[44] Kairos Power, "Fuel Qualification Methodology for the Kairos Power Fluoride Salt-Cooled High Temperature Reactor (KP-FHR)," US Nuclear Regulatory Commission, Rockville, MD, 2022.

[45] J. Saurwein, "TRISO Fuel Design, Properties, and Requirements," in *HTGR Technology Course for the Nuclear Regulatory Commission*, Idaho Falls, ID, 2010.

[46] C. Condon, P. Ivanusa, J. Whiting, P. Mirick, A. Bunn, C. Varnum-Lowry and P. Jensen, "Fate and Transport of Unruptured Tri-Structural Isotropic (TRISO) Fuel Particles in the Event of Environmental Release for Advanced and Micro Reactor Applications," *Journal of Environmental Radioactivity,* vol. 234, no. 106630, pp. 1-6, 2021.

[47] P. Demkowicz, B. Liu and J. Hunn, "Coated Particle Fuel: Historical Perspectives and Current Progress," *Journal of Nuclear Materials,* vol. 215, pp. 434-450, 2019.

[48] Z. Richter, E. Davidson, S. Skutnik and M. Munk, "Modeling and Simulation of an Xe-100 Type Pebble Bed Gas-Cooled Reactor with SCALE," Oak Ridge National Laboratory, Oak Ridge, TN, 2023.

[49] X-energy, "Xe-100 Licensing Topical Report Reactor Core Design Methods and Analysis," U.S. Nuclear Regulatory Commission, Bethesda, MD, 2024.

[50] P. Venter, "Pebble Bed HTGR Core Design Description," in *HTGR Technology Course for the Nuclear Regulatory Commission*, Idaho Falls, ID, 2010.

[51] P. Venter, "Pebble Bed HTGR Refueling Design," in *HTGR Technology Course for the Nuclear Regulatory Commission*, Idaho Falls, ID, 2010.

[52] Z. Han, H. Zhou, H. Zhang and D. Du, "A Detecting Method for Spherical Fuel Elements in a Pebble-Bed HTGR Using Eddy Current Detection," *NDT&E International,* vol. 79, pp. 81-91, 2016.

[53] J. Wang, Z. Zhang, B. Wu and Y. Li, "Design of the HTR-PM Spent Fuel Storage Facility," in *Proceedings of the HTR 2014*, Weihai, China, 2014.

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

[55] Z. Zhang and Y. Sun, "Economic Potential of Modular Reactor Nuclear Power Plants Based on the Chinese HTR-PM Project," *Nuclear Engineering and Design,* vol. 237, pp. 2265-2274, 2007.

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

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

[58] C. McDonald, M. Nichols and J. Kaufman, "Helium Circulator Design Concepts for the Modular High Temperature Gas-Cooled Reactor (MHTGR) Plant," in *International Gas Turbine Conference and Exhibition*, Anaheim, CA, 1986.

[59] H. Zhou and J. Wang, "Helium Circulator Design and Testing," *Nuclear Engineering and Design,* vol. 218, pp. 189-198, 2002.

[60] Y. Brits and J. Crowell, "X-Energy: Xe-100 Reactor the Key to an Integrated Energy System, Reliable Baseload, Agile Load Following, Industrial Applications," NICE Future, 2020.

[61] T. Furusawa, M. Shinozaki, S. Hamamoto and Y. Oota, "Cooling System Design and Structural Integrity Evaluation," *Nuclear Engineering and Design,* vol. 233, pp. 113-124, 2004.

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

[63] C. Fang, X. Bao, C. Yang, Y. Yang and J. Cao, "The R&D of HTGR High Temperature Helium Smapling Loop: From HTR-10 to HTR-PM," *Nuclear Engineering and Design,* vol. 306, pp. 192-197, 2016.

[64] O. Gastaldi, K. Liger, J. Robin and C. Poletiko, "Helium Purification," in *International Topical Meeting on High Temperature Reactor Technology*, Johannesburg, South Africa, 2006.

[65] L. Lommers, "Reactor Cavity Cooling System," in *HTGR Technology Course for the Nuclear Regulatory Commission*, Idaho Falls, ID, 2010.

[66] U.S. Department of Energy, "Fort St. Vrain Gas Cooled Reactor: Decommissioning Project Final Report," U.S. Department of Energy, Washington, DC, 1992.

[67] S. Takada, "Research and Development on Passive Cooling System," *Nuclear Engineering and Design,* vol. 233, pp. 185-195, 2004.

[68] Z. Yanhau, C. Zhipeng and Z. Han, "Preliminary Study on HTR-10 Operating at Higher Outlet Temperature," *Nuclear Engineering and Design,* vol. 397, no. 111958, 2022.

[69] Z. Zhang, Y. Dong, F. Li, X. Huang, Y. Zheng, Z. Dong, H. Zhang, Z. Chen and X. Li, "Loss-of-Cooling Tests to Verify Inherent Safety Feature in the World's First HTR-PM Nuclear Power Plant," *Joule,* vol. 8, no. 7, pp. 2146-2159, 2024.

[70] B. Waites, K. Fleming, F. Silday, A. Huning and J. Redd, "High Temperature, Gas-Cooled Pebble Bed Reactor Licensing Modernization Project Demonstration," Southern Company, Atlanta, GA, 2018.

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

[72] U.S. Atomic Energy Commission, "Peach Bottom Atomic Power Station: Final Safety Analysis Report," U.S. Atomic Energy Commission, Washington, DC, 1975.

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

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

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

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

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

[78] Southern Company, "Technology Inclusive Content of Application Project for Non-Light Water Reactors: X-energy Xe-100 TICAP Tabletop Exercise Report," U.S. Nuclear Regulatory Commission, Bethesda, MD, 2021.

[79] T. Wilson Jr., S. Ball, R. Wood, M. Cetiner and W. Poore, "Advanced Control and Protection System Design Methods for Modular HTGRs," Oak Ridge National Laboratory, Oak Ridge, TN, 2012.

[80] S. Ball, D. Holcomb and S. Cetiner, "HTGR Measurements and Instrumentation Systems," Oak Ridge National Laboratory, Oak Ridge, TN, 2012.

[81] D. Pfremmer, "Instrumentation and Controls (I&C) and Control Room Design," in *HTGR Technology Course for the Nuclear Regulatory Commission*, Idaho Falls, ID, 2010.

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

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

[84] 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.

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

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

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

[88] 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.

[89] 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.

[90] F. Silady, "HTGR Accident Analyses," in *HTGR Technology Course for the Nuclear Regulatory Commission*, Idaho Falls, ID, 2010.

This page left blank

APPENDIX A. VISUALIZATIONS OF DEFENSIVE STRATEGIES

This appendix provides visual representations of the fortification, choke-point, and access control defensive strategies based on the U.S. NRC's defense-in-depth concept shown in NEI 18-04 [23].

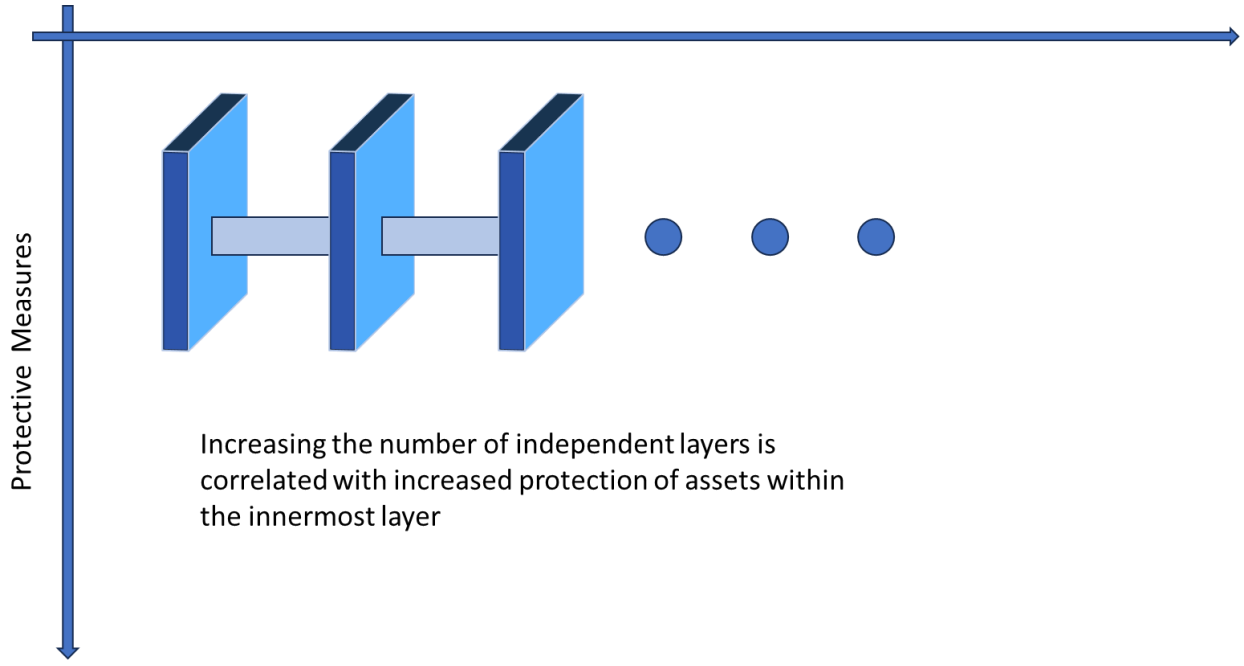

Figure 21. Fortification Defensive Strategy Applied to Multiple Layers

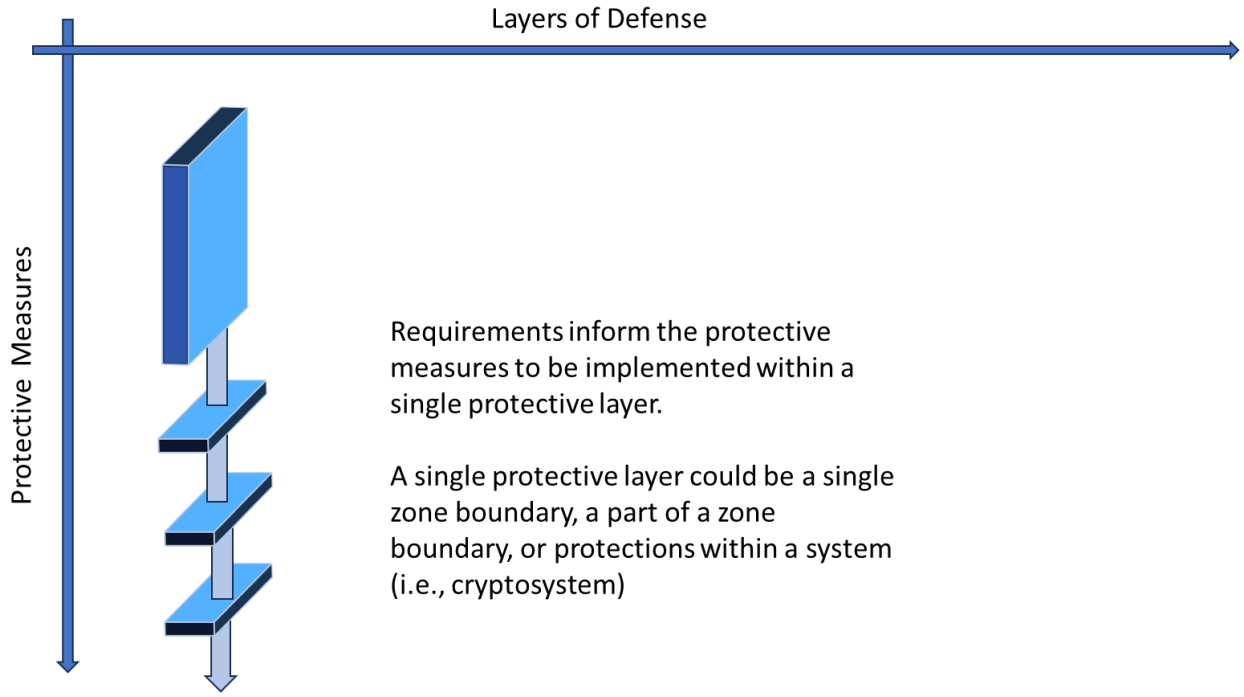

Figure 22. Fortification Defensive Strategy Applied Within an Individual Layer

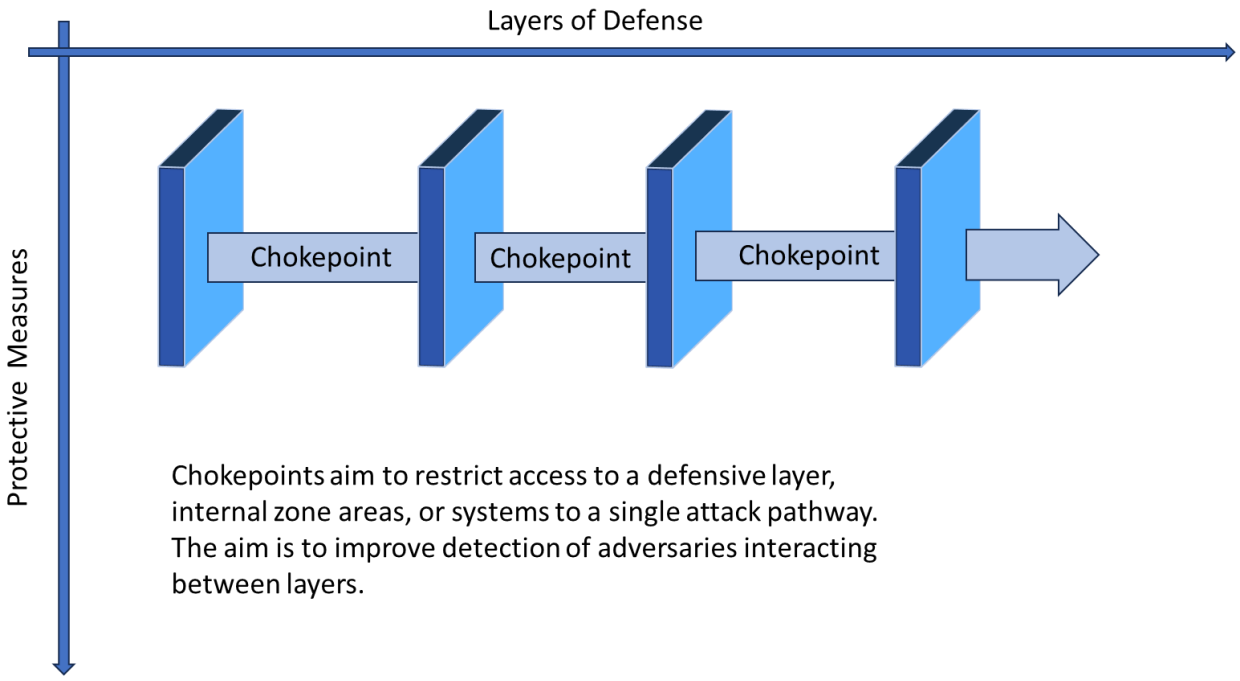

Figure 23. Chokepoint Defensive Strategy Applied Between Multiple Layers

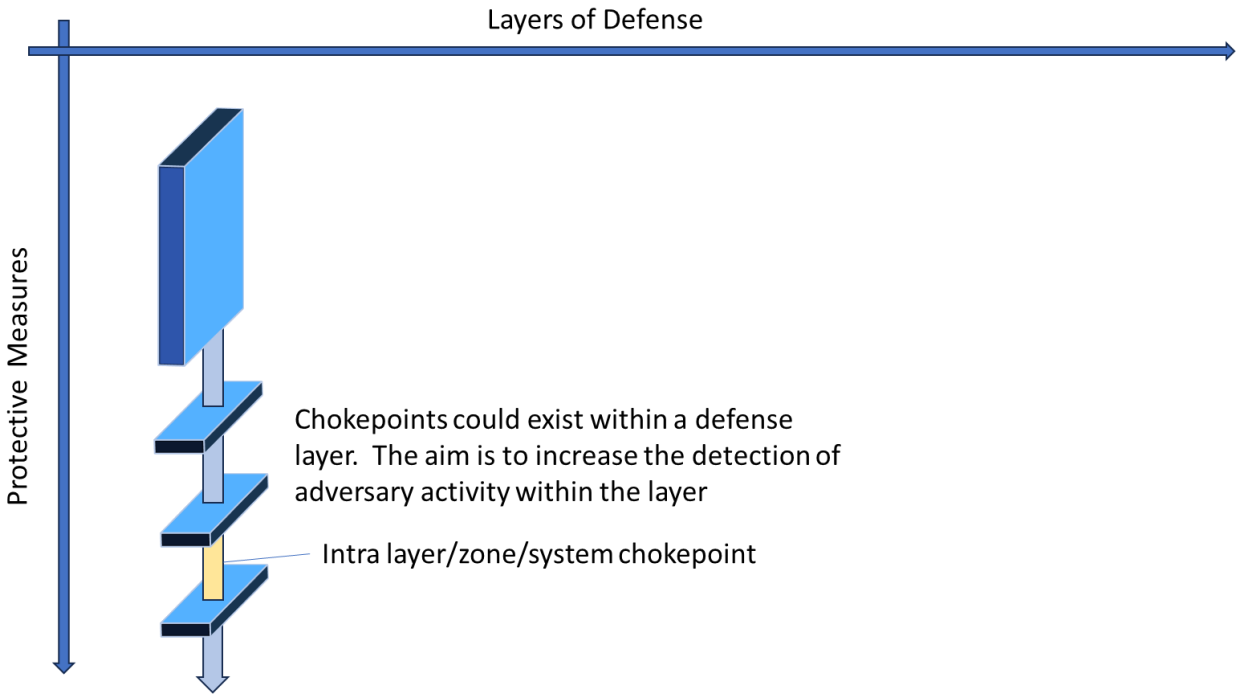

Figure 24. Chokepoint Defensive Strategy Applied Within an Individual Layer

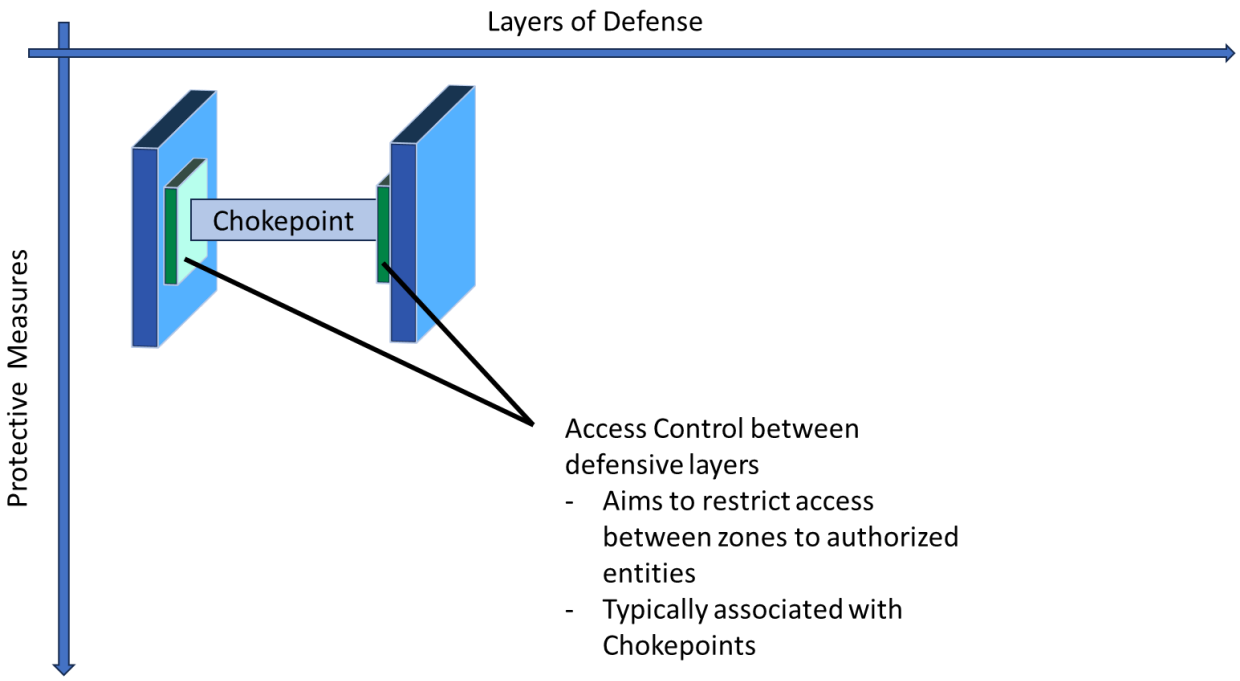

Figure 25. Access Control Defensive Strategy Applied Between Defensive Layers

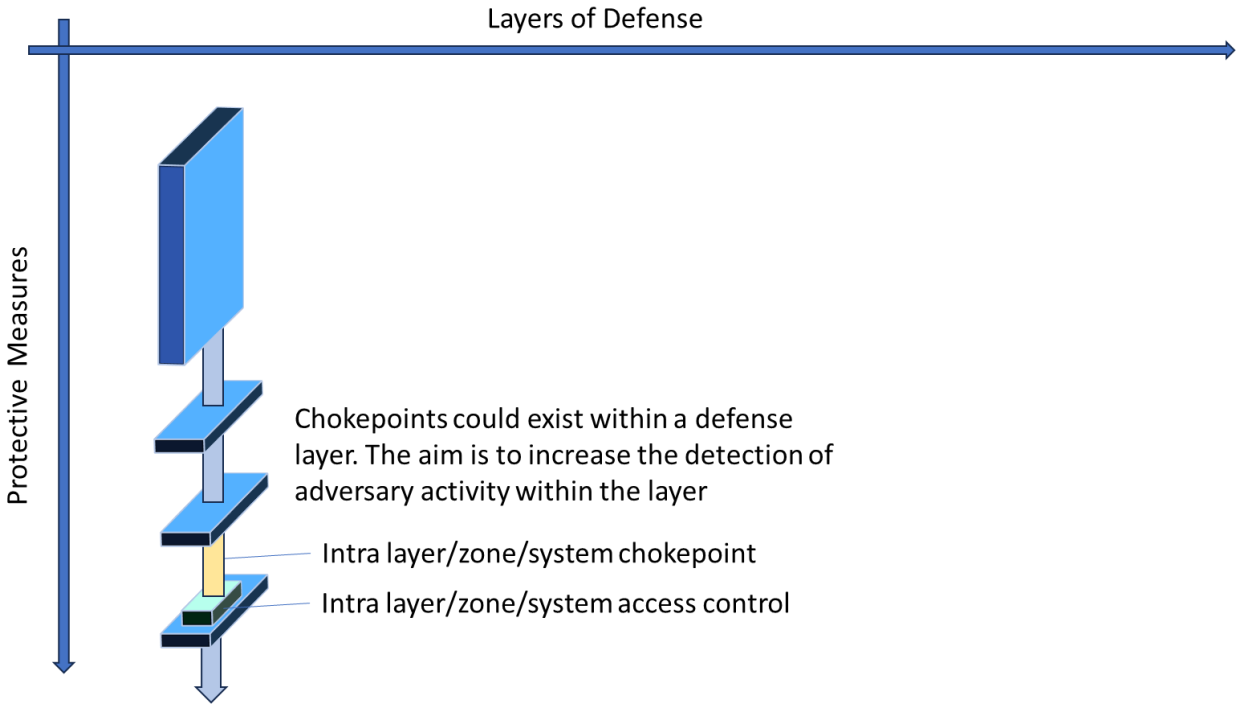

Figure 26. Access Control Defensive Strategy Applied Within an Individual Defensive Layer

This page left blank

APPENDIX B. HTGR FUNDAMENTAL SENSORS AND ACTUATORS

This appendix contains the tables of fundamental sensors and actuators necessary for operation of the HTGR 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 XIV. FHS Sensors

Sensor ID	Sensor Purpose
FHS.S.1	Measures sphere location along charging path
FHS.S.2	Measures sphere location in new sphere loading area
FHS.S.3	Measures sphere location in used sphere loading area
FHS.S.4	Measures extracted sphere for physical defects
FHS.S.5	Measures extracted sphere for burnup
FHS.S.6	Measures sphere location along discharge path

Table XV. FHS Actuators

Actuator ID	Actuator Purpose
FHS.A.1	Removes sphere from storage drum
FHS.A.2	Transits sphere through charging path
FHS.A.3	Deposits sphere from charging path to circulating circuit
FHS.A.4	Transits sphere to used sphere loading area
FHS.A.5	Transits sphere to new sphere loading area
FHS.A.6	Deposits sphere from used sphere loading area into the reactor
FHS.A.7	Deposits sphere from new sphere loading area into the reactor
FHS.A.8	Separates extracted unusable spheres from usable spheres
FHS.A.9	Transits unusable spheres from sphere separator to spent fuel storage
FHS.A.10	Transits usable spheres from sphere separator to circulating circuit

Table XVI. SFSS Sensors

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

Table XVII. SFSS Actuators

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

Table XVIII. RCS Sensors

Sensor ID	Sensor Purpose
RCS.S.1-9	Measures control rod position
RCS.S.10-18	Measures position of control rod release actuator
RCS.S.19	Measures neutron flux across core
RCS.S.20	Measures hot leg temperature
RCS.S.21	Measures cold leg temperature
RCS.S.22	Measures helium flow rate

Table XIX. RCS Actuators

Actuator ID	Actuator Purpose
RCS.A.1-9	Manipulates position of control rods
RCS.A.10-18	Releases control rods

Table XX. RSS Sensors

Sensor ID	Sensor Purpose
RSS.S.1-9	Measures reserve shutdown rod position
RSS.S.10-18	Measures position of reserve shutdown rod release actuator

Table XXI. RSS Actuators

Actuator ID	Actuator Purpose
RSS.A.1-9	Releases reserve shutdown rods

Table XXII. HCS Sensors

Sensor ID	Sensor Purpose
HCS.S.1	Measures helium temperature at reactor inlet
HCS.S.2	Measures helium temperature at reactor outlet
HCS.S.3	Measures helium flow rate
HCS.S.4-5	Measures speed of helium circulators
HCS.S.6-7	Measures vibration of helium circulators

Table XXIII. HCS Actuators

Actuator ID	Actuator Purpose
HCS.A.1-2	Helium circulators

Table XXIV. HPS Sensors

Sensor ID	Sensor Purpose
HPS.S.1	Measures chemical contaminants in helium
HPS.S.2	Measures radionuclide contaminants in helium

Sensor ID	Sensor Purpose
HPS.S.3	Measures moisture in helium
HPS.S.4	Measures helium pressure in purification loop
HPS.S.5	Measures helium flow rate in purification loop
HPS.S.6	Measures helium compressor speed
HPS.S.7	Measures helium compressor vibration

Table XXV. HPS Actuators

Actuator ID	Actuator Purpose
HPS.A.1	Control helium pathway through contaminant filters
HPS.A.2	Control helium pathway through moisture removal system
HPS.A.3	Helium compressor

Table XXVI. HTSS Sensors

Sensor ID	Sensor Purpose
HTSS.S.1	Measures helium pressure in primary loop
HTSS.S.2	Measures helium pressure in high pressure supply tanks
HTSS.S.3	Measures helium pressure in storage tanks
HTSS.S.4	Measures position of helium control valve to storage tanks
HTSS.S.5	Measures position of helium control valve to high pressure supply tanks
HTSS.S.6	Measures position of helium control valve to auxiliary plant services
HTSS.S.7	Measures position of helium control valve to primary loop
HTSS.S.8	Measures speed of pump into HTSS
HTSS.S.9	Measure vibration of pump into HTSS
HTSS.S.10	Measures speed of pump from storage tanks
HTSS.S.11	Measure vibration of pump from storage tanks
HTSS.S.12	Measures speed of pump from high pressure supply tanks
HTSS.S.13	Measure vibration of pump from high pressure supply tanks

Table XXVII. HTSS Actuators

Actuator ID	Actuator Purpose
HTSS.A.1	Control helium pathway to storage tanks
HTSS.A.2	Control helium pathway to high pressure supply tanks
HTSS.A.3	Control helium pathway from high pressure storage tanks to auxiliary plant services
HTSS.A.4	Control helium pathway to primary loop
HTSS.A.4	Pump helium from primary loop into HTSS
HTSS.A.5	Pump helium from storage tanks into primary loop

Actuator ID	Actuator Purpose
HTSS.A.6	Pump helium from high pressure supply tanks into auxiliary plant services

Table XXVIII. RCCS Sensors

Sensor ID	Sensor Purpose
RCCS.S.1	Measures temperature of air at inlet
RCCS.S.2	Measures temperature of air at outlet
RCCS.S.3	Measures air flow rate
RCCS.S.4	Measures air pressure at inlet
RCCS.S.5	Measures air pressure at outlet
RCCS.S.6	Measures air humidity at inlet
RCCS.S.7	Measures air humidity at outlet

Table XXIX. 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
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

Sensor ID	Sensor Purpose
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 XXX. 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 XXXI. SSS Sensors

Sensor ID	Sensor Purpose
SSS.S.1	Measures SSS coolant temperature at reactor inlet
SSS.S.2	Measures SSS coolant temperature at reactor outlet
SSS.S.3	Measures SSS coolant pressure
SSS.S.4	Measures SSS coolant flow rate
SSS.S.5	Measures speed of SSS coolant forcing actuator
SSS.S.6	Measures vibration of SSS coolant forcing actuator
SSS.S.7	Measures position of SSS coolant control valve
SSS.S.8	Measures position of SSS isolation valve

Table XXXII. SSS Actuators

Actuator ID	Actuator Purpose
SSS.A.1	Forces coolant (e.g., pump or circulator)
SSS.A.2	SSS coolant control valve
SSS.A.3	SSS isolation valve

Table XXXIII. DCS Sensors

Sensor ID	Sensor Purpose
DCS.S.1	Measures helium temperature at steam generator inlet
DCS.S.2	Measures main steam pressure

Sensor ID	Sensor Purpose
DCS.S.3	Measures main steam temperature
DCS.S.4	Measures electrical load
DCS.S.5-13	Measures control rod position
DCS.S.14-15	Measures speed of helium circulators
DCS.S.16-17	Measures vibration of helium circulators
DCS.S.18	Measures feedwater pump speed
DCS.S.19	Measures vibration of feedwater pump
DCS.S.20	Measures feedwater isolation valve position
DCS.S.21	Measures feedwater control valve position
DCS.S.22	Measures turbine throttle valve position

Table XXXIV. DCS Actuators

Actuator ID	Actuator Purpose
DCS.A.1-9	Manipulates position of control rods (RCS.A.1-9)
DCS.A.10-11	Helium circulators (HCS.A.1-2)
DCS.A.12	Feedwater pump (SCPCS.A.6)
DCS.A.13	Feedwater isolation valve (SCPCS.A.2)
DCS.A.14	Feedwater control valve (SCPCS.A.3)
DCS.A.15	Turbine throttle valve (SCPCS.A.4)

Table XXXV. IPS Sensors

Sensor ID	Sensor Purpose
IPS.S.1	Measures helium pressure boundary pressure
IPS.S.2	Measures neutron flux
IPS.S.3	Measures intermediate range start-up rate
IPS.S.4	Measures helium pressure boundary humidity
IPS.S.5	Measures hot helium temperature
IPS.S.6	Measures cold helium temperature
IPS.S.7	Measures helium flow rate
IPS.S.8	Measures feedwater flow rate
IPS.S.9	Measures main breaker position
IPS.S.10	Measures turbine speed
IPS.S.11	Measures auxiliary bus frequency
IPS.S.12	Measures feedwater isolation valve position
IPS.S.13	Measures main steam isolation valve position
IPS.S.14	Measures steam flow rate at the steam generator outlet

Sensor ID	Sensor Purpose
IPS.S.15	Measures steam pressure in the steam generator
IPS.S.16	Measures turbine bypass valve position
IPS.S.17	Measures turbine speed
IPS.S.18	Measures helium flow rate
IPS.S.19	Measures helium pressure
IPS.S.20-21	Measures circulator speed
IPS.S.22-30	Measures control rod position

Table XXXVI. IPS Actuators

Actuator ID	Actuator Purpose
IPS.A.1	Main steam isolation valve (SCPCS.A.1)
IPS.A.2	Feedwater isolation valve (SCPCS.A.2)
IPS.A.3	Steam generator dump valve (SCPCS.A.8)
IPS.A.4	Turbine bypass valve (SCPCS.A.5)
IPS.A.5-6	Helium circulators (HCS.A.1-2)
IPS.A.7-15	Manipulates control rod position (RCS.A.1-9)

Table XXXVII. RPS Sensors

Sensor ID	Sensor Purpose
RPS.S.1-4	Measures helium pressure boundary pressure
RPS.S.5-8	Measures neutron flux
RPS.S.9-12	Measures intermediate range start-up rate
RPS.S.13-16	Measures helium pressure boundary humidity
RPS.S.17-20	Measures hot helium temperature
RPS.S.21-24	Measures cold helium temperature
RPS.S.25-28	Measures helium flow rate
RPS.S.29-32	Measures feedwater flow rate
RPS.S.33-41	Measures control rod position
RPS.S.42-50	Measures position of control rod release actuator
RPS.S.51-59	Measures reserve shutdown rod position
RPS.S.60-68	Measures position of reserve shutdown rod release actuator
RPS.S.69-70	Measures speed of helium circulators
RPS.S.71	Measures main steam isolation valve position
RPS.S.72	Measures feedwater isolation valve position

Table XXXVIII. RPS Actuators

Actuator ID	Actuator Purpose
RPS.A.1-9	Releases reserve shutdown rods (RSS.A.1-9)
RPS.A.10-18	Releases control rods (RCS.A.10-18)
RPS.A.19-20	Helium circulators (HCS.A.1-2)
RPS.A.21	Main steam isolation valve (SCPCS.A.1)
RPS.A.22	Feedwater isolation valve (SCPCS.A.2)

APPENDIX C. SMALL HELIUM DEPRESSURIZATION EVENT TREE ANALYSIS FOR COMPROMISE OF TWO FUNCTIONS

This appendix contains additional figures for the analysis of the small helium depressurization event tree discussed in Section 4.2.1 and shown in Figure 16. For completeness, Figure 18 is reproduced as Figure 27 below.

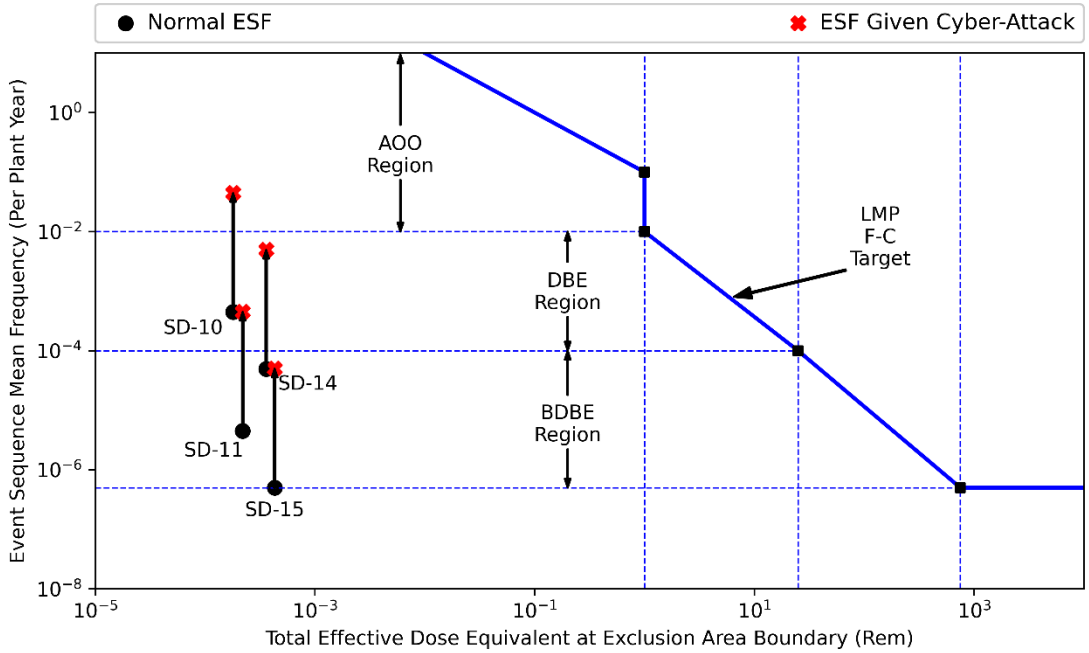

Figure 27. Event Sequences Plotted Against the LMP F-C Target for Forced Cooling on the Main Line and Via Start-Up/Shut-Down [18]

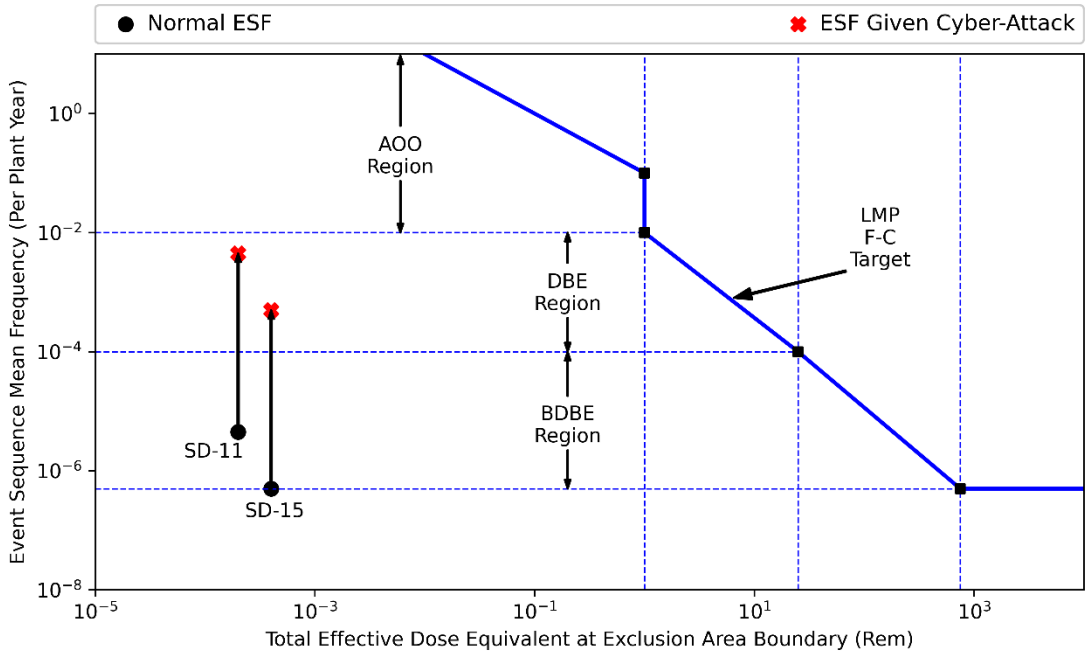

Figure 28. Event Sequences Plotted Against the LMP F-C Target for Forced Cooling on the Main Line and Reactor Building HVAC Filtration

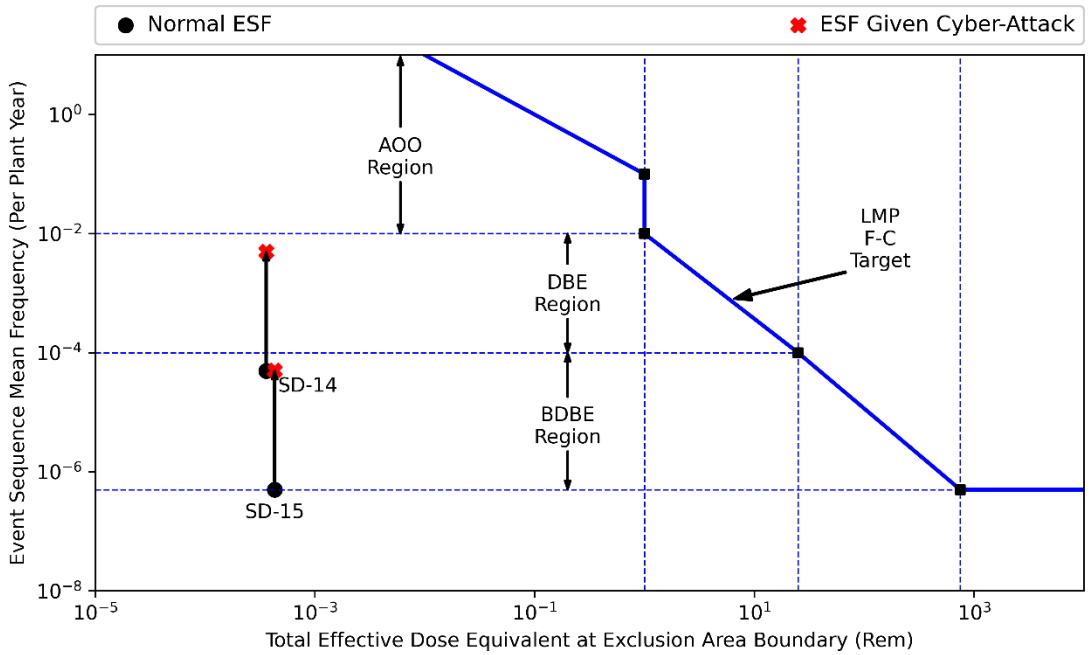

Figure 29. Event Sequences Plotted Against the LMP F-C Target for Forced Cooling on the Main Line and Pumpdown of Primary System

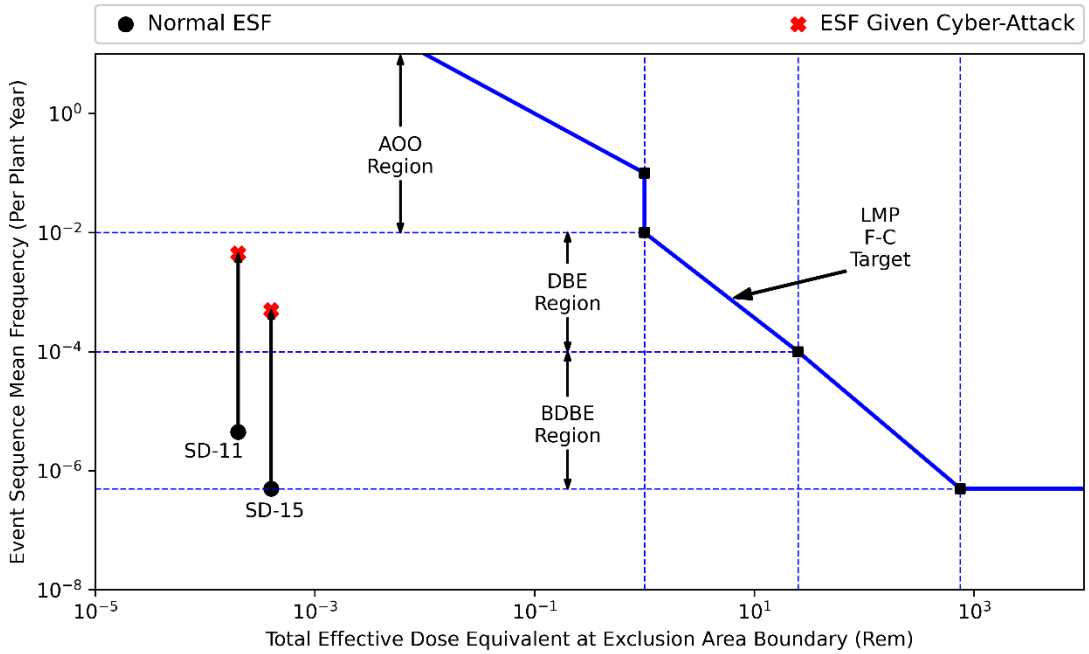

Figure 30. Event Sequences Plotted Against the LMP F-C Target for Forced Cooling Via Start-Up/Shut-Down and Reactor Building HVAC Filtration

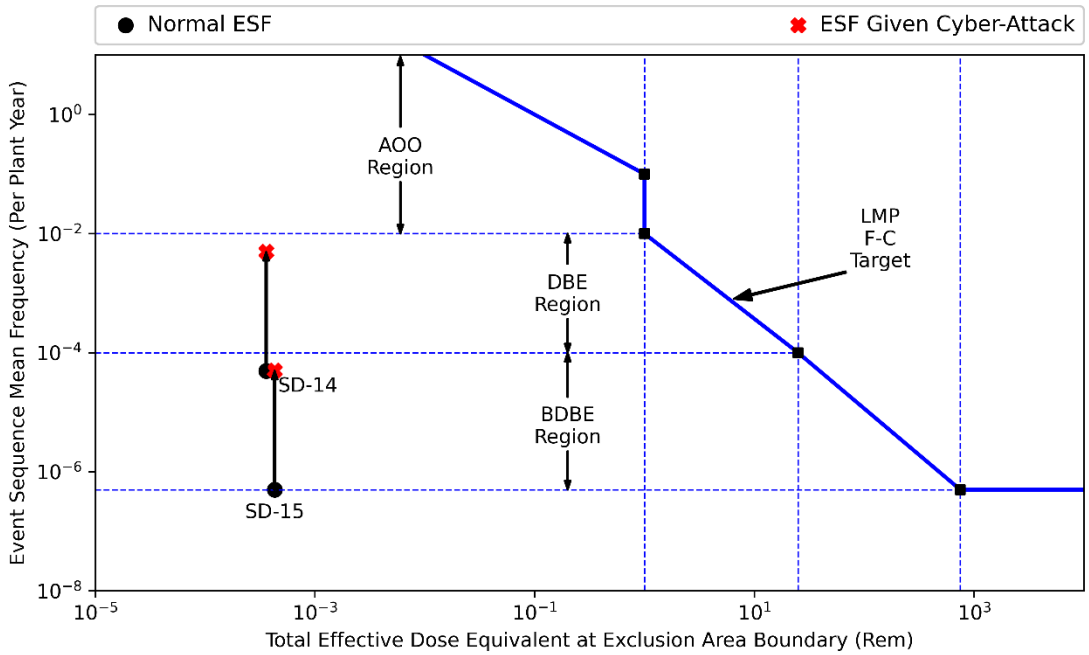

Figure 31. Event Sequences Plotted Against the LMP F-C Target for Forced Cooling Via Start-Up/Shut-Down and Pumpdown of Primary System

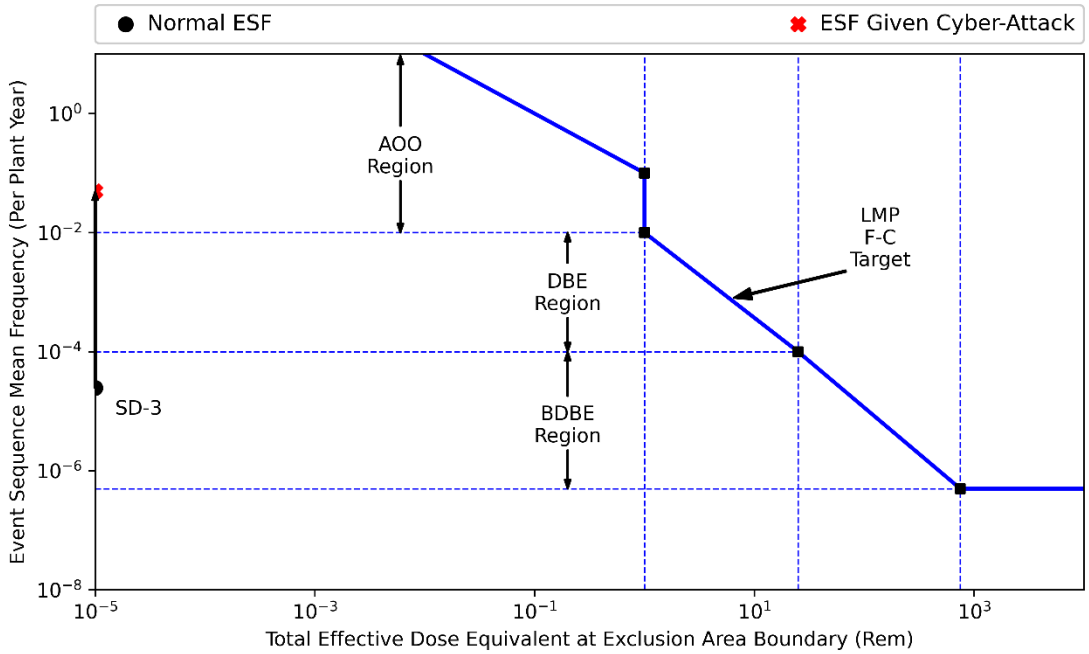

Figure 32. Event Sequences Plotted Against the LMP F-C Target for Forced Cooling on the Main Line and Operational Control System Maintains Power

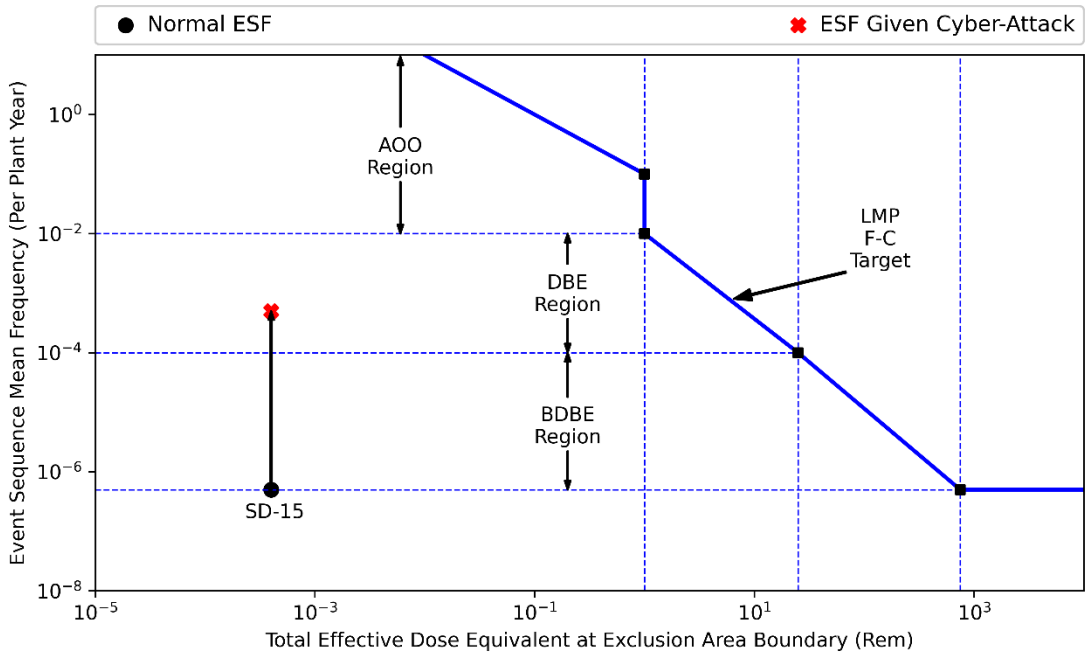

Figure 33. Event Sequences Plotted Against the LMP F-C Target for Pumpdown of Primary System and Reactor Building HVAC Filtration

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
Andrew S. Hahn	8851	ashahn@sandia.gov
Lee T. Maccarone	8851	lmaccar@sandia.gov
Michael T. Rowland	8851	mtrowla@sandia.gov
J. Connor Grady	88011	jcgrady@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Katya Le Blanc	katya.leblanc@inl.gov	INL
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.