U.S. NUCLEAR REGULATORY COMMISSION

DRAFT REGULATORY GUIDE DG-5075

Proposed new Regulatory Guide 5.96, Revision 0

Issue Date: October 2024
Technical Leads: Ismael Garcia and Tammie Rivera

ESTABLISHING CYBERSECURITY PROGRAMS FOR COMMERCIAL NUCLEAR PLANTS LICENSED UNDER 10 CFR PART 53

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes a method that the U.S. Nuclear Regulatory Commission (NRC) staff deems acceptable for complying with the Commission's regulations for establishing, implementing, and maintaining a cybersecurity program at commercial nuclear plants that would be licensed under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 53, "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants" (Ref. [1]), subject to the requirements in 10 CFR 73.110, "Technology inclusive requirements for protection of digital computer and communication systems and networks" (Ref. [2]). Licensees may use methods other than those described in this guide to meet the Commission's regulations if such methods satisfy the stated regulatory requirements.

Applicability

This RG applies to applicants and holders of a license under the provisions of 10 CFR Part 53 and 10 CFR 73.110.

Applicable Regulations and Orders

- 10 CFR Part 53 provides an alternative risk-informed and technology-inclusive regulatory framework for the licensing, construction, operation, and decommissioning of commercial nuclear plants.
    - 10 CFR 53.860, "Security programs," contains the requirements for establishing and maintaining a physical protection program that provides reasonable assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety.

This RG is being issued in draft form to involve the public in the development of regulatory guidance in this area. It has not received final staff review or approval and does not represent an NRC final staff position. Public comments are being solicited on this RG and its associated regulatory analysis. Comments should be accompanied by appropriate supporting data. Comments may be submitted through the Federal-rulemaking website, http://www.regulations.gov, by searching for draft regulatory guide DG-5075. Alternatively, comments may be submitted to Office of the Secretary, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Rulemakings and Adjudications Staff. Comments must be submitted by the date indicated in the *Federal Register* notice.

Electronic copies of this RG, previous versions of RGs, and other recently issued guides are available through the NRC's public website under the Regulatory Guides document collection of the NRC Library at https://www.nrc.gov/reading-rm/doc-collections/reg-guides/index.html. The RG is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML22199A257. The regulatory analysis is associated with a rulemaking and may be found in ADAMS under Accession No. ML24095A166.

- 10 CFR 53.860(d) requires licensees to have a cybersecurity program under 10 CFR 73.110 or 10 CFR 73.54, "Protection of digital computer and communication systems and networks."

- 10 CFR 53.860(e) requires the licensee to have an information protection system under 10 CFR 73.21, 73.22, and 73.23, as applicable.

- 10 CFR 53.1565(d)(4) contains the requirements for making modifications to the security programs and associated plans.

- 10 CFR Part 73, "Physical Protection of Plants and Materials," prescribes requirements for the establishment and maintenance of a physical protection system (PPS) that will be capable of protecting special nuclear material at fixed sites and in transit, as well as at plants that use special nuclear material.

  - 10 CFR 73.1, "Purpose and scope," describes the design-basis threats that must be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material.

  - 10 CFR 73.54, "Protection of digital computer and communication systems and networks," establishes the requirements for cybersecurity at operating power reactors and combined license applicants.

  - 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," contains the requirements for establishing and maintaining a physical protection program that provides high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety.

  - 10 CFR 73.77, "Cyber security event notifications," stipulates the types of cyberattacks that require notification to the NRC, the time requirements for making the notifications, how licensees should make the notifications, and how to submit follow-up written reports to the NRC.

  - 10 CFR 73.100, "Technology inclusive requirements for physical protection of licensed activities at commercial nuclear plants against radiological sabotage," establishes physical security requirements for commercial nuclear plants licensed under 10 CFR Part 53.

  - 10 CFR 73.110, "Technology inclusive requirements for protection of digital computer and communication systems and networks," contains the requirements for a cybersecurity program for commercial nuclear plants licensed under 10 CFR Part 53 that provides reasonable assurance that digital computers and communication systems and networks are adequately protected against cyberattacks. Compliance with this regulation is the focus of this RG.

- NRC Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," dated February 25, 2002 (Ref. [3]), identifies the perceived threat environment that arises from computer and communication networks for safety and security vulnerabilities, including modem access vulnerabilities, as of the order's issue date.

- NRC Order EA-03-086, "Design Basis Threat for Radiological Sabotage," dated April 29, 2003 (Ref. [4]), in part, requires licensees to address additional cyberattack characteristics.

Historically, the Commission has issued a series of security orders (e.g., EA-02-026 and EA-03-086) to reactor licensees describing the protection of electronic devices and computer networks from cybersecurity threats. The NRC has not codified these requirements in the CFR because of the sensitivity of the security-related information.

On October 21, 2010, the Commission issued Staff Requirements Memorandum (SRM)-COMWCO-10-0001, "Staff Requirements—COMWCO-10-0001—Regulation of Cybersecurity at Nuclear Power Plants" (Ref. [5]), in which the Commission determined as a matter of policy that the NRC's cybersecurity regulation (10 CFR 73.54) should be interpreted to include structures, systems, and components (SSCs) in the balance of plant (BOP) areas that have a nexus to radiological health and safety. This decision meant that digital assets previously covered by cybersecurity regulations of the Federal Energy Regulatory Commission would now be covered by the NRC's cybersecurity regulation (10 CFR 73.54). In response to this SRM, the licensees updated their cybersecurity plans (CSPs) to incorporate BOP systems. This RG includes guidance for SSCs in the BOP.

Related Guidance

- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Ref. [6]), provides specific guidance to nuclear power plant (NPP) licensees for use in the design, development, and implementation of protection measures for digital instrumentation and controls (I&C) used in safety-related applications.

- RG 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licensees, Certifications, and Approvals for Non-Light-Water Reactors" (Ref. [7]), endorses Nuclear Energy Institute (NEI) 18-04, Revision 1, August 2019, "Risk-Informed Performance-based Guidance for Non-Light Water Reactor Licensing Basis Development" (Ref. [8]), as one acceptable method for non-light-water reactor designers to use when preparing their applications.

- Draft Regulatory Guide (DG)-5076 (proposed new RG 5.97), "Guidance for Technology Inclusive Requirements for Physical Protection of Licensed Activities at Commercial Nuclear Plants" (Ref. [9]), currently under development, provides guidance for a technology-inclusive approach to implementing physical protection for commercial nuclear plants.

- DG-5061, Revision 1 (proposed Revision 1 to RG 5.71), "Cyber Security Programs for Nuclear Power Reactors," issued February 2022 (Ref. [10]), provides an approach that the NRC staff considers acceptable for complying with the requirements in 10 CFR 73.54.

- RG 5.83, "Cyber Security Event Notifications" (Ref. [11]), describes approaches and methodologies that the NRC staff considers acceptable for use by nuclear power reactor licensees when categorizing certain cybersecurity events and the process for notifying the NRC and submitting written security follow-up reports for cybersecurity events.

Purpose of Regulatory Guides

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific issues or postulated events, and to describe information that the staff needs in its review of applications

for permits and licenses. Regulatory guides are not NRC regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs are acceptable if supported by a basis for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG provides voluntary guidance for implementing the mandatory information collections in 10 CFR Parts 53 and 73 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collections were approved by the Office of Management and Budget (OMB), under control number 3150-XXXX, and 3150-0002, respectively. Send comments regarding this information collection to the FOIA, Library, and Information Collections Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by email to Infocollects.Resource@nrc.gov, and to the OMB Office of Information and Regulatory Affairs, Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

TABLE OF CONTENTS

A. INTRODUCTION....1

Purpose....1
Applicability....1
Applicable Regulations and Orders....1
Related Guidance....3
Purpose of Regulatory Guides....3
Paperwork Reduction Act....4
Public Protection Notification....4

B. DISCUSSION....7

Reason for Issuance....7
Background....7
Consideration of International Standards....9

C. STAFF REGULATORY GUIDANCE....11

General Requirements....11
Cybersecurity Plan....12
Cybersecurity Program Performance Objectives....13
Risk Management Framework....13
10 CFR 73.110(a) Consequences....15
Risk Assessment....15
Effects of Compromise on System Function....17Physical Intrusion Consequence....18Radiological Sabotage Consequence....19Blended Attack....20
Three-Tier Analysis Approach....21
Facility Scenario Analyses....24
Cyber-Enabled Accident Scenarios Analysis....25
Cyber-Enabled Intrusion Scenario Analysis....28
Adversary Functional Scenario Analysis....32
System-Level Analysis....36
System Critical Functions....36
Categorization of Critical Systems....37
Adversary Technical Sequence Analysis....40
Elements of a Cybersecurity Plan....43
Identification of Digital Assets Associated with Critical Systems....44
Cybersecurity Controls....44
Configuration Management....45
Supply Chain....45
Cybersecurity Measures for Critical Systems....46
Cybersecurity Measures for Most Critical Systems....46
Establishing and Implementing a Cybersecurity Program....47
Defensive Cybersecurity Architecture....47
Maintaining the Cybersecurity Program....49
Cybersecurity Impact Analysis....49
Sitewide Considerations....50
Event Reporting and Tracking....51

Records Retention and Handling....51
D. IMPLEMENTATION....52
GLOSSARY....53
REFERENCES....57
APPENDIX A (Cybersecurity Plan Template)....A-1
APPENDIX B (Cyber-Enabled Accident Scenario - Analysis and Example of an Adversary Functional Scenario)....B-1
APPENDIX C (Cyber-Enabled Intrusion Scenario - Analysis and Adversary Functional Scenario Example....C-1

B. DISCUSSION

Reason for Issuance

Currently, cybersecurity requirements for large light-water reactors are in 10 CFR 73.54 and supported by RG 5.71, "Cyber Security Programs for Nuclear Power Reactors." This security approach is focused on protecting important plant functions and associated critical digital assets for light-water reactor technologies. The NRC has promulgated 10 CFR 73.110 as an alternative regulatory framework for licensing other technologies in addition to light-water reactor technologies. This section provides technology-inclusive requirements for protecting digital computer and communications systems and networks. This RG would provide a commercial NPP licensed under 10 CFR Part 53 with an approach that is acceptable for meeting the requirements of 10 CFR 73.110.

Background

In recent years, the threat of cyberattacks has steadily risen, both globally and nationally. The U.S. Government has observed an increase in the number of cyberattacks and the level of sophistication of such attacks. These attacks can be conducted anonymously from remote locations throughout the world.

As stated in 10 CFR 53.440(f), "Safety and security must be considered together in the design process such that, where possible, security issues are effectively resolved through design and engineered security features." The regulations in 10 CFR 53.860(d) require the licensee to establish, maintain, and implement a cybersecurity program in accordance with 10 CFR 73.54 or 10 CFR 73.110 and require the licensee to describe the cybersecurity program in the CSP. Accordingly, each licensee that elects to use 10 CFR 73.110 needs to provide reasonable assurance that digital computer and communication systems and networks are adequately protected against cyberattacks that can cause the following consequences in 10 CFR 73.110(a):

(1) adversely impacting the functions performed by digital assets that would prevent a postulated fission product release resulting in offsite doses that would exceed the values in 10 CFR 53.210, "Safety criteria for design-basis accidents"

(2) adversely impacting the functions performed by digital assets used by the licensee for implementing the physical security requirements that would be established under 10 CFR 53.860(a)

For the consequences listed in 10 CFR 73.110(a)(2), the intent would be for the licensee to protect such functions from a cyberattack that could adversely affect them, thus preventing a 10 CFR Part 53 licensee from being able to meet the physical security requirements for the protection of special nuclear material based on the form, enrichment, and quantity in accordance with 10 CFR Part 73, as applicable, and the protection of Category 1 and Category 2 quantities of radioactive material in accordance with 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material" (Ref. [12]).

The new 10 CFR 73.110 considers (1) the operating experience from nuclear facilities and (2) the 10 CFR 73.54 framework, which contains some of the basic requirements needed for cybersecurity regardless of type of reactor. Differences between the 10 CFR 73.54 requirements and those discussed in 10 CFR 73.110 are primarily based on the implementation of a graded

approach to cybersecurity for commercial nuclear plants to account for the wide range of technologies and associated risks to be assessed by the NRC.

This RG provides an acceptable method for meeting the requirements of 10 CFR 73.110 that applies risk-informed, performance-based approaches. Specifically, the guidance in this RG accounts for the differing risk levels among commercial nuclear plant technologies, while providing reasonable assurance of adequate protection of public health and safety and the common defense and security. As such, this RG provides guidance to the licensee to scale the design and implementation of the CSP. This RG also describes the elements required in a CSP, includes a CSP template (appendix A), and incorporates certain guidance from RG 5.71, such as the cybersecurity controls in appendices B and C of RG 5.71. This RG also provides sample scenarios (appendices B and C) showing the use of the guidance documented here. This RG provides an acceptable method that applies risk-informed, performance-based approaches.

The RG leverages information from domestic and international sources such as the following:[1]

- The most recent revision to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 5, issued April 2013 (Ref. [13])

- NIST SP800-82, "Guide to Industrial Control Systems (ICS) Security," Revision 2, issued May 2015 (Ref. [14])

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002:2013, "Information technology—Security techniques—Code of practice for information security controls" (Ref. [15])

- IEC 63096:2020, "Nuclear power plants—Instrumentation, control and electrical power systems—Security controls" (Ref. [16])

- IEC 62443-3-3:2013, "Industrial communication networks—Network and system security —Part 3-3: System security requirements and security levels," issued in 2013 (Ref. [17])

- Information Systems Audit and Control Association, "Control Objectives for IT 2019 (COBIT 2019)," issued in 2018 (Ref. [18])

[1] 1Application of national and international standards typically aims to improve the quality, repeatability, and consistency of analyses and promulgate good practices.

Consideration of International Standards

The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA has established a series of security guides to address nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access, and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities. IAEA security guides present international good practices and increasingly reflect best practices to help users striving to achieve high levels of security. To inform its development of this RG, the NRC considered IAEA requirements and guides pursuant to the Commission's International Policy Statement (Ref. [19]) and Management Directive and Handbook 6.6, "Regulatory Guides" (Ref. [20]). The following IAEA publications were considered in the development of this RG:

- IAEA Nuclear Security Series (NSS) No. 42-G, "Computer Security for Nuclear Security," issued July 2021 (Ref. [21]), addresses computer security considerations for all organizations including the competent authority and operators of nuclear facilities within a country's nuclear security regime.

- IAEA NSS No. 23-G, "Implementing Guide for Security of Nuclear Information," issued February 2015 (Ref. [22]), addresses appropriate steps to effectively execute an information security plan and discusses cybersecurity issues.

- IAEA NSS No. 17-T, "Computer Security Techniques at Nuclear Facilities," issued September 2021 (Ref. [23]), addresses concepts and considerations for cybersecurity at nuclear facilities.

- IAEA NSS No. 33-T, "Computer Security of Instrumentation and Control Systems at Nuclear Facilities," issued May 2019 (Ref. [24]), details key methods and measures for the protection of I&C systems in nuclear facilities.

- IAEA Nuclear Energy Series Technical Report NR-T-3.30, "Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants," issued December 2020 (Ref. [25]), details the benefits and challenges of the various computer security methods and controls with their implementation in NPP I&C systems.

- IAEA Nuclear Energy Series Technical Report NP-T-3.21, "Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities," issued September 2016 (Ref. [26]), discusses the concepts and processes involving supplied items and services and guidance on addressing the challenges in the supply chain with respect to quality assurance.

- IAEA Nuclear Energy Series Technical Report NP-T-1.13, "Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants," issued November 2015 (Ref. [27]), discusses the challenges of addressing cybersecurity in the context of implementing and maintaining digital instrumentation and control systems.

- IAEA Non-Serial Nuclear Security Publication, IAEA-TDL-011, "Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain," to be published (Ref. [28]), discusses the challenges of supply chain risk management associated with cybersecurity and provides guidance for methods and approaches to minimize these risks.

The International Electrotechnical Commission (IEC) has developed cybersecurity standards and technical reports on the protection of I&C and electrical systems that perform important functions necessary for the safe and secure operation of NPPs. Founded in 1906, the IEC is the world's leading organization for the preparation and publication of international standards for all electrical, electronic, and related technologies. These international standards and reports advance and promote the implementation of good practices around the world. The IEC cybersecurity nuclear standards are aligned with documents in the IAEA Nuclear Security Series and provide additional technical details. These standards also directly leverage the ISO/IEC 27000 series standards to ensure that cybersecurity guidance is consistent with practices and approaches found in other sectors. The NRC staff considered the following IEC publications in the development of this RG:

- IEC 62645:2019, "Nuclear power plants—Instrumentation, control and electrical power systems—Cybersecurity requirements" (Ref. [29]), which details key elements of a cybersecurity program for I&C and electrical systems at NPPs, follows ISO/IEC 27001:2013, "Information technology—Security techniques—Information security management systems—Requirements" (Ref. [30]), for alignment with the standards information security management system requirements.

- IEC 62859:2016+AMD1:2019 CSV, "Consolidated version nuclear power plants—Instrumentation and control systems—Requirements for coordinating safety and cybersecurity" (Ref. [31]), details the considerations in reconciling safety and cybersecurity requirements.

- IEC 63096:2020, "Nuclear power plants—Instrumentation, control and electrical power systems—Security controls," details the security controls recommended for I&C and electrical systems at NPPs and follows ISO/IEC 27002.

- IEC 62443 series standards, "Industrial communication networks—IT security for networks and systems," which details information for securing industrial automation and control systems throughout their lifecycle. (Ref. [32]).

C. STAFF REGULATORY GUIDANCE

General Requirements

1. A licensee's cybersecurity program is required to provide reasonable assurance that digital computer and communication systems and networks are adequately protected against cyberattacks that could cause the consequences in 10 CFR 73.110(a). Furthermore, under 10 CFR 73.110(b)(2), the cybersecurity program needs to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, delay, respond to, and recover from cyberattacks capable of causing the consequences identified in 10 CFR 73.110(a).

2. This cybersecurity program is part of the licensee's site physical protection program. Licensees are required to protect digital computer and communication systems and networks associated with the functions identified in 10 CFR 73.110 in a manner that is commensurate with the potential consequences resulting from cyberattacks. Specifically, 10 CFR 73.110 identifies those functions that if compromised have the potential to lead to the consequences listed in 10 CFR 73.110(a).

3. The licensee needs to ensure that cybersecurity risks are effectively managed commensurate with the potential consequences. Cybersecurity risks can be avoided through effective application of technically viable alternatives including analog systems, passive features and structures, and noncyber independent protection layers (IPLs). However, the implementation of such risk avoidance alternatives assumes that digital equipment is not relied on to maintain or develop them. Therefore, it is important to implement a cybersecurity program for identifying, requiring, and establishing security controls, including those associated with the supply chain, that protects against potential cyberattacks against digital devices associated with such alternatives. For example, a digital calibration system used at the NPP may be unknowingly compromised through its supply chain to incorrectly calibrate an analog system, thus degrading the system's ability to adequately protect against cyber-enabled accident scenarios (CEASs). Cybersecurity supply chain guidance is found in sections C.145 through C.151.

4. Licensees are required to protect against cyberattacks capable of causing a consequence as defined in 10 CFR 73.110 and as shown in below. This RG provides guidance on the development of a CSP and examples for establishing cybersecurity controls, including a defensive computer security architecture (DCSA) to protect functions in a manner commensurate with the potential consequences of cyberattacks.

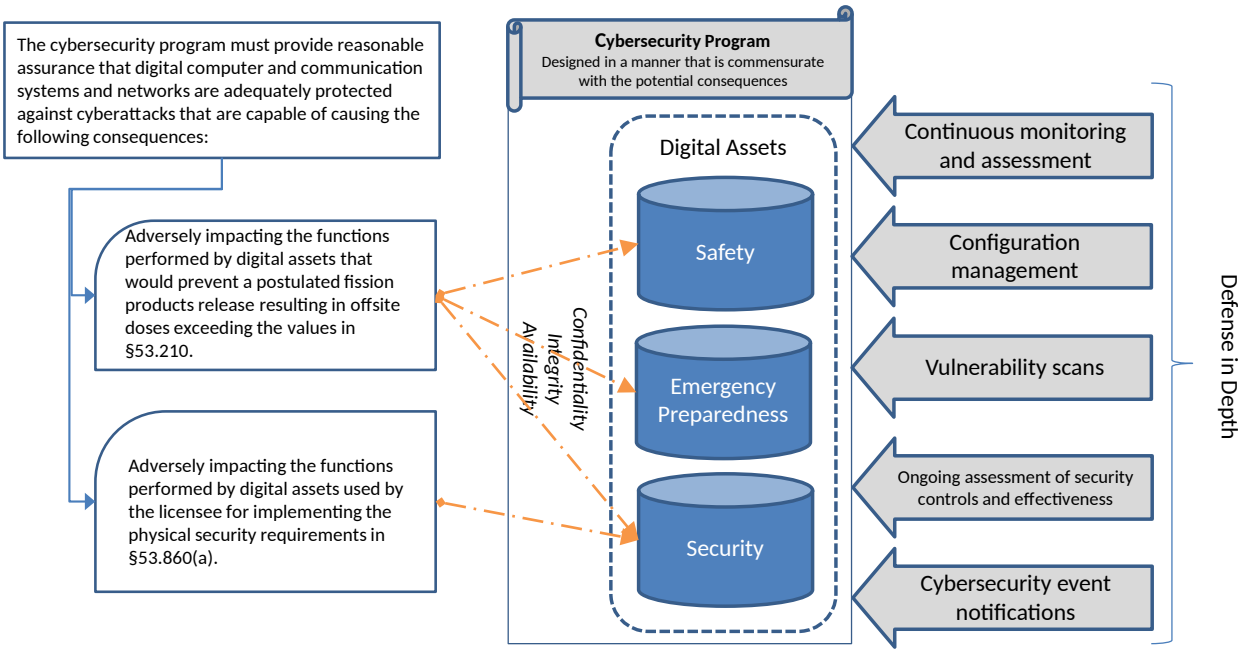


Figure 1. 10 CFR 73.110—High-Level Overview

5. The provisions of 10 CFR 73.110 identify the cybersecurity program performance objectives for a commercial nuclear plant licensee and the requirements needed to meet those objectives. The cybersecurity program performance objectives identified in 10 CFR 73.110(a) require each licensee under 10 CFR Part 53 to establish, implement, and maintain a cybersecurity program that is commensurate with the potential consequences of cyberattacks.

6. The rule identifies two consequences resulting from cyberattacks that establish thresholds for potential events involving radiological sabotage and physical intrusion. Preventing these events protects public health and safety and promotes the common defense and security. A physical intrusion consequence refers to a scenario in which a potential cyberattack adversely impacts the functions performed by digital assets used by the licensee for implementing the physical security requirements in 10 CFR 53.860(a). Such a scenario could facilitate, for example, subsequent theft or diversion of special nuclear material through a blended attack (i.e., an attack that has cyber and physical elements).

7. The cybersecurity program includes (1) developing a site-specific CSP that the licensee submits to the NRC in its license application, (2) conducting an analysis to identify digital assets associated with the potential consequences of a cyberattack and evaluating the digital assets to determine whether they require protection (i.e., they are associated with critical systems), (3) establishing and maintaining written implementation procedures for digital assets and documenting the measures taken to address the performance specifications associated with the identified cybersecurity controls, and (4) managing the CSP to detect, protect against, and respond to cyberattacks capable of causing a consequence as defined in 10 CFR 73.110(a).

Cybersecurity Plan

8. In accordance with 10 CFR 73.110(e)(2), the licensee is required to establish, implement, and maintain a CSP that implements the cybersecurity program requirements in a manner that is commensurate with the potential consequences resulting from cyberattacks. The CSP describes

the facility's cybersecurity program with sufficient detail for the NRC to determine its compliance with 10 CFR 73.110.

9. To meet the requirements of 10 CFR 73.110(e)(2), the CSP should describe the cybersecurity controls implemented by the licensee to protect digital assets commensurate with the potential consequences of cyberattacks. Upon implementation of the licensee's CSP, the NRC will periodically inspect the CSP for its compliance with 10 CFR 73.110.

10. Sections C.136 through C.138 provide additional guidance on the CSP, while appendix A includes a template showing an acceptable format and content for the CSP that the licensee must develop.

Cybersecurity Program Performance Objectives

11. A performance-based approach for cybersecurity focuses on protecting against cyberattacks and providing contingency responses. The objectives of the performance-based approach, in accordance with 10 CFR 73.110(a), are for a licensee to establish, implement, and maintain a cybersecurity program that is commensurate with the potential consequences resulting from cyberattacks that could lead to radiological sabotage or facilitate physical intrusion.

12. The cybersecurity requirements established in 10 CFR 73.110 are risk-informed and performance-based to account for the dose/consequence considerations, reactor thermal power, and the attributes for accomplishing the protection functions among the different reactor technologies (Ref. [33] and Ref. [34]).

13. In 10 CFR 73.110, the NRC implements a graded approach to determine the level of cybersecurity protection required for digital computer and communication systems and networks (i.e., protection at the CSP level and the security controls implementation level). A graded approach based on potential attack consequences is intended to facilitate differing risk-informed approaches and results and insights for various reactor technologies. Specifically, the proposed performance-based, risk-informed approach requires licensees to demonstrate reasonable assurance of cybersecurity protection against cyberattacks capable of causing the consequences defined in 10 CFR 73.110(a), as discussed in sections C.14 through C.64 below.

Risk Management Framework

14. As required by 10 CFR 73.110, the licensee must determine the level of cybersecurity protection required for digital computer and communication systems and networks that accounts for different levels of risk associated with diverse reactor technologies.

15. This RG presents a graded approach for computer system security in which security measures are applied commensurate with the potential consequences from a cyberattack. This and subsequent sections provide guidance on a tiered approach and are consistent with NIST SP800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," issued in 2018 (Ref. [35]); IAEA NSS No. 17-T; and IEC 62443 risk management processes.

16. This RG implements a three-tier approach, similar to the one documented in NIST SP800-37 and shown in figure 2, using risk assessments (section C.19) or analyses at the facility level, function level, and system level as discussed in sections C.65 through C.105. The intent of this approach is to ensure that the analyses of each tier are performed until it is demonstrated that a cyberattack

cannot result in the consequences listed in 10 CFR 73.110(a). This may result in a single tier of analysis being performed, two tiers of analysis being performed (i.e., first and second tier), or all three tiers of analysis being performed.

a. At the facility level, the intent of the analysis is to rely on existing safety and security assessments to determine whether the plant's design basis and existing physical protection (security) system (PPS) are sufficient to effectively prevent the potential consequences of a cyberattack. The first tier (facility-level) analysis uses risk and safety assessments to determine whether the plant design basis and existing PPS are sufficient to effectively prevent the potential consequences of a cyberattack. If the analysis proves that the design-basis elements and physical protection features prevent cyberattacks from resulting in the consequences listed in 10 CFR 73.110(a), then no further analyses would be needed. Otherwise, there would be a need for further defensive analysis as discussed in items (b) and (c) below.

b. At the function level, the intent of the analysis is to understand the adversary's access to attack pathways that allow for the compromise of plant functions resulting in the unacceptable consequences defined in 10 CFR 73.110(a). The second tier (function-level analysis) involves additional analyses for scenarios in which potential cyberattacks result in the consequences listed in 10 CFR 73.110(a) and the implementation of any identified improvements in item (a) above to the design basis or PPS is not possible. The additional analyses include developing adversary functional scenarios to understand the adversary's access to attack pathways that allow for the compromise of critical plant functions such as those associated with safety, security, and emergency preparedness (EP). The goal of these analyses is to identify CSP implementation measures (e.g., wireless prohibitions) and passive or deterministic DCSA features (e.g., data diode implementation) to eliminate or control attack access. Any adversary functional scenarios that remain unmitigated despite the application of CSP implementation measures and passive or deterministic DCSA features are addressed as part of the third tier discussed in item (c) below.

c. At the system level, the intent of the analysis is to identify protective measures including system-level cybersecurity controls to prevent or mitigate the impact on compromised plant functions. For the third tier (system-level analysis), critical plant functions would be identified along with adversary technical sequences (ATSs) that involve detailed attack steps to determine active CSP and DCSA implementation measures (e.g., use of detection and response systems), as well as system-level cybersecurity controls to prevent or mitigate the impact on such functions. This tier would also include an analysis to identify critical systems, and their corresponding digital assets, associated with a cyberattack consequence defined in 10 CFR 73.110 and the processes for determining the appropriate defensive measures. Both the function-level and system-level analyses use a graded approach to determine the level of cybersecurity protection commensurate with potential consequences from a cyberattack.

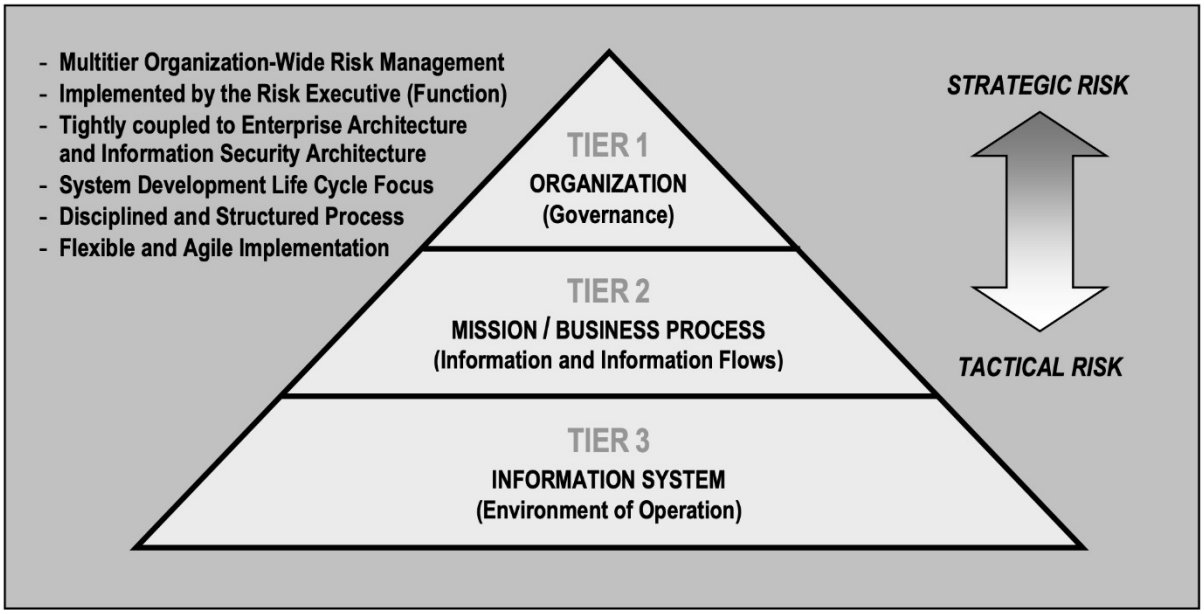


Figure 2. NIST SP800-37 Tiered Risk Management Approach

10 CFR 73.110(a) Consequences

17. As discussed in the Background section of this RG, 10 CFR 73.110(a) lists two consequences that are within the scope of what a licensee should address through its cybersecurity program:

    a. adversely impacting the functions performed by digital assets that would prevent a postulated fission product release resulting in offsite doses exceeding the values in 10 CFR 53.210, and

    b. adversely impacting the functions performed by digital assets used by the licensee for implementing the physical security requirements in 10 CFR 53.860(a).

18. The licensee should use these consequences as the starting point to determine which functions, systems, and associated digital assets could be affected by a cyberattack and lead to a consequence. A licensee should focus its cybersecurity efforts to effectively protect against cyber threats associated with these functions and the digital systems that perform the necessary actions that prevent or mitigate these consequences.

Risk Assessment

19. As discussed in section C.16, this RG uses a tiered risk management framework that allows for focus on strategic risks at a level of abstraction that reduces complexity and offers independence in risk assessments at different tiers providing for defense in depth and minimizing the potential that errors within a single tier will result in ineffective cybersecurity programs.

20. The risk assessment provides the basis for meeting the requirements of 10 CFR 73.110(b)(1):

    > Analyze the potential consequences [i.e., those that fall within the consequences listed in 73.110(a) dealing with radiological sabotage and physical intrusion] resulting from cyberattacks on digital computer and communication systems and

networks and identify those assets that must be protected to satisfy paragraph (a) of this section.

The risk assessment to be performed for each tier of the risk management framework would include the following stages:

a. Risk Identification: This is the process of finding, recognizing, and describing risks.

b. Risk Analysis: While risk identification involves generating a list of risks that can interfere with the facility, risk analysis aims to understand the risk, its sources, causes, and consequences. Specifically, risk analysis is the process to comprehend the nature of risk and to determine the level of risk. The process determines (1) what can go wrong, (2) how likely it is, and (3) the consequences. This includes evaluating functions, performing event sequence identification (which is a process of postulating initiating event(s)), evaluating system function, SSCs, and operator (if applicable) responses to postulated initiating event(s), and predicting the potential consequences of cyberattacks that may lead to radiological sabotage or physical intrusion.

c. Risk Evaluation: This process of comparing the results of risk analysis with risk criteria to determine whether risk and its magnitude is acceptable or tolerable may include comparing the event sequence consequences to quantitative health objectives to determine acceptable levels of risk. This aids in decision-making processes, such as, but not limited to, prioritization of risk treatment options, establishing requirements and procedures for operations and maintenance, evaluating defense in depth, and classifying SSCs.

21. The risk assessment to be performed at the facility level, or the first tier of the risk management framework, would need to consider the effects of compromise on system function and focus on consequences resulting from either CEASs (see sections C.68 through C.77) or cyber-enabled intrusion scenarios (CEISs) (see sections C.78 through C.87).

22. The risk assessment to be performed at the function level, or the second tier of the risk management framework, would need to consider adversary access to system(s). This second-tier risk assessment addresses the CEASs or CEISs that have the potential to lead to radiological sabotage or physical intrusion. At a minimum, a facility design that consists of conceptual architecture and system designs is needed to address or manage the risks identified by the risk assessment. This risk assessment considers adversary functional scenarios (see sections C.88 through C.103) and provides a method for identifying functions that are associated with digital computers and communications systems and networks that can contribute to 10 CFR 73.110(a)(1) and (2) consequences.

23. The risk assessment to be performed at the system level, or the third tier of the risk management framework, would need to consider the protection of confidentiality, integrity, and availability (CIA) for systems and networks covered by 10 CFR 73.110(b)(1) to determine the necessary security controls to provide the protection required by 10 CFR 73.110(c).

24. The tiered risk assessment would be used to determine whether risks can be avoided (e.g., cyberattacks cannot result in the potential for radiological sabotage due to security by design (SeBD) features) and to determine both sufficient and efficient combinations of protective measures (e.g., cybersecurity controls) to mitigate the potential consequences of a cyberattack.

25. In each tier of the risk assessment, cyberattacks are assumed to be able to compromise functions and have the potential to alter the functions' behavior and actions, failure modes, and effects, or to raise the potential for new accident or intrusion sequences that can overcome or bypass several layers of defense in depth.

26. The risk assessment should be used to assess whether a cyberattack could result in the consequences defined in 10 CFR 73.110(a). Furthermore, the risk assessment should incorporate any existing safety and security analyses, as appropriate.

27. The facility scenario analysis, sections C.65 through C.103, identifies cybersecurity threats that are applicable to the facility and the functions that are linked to the consequences defined in 10 CFR 73.110(a). These analyses also support the risk analysis and risk evaluation stages through adversary functional scenario analysis (AFSA) (see sections C.88 through C.103).

28. The system-level analysis, sections C.104 through C.105, identifies and categorizes critical systems that perform or support functions that are linked to the consequences defined in 10 CFR 73.110(a). The licensee uses the system-level analyses to develop ATSs to inform selection of controls and enhance detection and response capability. The system-level analyses support risk identification and analysis through system categorization and ATS development, and risk evaluation through the prioritization and selection of controls.

Effects of Compromise on System Function

29. Impacts on a function's CIA resulting from cyberattacks may lead to the 10 CFR 73.110(a) consequences. For this reason, the licensee would be required to meet the CIA requirements in 10 CFR 73.54(c) for the systems and networks covered by 10 CFR 73.110(b)(1) in a manner that is commensurate with the potential consequences resulting from cyberattacks. If the outcome of the assessment by the licensee pursuant to 10 CFR 73.110(b)(1) reveals that a potential cyberattack would not compromise any digital assets that support safety and security functions and therefore would not result in the consequences listed in 10 CFR 73.110(a) (e.g., does not exceed the dose rate values), then there would be no need to meet this requirement.

30. The impact on a function's CIA resulting from a cyberattack can be determined through an assessment of the effects of compromise of function(s), and the associated system(s) and digital assets, and validated through AFSA (see sections C.88 through C.103).

31. As part of the AFSA, the licensee should assess the potential consequences of a function compromise as follows (see Ref. 25)*:*

    a. The function fails.

    b. The function performs as expected, meaning the compromise does not adversely affect system function (i.e., it is fault tolerant).

32. The risk assessment should consider the worst consequences for systems, especially those that perform functions whose failure could result in the 10 CFR 73.110(a) consequences.

Physical Intrusion Consequence

33. As discussed in sections C.17 through C.18 above, 10 CFR 73.110(a)(2) deals with a scenario in which a potential cyberattack adversely impacts the functions performed by digital assets used by the licensee for implementing the physical security requirements in 10 CFR 53.860(a).

34. PPSs are used for the protection of special nuclear material, source material, and byproduct material. A licensee would be permitted to rely on the use of digital assets for implementing the PPS functions that would be required to meet the 10 CFR 53.860(a) requirements. Therefore, this consequence deals with a scenario in which, for example, a cyberattack adversely impacts the digital assets and associated security functions used by the licensee to meet the 10 CFR 53.860(a) requirements. Security digital assets include those used for nuclear material control and accounting. Such a consequence would not be applicable to commercial nuclear plant designs that do not rely on the use of digital assets for implementing the security functions required for meeting the 10 CFR 53.860(a) requirements.

35. Security digital assets to be assessed as part of consequence 10 CFR 73.110(a)(2) include those used for nuclear material control and accounting. Such a consequence would not be applicable to commercial nuclear plant designs that do not rely on the use of digital assets for implementing the security functions required for meeting the 10 CFR 53.860(a) requirements.

36. In accordance with 10 CFR 73.110(d)(2), a licensee would need to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, delay, respond to, and recover from cyberattacks capable of causing the consequences identified in 10 CFR 73.110(a).

37. CEISs may be developed to inform the risk analysis and risk evaluation for the physical intrusion consequence. The adversary may target PPSs and components, including detection equipment, for a compromise that would result in a malicious physical intrusion not being detected or might preclude the ability to respond to a physical intrusion. Therefore, systems and components that perform detection should be considered the highest contributor to risk of physical intrusion resulting from a cyberattack. However, if a scenario involving the compromise of systems and components that perform detection can be avoided by implementing SeBD features (i.e., facility design and engineered security features), then the potential consequences from such a cyberattack can be negated.

38. Supporting systems, components, and personnel may either reduce or add to the risk from a compromise of the detection equipment. Random patrols may detect precursors or evidence of malicious activity, thus reducing risk. Conversely, interconnection of systems may provide for new attack pathways to compromise the detection equipment.

39. CEISs may be used to validate assumptions made during the PPS design and implementation. The assumptions made in developing a set of CEISs should include at a minimum the following:

    a. loss of detection performed by digital technology with no indication of failure;

    b. failure of one or more of the detection, delay, response, or recovery capabilities; and

    c. unexpected behaviors or actions of digital equipment concurrent with the start of a physical intrusion.

40. Evaluations of CEISs may result in updates to the design basis of the reactor or PPS design with the aim to minimize cybersecurity measures and activities (e.g., assurance, updates, modifications) that may be needed to address advances in adversary capabilities or to resolve discovered vulnerabilities. Potential options include the following:

    a. passive structures that do not rely on detection;

    b. analog systems or physically isolated digital systems that are tamper resistant to provide detection functions;

    c. independent, redundant, or diverse systems that can reduce the contribution of key systems to risk of physical intrusion; and

    d. independent continuous monitoring of cybersecurity of PPS, which can reduce the potential that the compromise will not be detected, further reducing the contribution of key systems to risk of physical intrusion.

41. Those PPS functions that have the potential to require or depend on digital technology for the licensee to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, delay, respond to, and recover from a physical intrusion should be identified, including their contribution to the risk of physical intrusion given the AFSA.

42. The identified PPS functions should be assigned a set of graded controls for cybersecurity, using their associated systems and digital assets, to ensure their protection.

Radiological Sabotage Consequence

43. As discussed in sections C.17 through C.18, 10 CFR 73.110(a)(1) deals with the radiological sabotage scenario in which a potential cyberattack adversely impacts the functions performed by the digital assets used by the licensee to avoid exceeding the offsite dose values established in 10 CFR 53.210. The risk assessment should identify functions that could contribute to or mitigate the radiological sabotage consequence identified in 10 CFR 73.110(a)(1).

44. Radiological sabotage may involve compromise(s) of function(s) resulting in events such as the following:

    a. loss of reactivity control leading to an unacceptable reactor power increase,

    b. overpressure event leading to a pressure boundary failure,

    c. loss-of-coolant event (from a pressure boundary breach) leading to reactor core damage,

    d. equipment malfunction or failure leading to fire,

    e. a physical breach resulting from a kinetic event in which control of rotational equipment (e.g., turbine) is altered because of a cyberattack, and

    f. equipment malfunction or failure resulting from an electrical power system event.

45. For reactor designs that include passive safety features, the licensee provides an analysis of how events such as those listed in section C.44 are accounted for when considering the effects of

compromise on function(s). The events resulting from function(s) compromised by potential cyberattacks produce CEASs.

46. To aid in the risk assessment, the licensee should develop adversary functional scenarios to validate assumptions made during the reactor design and implementation. These scenarios should assess whether a radiological sabotage scenario involving compromise(s) of function(s) that results in events such as those listed in section C.43 could lead to the consequence identified in 10 CFR 73.110(a)(1). A licensee may use existing documentation and analyses (e.g., integrated safety analysis, process hazards analysis, security plans) in support of the risk assessment to (1) determine those events that may lead to the consequence identified in 10 CFR 73.110(a)(1), and (2) subsequently identify the function(s) that may be adversely affected by a potential cyberattack thus leading to the consequence identified in 10 CFR 73.110(a)(1).

47. The licensee considers events such as the above and evaluates whether cyberattacks can escalate the impacts (i.e., increase the severity) of these events in the accident scenarios (i.e., CEASs) already considered, and whether they may create new pathways that result in consequences.

48. Those functions that could require or depend on digital technology and have the potential to result in the consequence identified in 10 CFR 73.110(a)(1) if compromised should be identified, including their contribution to the risk, given the applicable adversary functional scenario(s).

49. Systems and components that perform or support the functions identified as being associated with CEASs should be considered significant contributors to risk from a cyberattack. Therefore, such systems and components should be protected from a cyberattack using a graded approach as based on the analyses detailed in sections C.65 through C.105 of this RG to ensure their protection not only during operation, but also during their development, simulation, and maintenance environments.

50. Supporting systems, components, and personnel may either reduce or add to the risk from a compromise of the functions associated with a CEAS. For example, interconnected systems may detect precursors or evidence of malicious activity, thus reducing risk; conversely, interconnection of systems may provide for new attack pathways to compromise the function.

51. Independent and diverse systems providing redundant or backup functionality can reduce the contribution of the systems associated with the CEAS to the risk of radiological sabotage.

52. Independent continuous monitoring of cybersecurity can reduce the potential that compromise from cyberattack will not be detected, further reducing the contribution of the systems associated with the CEAS.

Blended Attack

53. A blended attack is one that has cyber and physical elements. Because CEIS is focused on physical intrusion, all CEISs are assumed to be blended attacks for the purpose of the analysis discussed in sections C.78 through C.87. If the physical intrusion is intended to cause radiological sabotage, a blended attack would also be relevant to CEASs.

54. The licensee should consider CEASs and CEISs along with the following physical events:

    a. physical tampering of fail-safe, analog systems or noncyber IPLs; and

b. explosive destruction of SSCs or passive features or structures.

55. Analysis of blended attacks may lead to changes in reactor design basis, PPSs, and passive features and structures with the aim of ensuring adequate cybersecurity.

Three-Tier Analysis Approach

56. To meet the requirements of 10 CFR 73.110, a risk-informed, performance-based, three-tier analysis as shown in figure 3 would be a permissible approach for the licensee. Only systems that perform or rely on functions whose compromise can contribute to the 10 CFR 73.110(a) consequences should be assessed and protected.

57. At the facility level, or the first analysis tier, CEASs and CEISs would help identify those cybersecurity scenarios with the potential to result in the consequences defined in 10 CFR 73.110(a) that would require the protection of digital computer and communication systems and networks associated with the functions described in 10 CFR 73.110(a)(1) and (2).

58. At the function level or the second analysis tier, an AFSA would aim to identify the most significant risks associated with cyberattacks (specifically, those risks having the consequences defined in 10 CFR 73.110(a)). The AFSA meets the intent of the Tier 2—Mission Risk Assessment shown in figure 2. IAEA NSS 17-T provides another example of this multitiered risk management approach.

59. The AFSA discussed in sections C.88 through C.103 helps identify incident scenarios to inform design, development, and implementation of the DCSA and other common, facilitywide elements that provide a plant capability (e.g., resilience) that could be used to protect against cyberattacks capable of causing the consequences defined in 10 CFR 73.110(a).

60. If the cyber risks assessed in the first two tiers of analyses are unacceptable, then an additional risk management process is necessary. Specifically, a system-level analysis (the third analysis tier), as discussed in sections C.104 through C.105, is needed to identify if a system under consideration supports critical functions (figure 4).

61. The licensee can perform a further optional analysis (figure 5), as discussed in sections C.112 through C.119, to grade the systems and allow for the allocation of resources to be based on the grading of the system (e.g., most, least, not critical) for the selection and application of cybersecurity measures.

62. ATSs (figure 6), as discussed in sections C.120 through C.135, need to be developed for a critical system as part of the system-level analysis. The ATS should provide sufficient detail to allow for specification of prevention, detection, and response capabilities necessary to ensure that the adversary cannot successfully initiate or complete CEISs and CEASs.

63. The analyses depicted in figures 4 through 6 meet the intent of the Tier 3—Information System Risk Assessment in figure 2 or IAEA NSS 17-T.

64. Figure 3 describes the major steps in this analysis approach:

a. The results of risk and safety assessments would be used to analyze the impact of the loss or compromise of a plant function resulting in the unacceptable consequences identified

in 10 CFR 73.110(a). The focus for this risk assessment is potential cyberattack consequences considering the plant design basis and PPS.

b. CEASs, CEISs, and blended attack scenarios would be considered, as further described in figures 4 and 5. Compromise and progression of accident or intrusion scenarios (i.e., attack success) are assumed immediately upon adversary access. If a cyberattack results in the 10 CFR 73.110(a) consequences, then enhancements or improvements to the design basis or PPS features should be considered.

c. If the preceding analysis shows that a cyber-enabled scenario results in exceeding the 10 CFR 73.110(a) consequences, then the approach would proceed to developing adversary functional scenarios aimed at managing functional risks by specifying prohibitive CSP and passive or deterministic DCSA elements to prevent attacks. Figure 6 describes this next level of analysis.

d. If the preceding analysis finds that unmitigated adversary scenarios remain, the performance-based approach would include steps to develop detailed ATSs to assist in the specification of graded prevention, detection, and response requirements (i.e., CSP, DCSA, and system controls) as described in figures 7, 8 and 9. Based on ATSs, the approach identifies measures and controls on system design and operation to protect the critical function by applying a graded approach and implementing defense in depth.

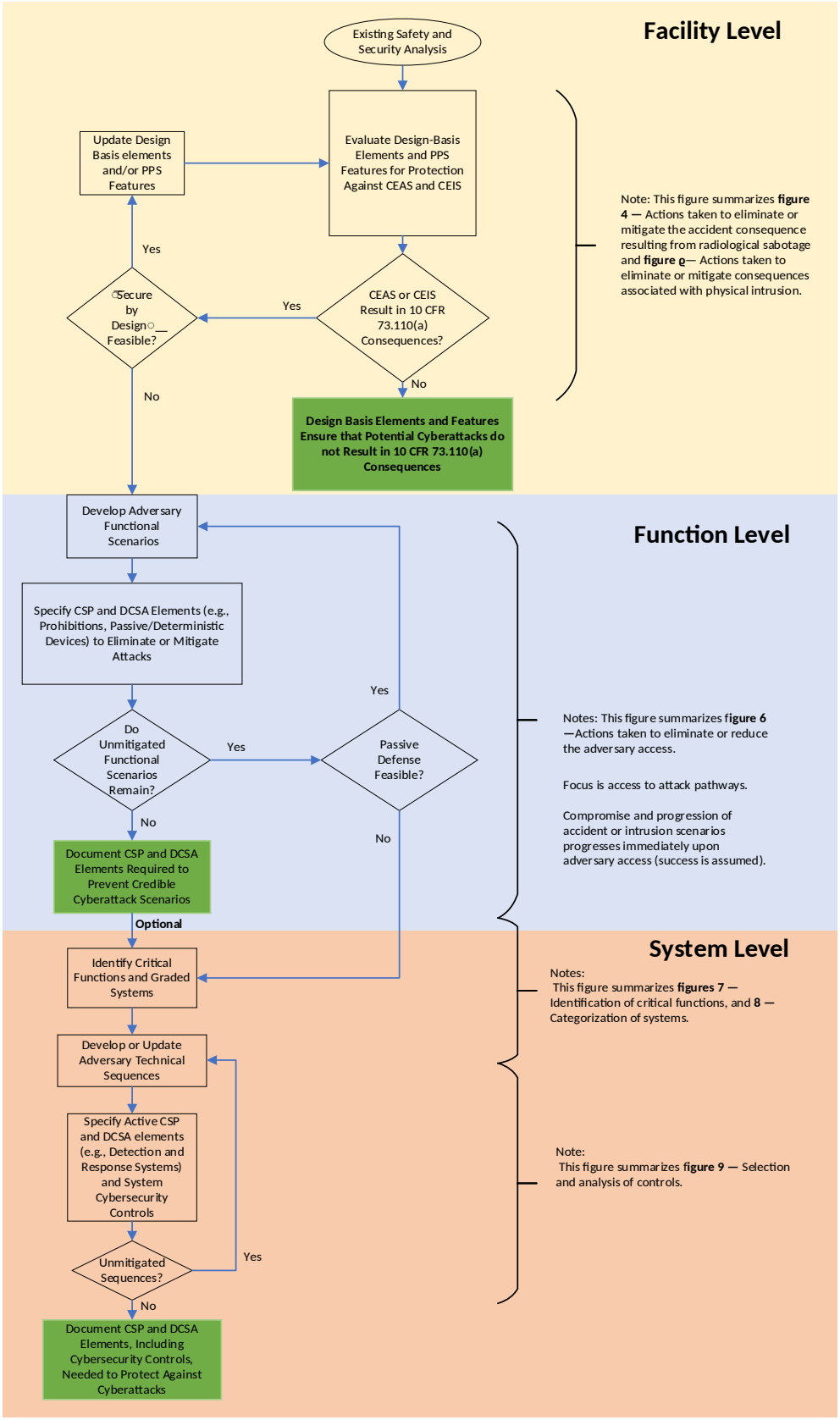


Figure 3. Overview of the Three-Tier Analysis Approach

Facility Scenario Analyses

65. The facility scenario analyses consist of two separate yet similar processes depicted in figures 4 and 5—figure 4 for CEAS analysis for radiological sabotage, and figure 5 for CEIS analysis for physical intrusion. These analyses determine whether cybersecurity activities should be focused solely on information security assurance (i.e., the 10 CFR 73.110(a) consequences are not possible) or a combined approach (that includes threat-risk assessments to determine cybersecurity measures). These analyses will be periodically reviewed and updated as required by 10 CFR 73.110(e)(4) based on emerging threats, discovered vulnerabilities, advances in adversary capabilities, or newly identified intrusion or accident scenarios.

66. If one or more of the CEASs or CEISs have the potential to result in the 10 CFR 73.110(a) consequences, then the AFSA discussed in sections C.88 through C.103 should be performed (see figure 6). Otherwise, the licensee should document the design-basis elements and features of the facility design that ensure that potential cyberattacks would not result in the 10 CFR 73.110(a) consequences. If the outcome of the assessment by the licensee pursuant to 10 CFR 73.110(b)(1) reveals that a potential cyberattack would not compromise any digital assets that support safety and security functions and thus would not result in the consequences listed in paragraph (a) (e.g., does not exceed the dose rate values in 10 CFR 53.210(a) and (b)), then the implementation of the cybersecurity program requirements in paragraphs (d) and (e) would be minimized. For example, the licensee would need only to develop a cybersecurity program that implements the requirements dealing with the following:

a. analyzing modifications of any asset before implementation to see if they meet the potential consequences in 10 CFR 73.110(a),

b. ensuring that employees and contractors are aware of cybersecurity requirements and have some sort of cybersecurity training,

c. evaluating and managing cybersecurity risks to their plant,

d. reviewing their CSP for any required changes, and

e. retaining records of their CSP along with any plan changes.

67. The analysis of the potential consequences of cyberattacks should factor in two scenarios: (1) the cyberattack directly causes a consequence, and (2) an initiating event (e.g., plant transient) separate from the effects of the cyberattack is needed to cause a consequence. For the first scenario, the cybersecurity controls and response efforts for such a consequence should account for a compromise that can directly cause a safety or security event. For this reason, robust protection is an important aspect of an adequate CSP because the time for response may be limited. For the second scenario, the analysis should factor as appropriate the potential time that may elapse between the compromise of the digital asset(s) by the cyberattack and the initiating event that leads to the consequence. Therefore, a licensee may have the opportunity to identify the compromised digital asset(s) associated with the consequences and implement measures to prevent a safety or security event. For this reason, robust detection and response capabilities are important aspects of an adequate CSP to account for such a scenario.

Cyber-Enabled Accident Scenarios Analysis

68. Figure 4 shows the CEAS analysis process for the radiological sabotage consequence. The outputs from the analysis would include a set of functions that require protection, insights for potential design-basis updates, and security engineering insights for CSP and DCSA implementation. The analysis also informs CSP implementation, cybersecurity supply chain implementation, periodic review implementation, and any other licensee-identified measures.

69. The CEAS analysis objective is to determine if cyberattacks can result in the following:

    a. accident scenarios considered in the safety analysis that would result in the consequence in 10 CFR 73.110(a)(1), or

    b. accident scenarios not considered in the safety analysis that would result in the consequence in 10 CFR 73.110(a)(1) (e.g., an accident scenario that could result only from a cyberattack).

70. The CEAS analysis aims to eliminate accident scenarios or provide reasonable assurance that such accidents as enabled by cyberattack do not result in consequences in 10 CFR 73.110(a)(1).

71. Development of CEASs can use the results of risk analysis, accident analysis, or other safety assessments to analyze the contribution of a cyberattack in the escalation of consequences associated with, for example, the loss of engineered systems to remove decay heat or that result in physical breaches.

72. Each CEAS analysis should consider, at a minimum, cyberattacks that result in any of the events listed in section C.44 and whether a cyberattack can escalate the impacts (i.e., increase the severity) of these events on the accident scenarios already considered or may create new pathways that result in the consequence in 10 CFR 73.110(a)(1).

73. Each CEAS analysis should determine whether it results in a consequence in 10 CFR 73.110(a)(1) while factoring, for example, design-basis features such as passive structures/features, analog or noncyber IPL, and PPS.

74. For each CEAS that has the potential to result in a consequence in 10 CFR 73.110(a)(1), one of the following may be chosen:

    a. Update the design basis to eliminate or reduce offsite dose values so they do not exceed those of 10 CFR 53.210. Subsequently, repeat the analysis in section C.73.

    b. Accept the risk as unavoidable, and apply additional cybersecurity measures to protect against the CEAS, as discussed in sections C.88 through C.103 and follow-on sections.

75. In summary, the licensee should perform the following:

    a. Document the CEAS and corresponding analysis, including the set of functions associated with each of the analyzed CEASs.

    b. Identify the design-basis elements (e.g., passive structures/features, analog or noncyber IPL) that provide the capability to avoid the CEAS, as appropriate. Special attention will be necessary to manage potential cybersecurity supply chain risks to these elements and

quality assurance based on their contribution to preventing cyberattacks that could result in a consequence in 10 CFR 73.110(a)(1).

c. Determine and record whether section C.76 or section C.77 applies.

d. Incorporate measures for periodic review and validation of CEAS analysis within the licensee's management system.

e. Perform CEIS analysis in accordance with sections C.78 through C.87, if not already performed.

f. Perform blended attack analysis in accordance with sections C.53 through C.55, if not already performed.

76. If no CEAS would result in 10 CFR 73.110(a)(1) consequences, the risk from cyberattacks resulting in radiological sabotage of regulatory concern would be effectively avoided. For such an outcome, the licensee should implement the CSP and DCSA identifying, establishing, and maintaining the design-basis features and PPS elements intended to protect against radiological sabotage, thus preventing the CEAS from resulting in those consequences. The CSP should also implement controls for cybersecurity supply chain risk management in accordance with sections C.145 through C.151 to protect those functions identified in the CEAS analysis. The design-basis features and PPS elements necessary for protecting against CEAS need to be identified, recorded, and monitored to ensure they remain effective. The licensee should provide evidence (e.g., modeling, testing) to support the demonstration of effectiveness of the design-basis features and PPS elements necessary for protecting against CEASs.

77. The licensee should perform an AFSA in accordance with sections C.88 through C.103 if any CEAS could result in a consequence under 10 CFR 73.110(a)(1) to determine the scope of the CSP and additional protective measures.

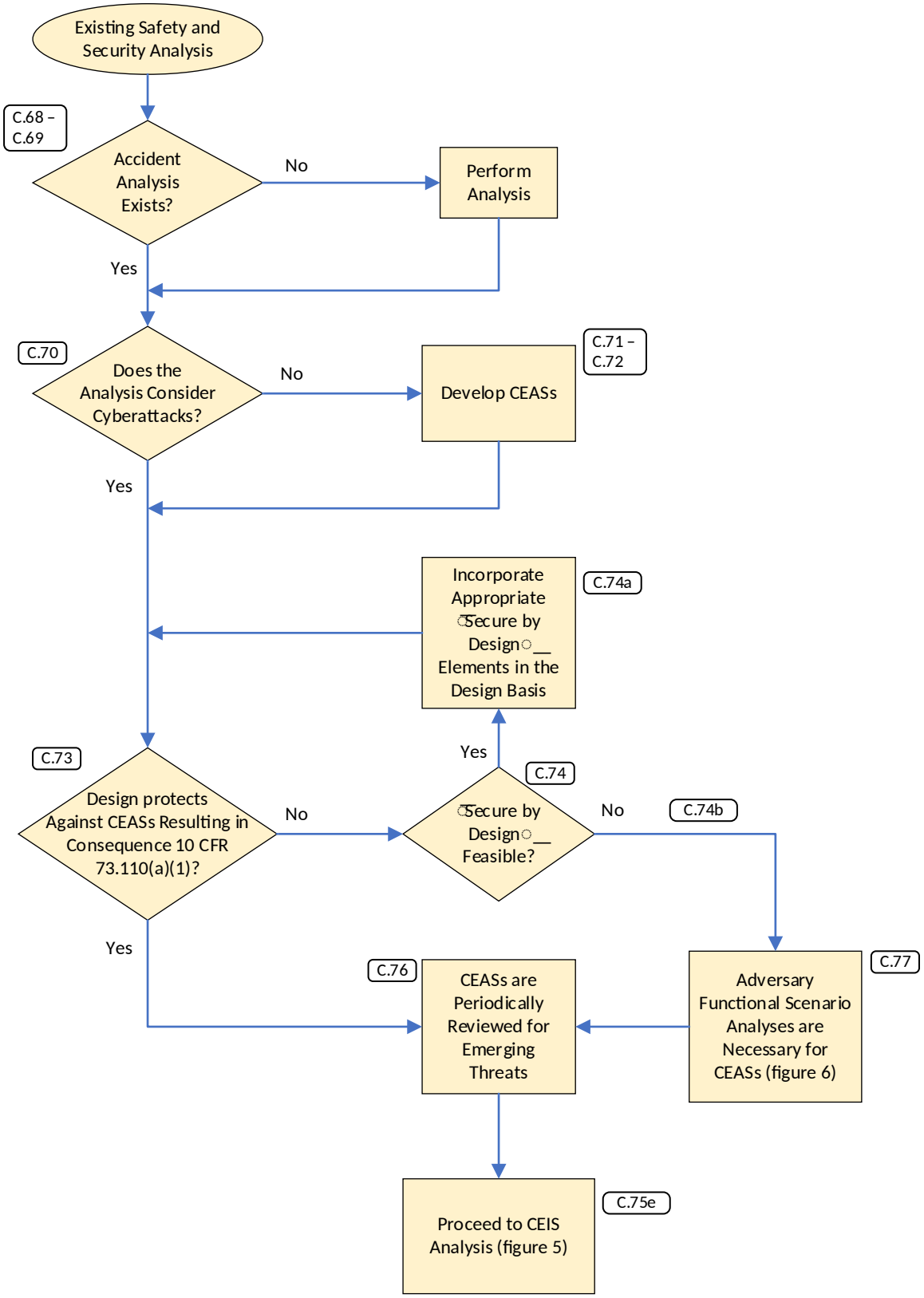


Figure 4. Cyber Extension to Safety Accident Scenario Analysis for Radiological Sabotage Consequence in 10 CFR 73.110(a)(1)

Cyber-Enabled Intrusion Scenario Analysis

78. Figure 5 shows the CEIS analysis process for the physical intrusion consequence. The outputs from the analysis would include a set of functions that require protection, insights for potential updates to the design basis or PPS design, and security engineering insights for CSP and DCSA implementation. The analysis also informs CSP implementation, cybersecurity supply chain implementation, periodic review implementation, and any other licensee-identified actions.

79. The CEIS analysis objective is to determine if cyberattacks can result in the following:

    a. 10 CFR 73.110(a)(2) consequence, or

    b. new scenarios not considered in the physical security analysis.

80. The CEIS analysis would aim to eliminate physical intrusion scenarios enabled by potential cyberattacks that would adversely impact the functions performed by digital assets used by the licensee for implementing the physical security requirements that would be established in 10 CFR 53.860(a).

81. Development of the CEIS analysis could use the results of risk analysis, security analysis, or other assessments to analyze the contribution of a cyberattack to assist in the physical intrusion into the facility for theft or sabotage of regulated quantities of special nuclear material, source material, and byproduct material.

82. The CEIS analysis should consider, at a minimum, cyberattacks that result in any of the events listed in section C.39 or any additional scenarios resulting from the effects of compromise of security-related functions.

83. For each analyzed CEIS, the analysis should determine whether it would result in a 10 CFR 73.110(a)(2) consequence while factoring, for example, design-basis features such as passive structures or features, analog or noncyber IPL, or PPSs or mitigations.

84. For each CEIS that has the potential to result in a 10 CFR 73.110(a)(2) consequence, one of the following may be chosen:

    a. Update the design basis or the PPS to prevent CEISs resulting in a 10 CFR 73.110(a)(2) consequence.

    b. Accept the risk as unavoidable and apply additional cybersecurity measures to protect against the CEIS, as discussed in sections C.88 through C.103 and follow-on sections.

85. In summary, the licensee should do the following:

    a. Document the CEIS and corresponding analysis, including the set of functions associated with each of the analyzed CEISs.

    b. Identify the design-basis elements (e.g., passive structures or features, analog or noncyber IPL), and PPS elements that provide the capability to avoid the CEISs, as appropriate. Special attention should be given to managing potential cybersecurity supply chain risks to these elements and quality assurance based on their contribution to preventing cyberattacks that could result in 10 CFR 73.110(a)(2) consequences.

c. Determine and record whether section C.86 or section C.87 applies.

d. Incorporate measures for periodic review and validation of CEIS analysis within the licensee's management system.

e. Perform CEAS analysis in accordance with sections C.68 through C.77, if not already performed.

f. Perform blended attack analysis in accordance with sections C.53 through C.55, if not already performed.

86. If no CEISs could result in 10 CFR 73.110(a)(2) consequences, then the risk of cyberattacks resulting in physical intrusion would be effectively avoided. For such an outcome, the licensee should implement a CSP and DCSA identifying, establishing, and maintaining the design-basis features and PPS elements that prevent the CEIS from resulting in those consequences. The CSP should also implement controls for cybersecurity supply chain risk management in accordance with sections C.145 through C.151 to protect those functions identified in the CEIS analysis. The design-basis features and PPS elements necessary for protecting against CEIS need to be identified, recorded, and monitored to ensure they remain effective. The licensee should provide evidence (e.g., modeling, testing) to support the demonstration of effectiveness of the design-basis features and PPS elements necessary for protecting against CEIS.

a. A cybersecurity evaluation performed by the NRC staff as part of the 2018 Radiation Source Protection and Security Task Force Report (ADAMS Accession No. ML18235A370) revealed that risk-significant radioactive materials licensees do not rely solely on digital systems to ensure safety or physical protection. Generally, NRC licensees apply a defense-in-depth approach to safety and security, using measures that include nondigital features such as doors, locks, physical barriers, personnel, and procedures, in addition to any digital assets. Therefore, the NRC staff determined that a compromise of digital assets used in these applications would not cause a direct dispersal of risk-significant quantities of radioactive material or expose individuals to radiation unless accompanied by a concurrent and targeted breach of other safety or security measures in place. Based on this evaluation, the NRC staff concluded that the requirements in 10 CFR Part 37, "Physical protection of Category 1 and 2 quantities of radioactive material," provide reasonable assurance of adequate protection of public health and safety when considering the potential consequences of a variety of attack vectors, including cyberattacks.

b. When performing the analysis per 10 CFR 73.110(b)(1), the licensee should determine whether the cybersecurity posture for Category 1 and 2 quantities of radioactive material is commensurate to that of current NRC licensees as discussed above. If that is the case then, there is no need for the licensee to implement the guidance discussed herein for meeting the 10 CFR 73.110 requirements. Instead, the licensee should follow the cybersecurity practices documented in Information Notice 2019-04, "Effective Cyber Security Practices to Protect Digital Assets of Byproduct Materials Licensees" (ADAMS Accession No. ML18044A350), which provides information for effectively protecting digital assets.

87. To determine the scope of the CSP and additional protective measures, the licensee should perform an AFSA in accordance with sections C.88 through C.103 if any CEIS could result in 10 CFR 73.110(a)(2) consequences.

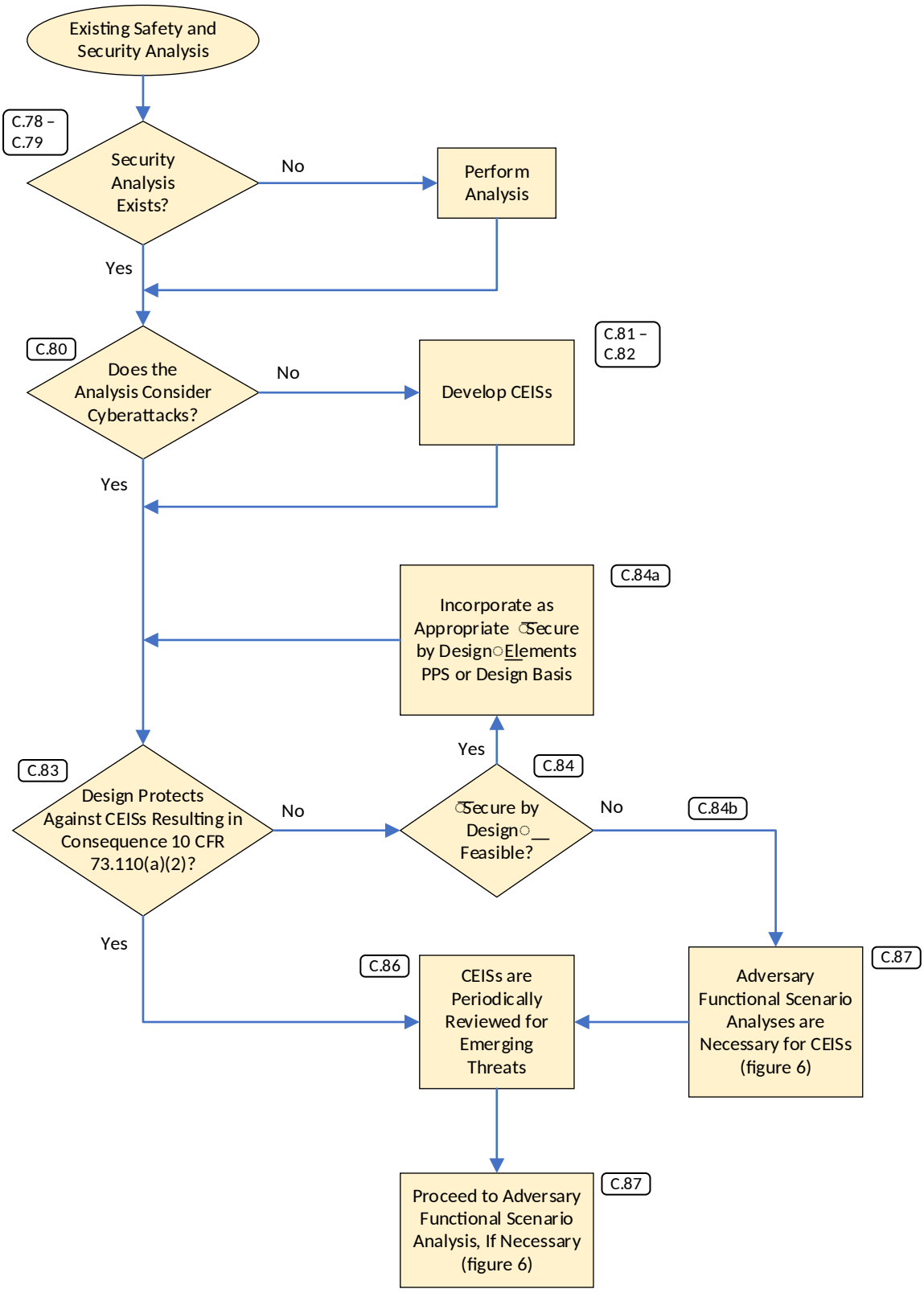


Figure 5. Cyber Extension to Intrusion Scenario Analysis for Physical Intrusion Consequence in 10 CFR 73.110(a)(2)

Adversary Functional Scenario Analysis

88. If any CEIS or CEAS results in the consequences listed in 10 CFR 73.110(a), then the licensee should perform an AFSA to further assess the potential consequences from such scenarios. This analysis excludes all CEISs and CEASs completely protected by SeBD elements (e.g., noncyber IPLs, analog systems, passive system/barriers).

89. The AFSA aims to provide plant capability defense in depth by specifying prohibitive CSP elements (e.g., forbid use of wireless communications) and passive, deterministic DCSA elements to mitigate or control adversary access to attack pathways or eliminate these pathways. Figure 6 describes the AFSA.

90. The analysis depicted in figure 6 emphasizes the relationship between critical security programs and processes. For example, the DCSA depends on support from processes and procedures, especially to protect against insider threats. The CSP should be coordinated with the insider mitigation program to ensure that DCSA protections remain effective.

91. The outputs from the AFSA include the complete list of DCSA elements, which are the initial elements to be addressed by the CSP with special focus on insider protections and the relationship to DCSA. (The DCSA elements support the SeBD concept by minimizing adversary access and mitigating the cyber-related risks of already identified safety and security events with special focus on understanding and controlling personnel activities.)

92. The essential element of the AFSA is the assumption that the adversary is able to compromise functions in any manner that allows for progression of attack scenarios (i.e., attack success) immediately upon adversary access.

93. For each CEIS and CEAS, the following attack pathways should be considered:

    a. physical access,
    b. wired communications,
    c. wireless communications, and
    d. portable media/device connectivity.

94. The supply chain attack pathway is addressed separately in sections C.145 through C.151, which provide guidance for mitigating the risk associated with such a pathway that may allow an adversary to compromise the system function(s) in a way that advances the CEAS or CEIS.

95. If the adversary can potentially advance a CEAS or CEIS to completion, the CSP or DCSA may need to include additional mitigation. A necessary attribute of these additional mitigation measures is that they do not require action by licensee personnel or action by a digital system to deny the adversary access to the attack pathway. The following are some mitigating measures that can be considered for inclusion:

    a. prohibitive CSP elements, such as prohibition of wireless for critical systems, remote access, or other capabilities that allow the adversary to access the attack pathway;

    b. location of critical systems within inaccessible or protected locations that will always deny adversary access; and

c. passive and deterministic technical measures needed as part of the DCSA implementation, such as a data diode or unidirectional taps.

96. Based on the analysis, the DCSA and CSP implementation should address the following:

a. Eliminate attack vectors. For example, the DCSA implements a deterministic, unidirectional communications pathway to eliminate access to wired networks from remote or adjacent networks. Another example is a CSP implementation that forbids wireless communications within critical systems.

b. Mitigate attack vectors using the following means:

(1) *Minimize attack vectors*. For example, the DCSA implementation places critical systems within the most secure boundaries with supporting CSP implementation of licensee-identified procedures that strictly control physical access to these systems.

(2) *Control access to attack vectors*. For example, CSP implementation of licensee-identified technical and administrative controls supplements the physical control measures of critical systems.

(3) *Detect unauthorized access to attack vectors*. This capability will rely on items b(1) and b(2) to increase the likelihood of detecting such access. For example, the CSP implements licensee-identified technical and administrative controls to detect unauthorized access to critical systems.

97. It may be necessary to bound certain analysis to be valid for specific plant states (e.g., operation, outage, construction) to simplify the analysis. If this is necessary, the licensee should consider all states for which the CSP will be in effect and cover all adversary functional scenarios that could occur during the specific plant states.

98. The licensee may specify multiple DCSAs based on different considerations such as the following:

a. type of system(s) (e.g., physical protection, safety, EP, BOP),

b. plant lifetime stage (e.g., design, construction, commissioning, operation, decommissioning), and

c. other considerations (e.g., security/trust model, organization).

99. The licensee should perform the following:

a. Document the AFSA associated with each analyzed CEIS or CEAS.

b. Identify the mitigation measures (e.g., prohibitive CSP elements, locations, DCSA elements) and PPS elements that provide the capability to mitigate or eliminate adversary access to attack pathways. (Special attention by the licensee will be required to manage potential cybersecurity supply chain risks for these mitigations and quality assurance based on their contribution to preventing cyberattacks.)

100. If the AFSA demonstrates that adversary access to the attack vectors necessary to complete a CEIS or CEAS scenario is prevented, then the licensee should do the following:

a. Implement the baseline cybersecurity program, baseline DCSA, and cybersecurity supply chain risk management in accordance with sections C.145 through C.151 to protect those functions identified in the analysis.

b. Implement additional protective measures and mitigations as identified in section C.99.

c. Incorporate measures for periodic review and validation of the AFSA within the licensee's management system.

101. Each CEAS or CEIS in which attack vectors are still available for each stage in the scenario progression should result in further system-level analysis in accordance with sections C.104 through C.105. These analyses include the following:

a. system analysis to identify critical functions confirming the CEAS and CEIS analysis at the system level (figure 7),

b. categorization of systems allowing for the application of a graded approach (figure 8), and

c. ATS analysis for each adversary functional scenario that could result in the CEIS or CEAS (figure 9).

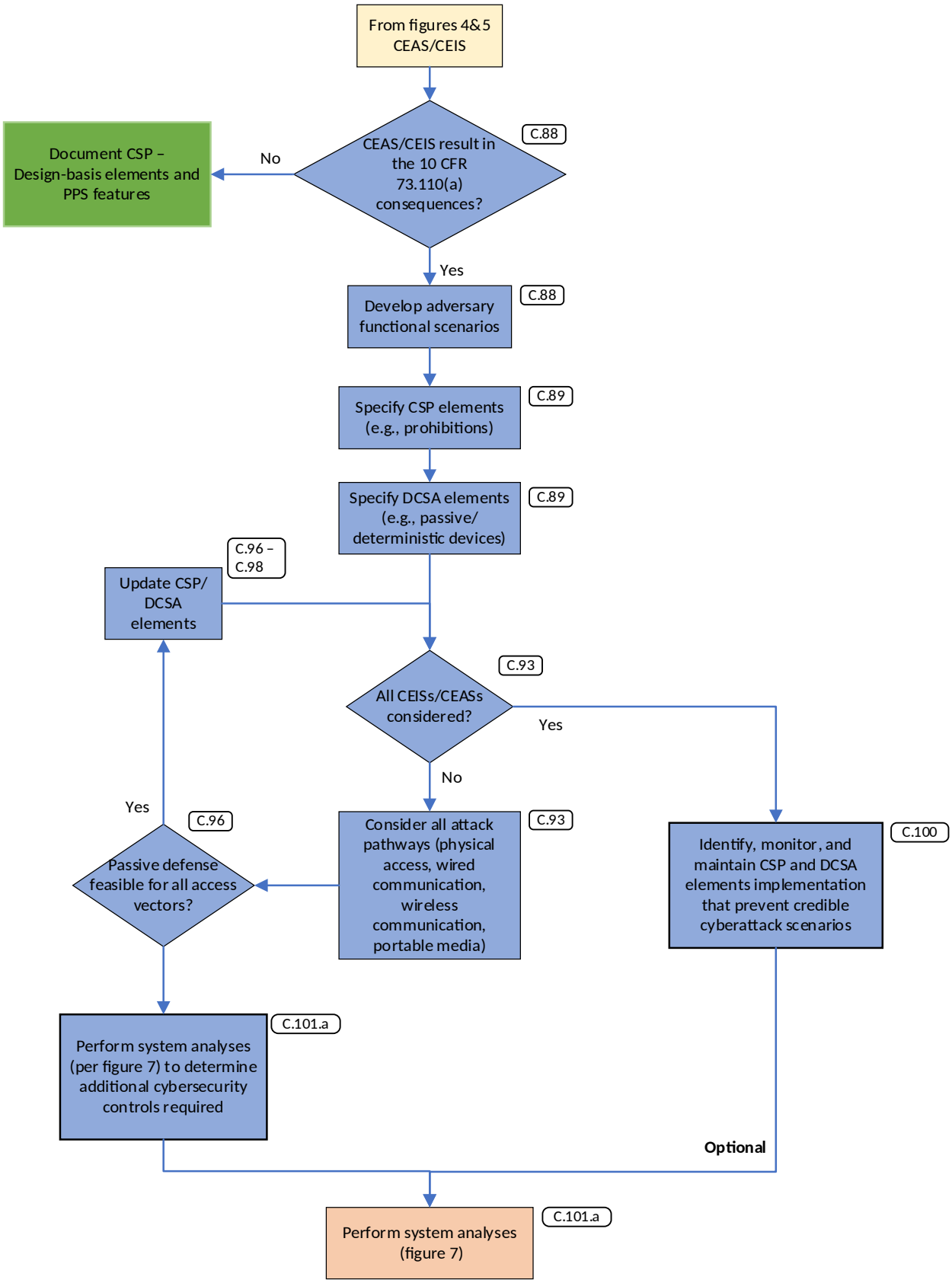


Figure 6. Adversary Functional Scenario Analysis

102. Sections C.156 through C.160 provide guidance related to DCSA implementation.

103. Sections C.136 through C.138 discuss relevant CSP sections.

System-Level Analysis

104. This section expands the system-level analyses detailed in the following figures: figure 7 for identification of critical functions performed by a system, figure 8 for grading systems, and figure 9 for determining the selection and implementation of cybersecurity controls. Pursuant to 10 CFR 73.110(e)(4), these would be periodically reviewed and updated, depending on discovered vulnerabilities to emerging threats, advances in adversary capabilities, or newly identified intrusion or accident scenarios.

105. System-level analyses should be conducted wherever an AFSA demonstrates that there is a potential for an adversary to successfully complete a CEIS or CEAS.

System Critical Functions

106. If the facility scenario analyses in accordance with sections C.65 through C.103 have not and will not be performed, the licensee may implement the 10 CFR 73.54 requirements and associated performance objectives.

107. In accordance with 10 CFR 73.110(b)(1), a licensee would identify digital assets that should be protected to satisfy the requirements in 10 CFR 73.110(a) through (c). The analysis discussed here provides an independent assessment of the system and the identification of critical functions that the system performs or supports.

108. For all CEASs or CEISs where attack pathways exist at each stage to allow the adversary to advance the scenario, the licensee should document the set of functions targeted in each scenario. This set of functions whose compromise could result in the 10 CFR 73.110(a) consequences would be the "critical functions" (see sections C.75(a) and C.85(a)).

109. For the system under consideration, all functions that the system performs or supports should be identified. These functions are then compared to the set of critical functions associated with the CEAS or CEIS. Systems that perform or support critical function(s) should result in the review of the associated CEAS or CEIS and AFSA, if available, to confirm that system design and the implementation do not invalidate the assumptions made in the analyses.

110. If one or more of the assumptions of the facility scenario analyses have been invalidated, one or more of the following may be necessary:

    a. Repeat the facility scenario analyses for the critical functions of the system, with subsequent updates to important cybersecurity elements identified in the analyses, CSP, or DCSA that eliminate the risk.

    b. Update the assumptions of the facility scenario analyses and repeat the necessary subsequent processes.

    c. Update or customize alternative compensating measures within the CSP, DCSA, or both to allow for protection of the system and its critical functions.

111. If the facility scenario analysis is still valid, and the system performs or supports critical functions, the system can then be categorized (graded) as critical and noncritical functions, as shown in figure 7.

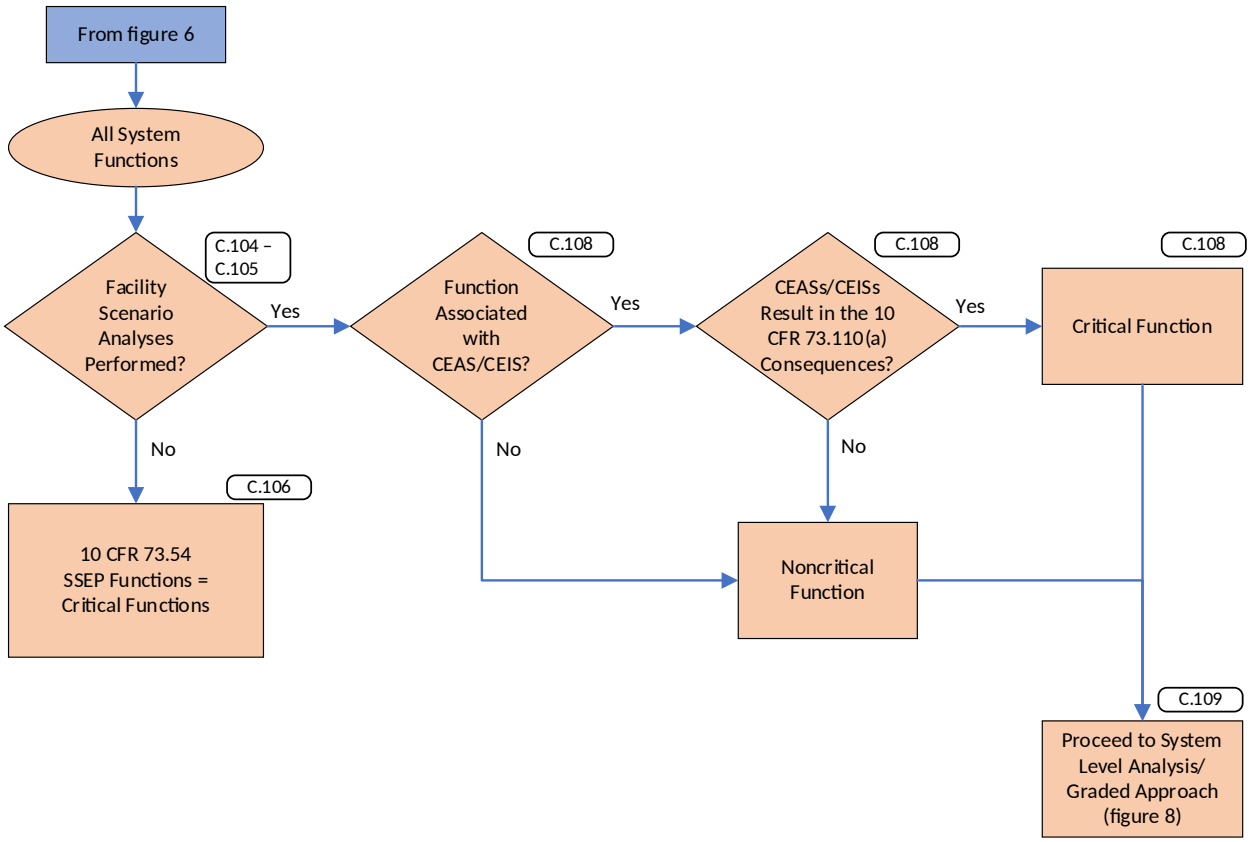


Figure 7. Identification of a System's Critical Functions

Categorization of Critical Systems

112. Categorization of critical systems is an optional assessment that allows for application of a graded approach with respect to the selection and implementation of cybersecurity control measures. The most critical systems will require assessment of all control measures listed within the organization's control catalog (see figure 9). Least critical systems will allow the licensee some flexibility and discretion with respect to control measures. Noncritical systems will not require the implementation of security controls, but they are recommended for enhancing the defense-in-depth posture of the DCSA.

113. For each system (including support systems[2]) associated with an AFSA, the licensee should determine whether the system does the following (in order of significance):

[2] Support systems may include but are not limited to (1) electrical power systems, (2) cybersecurity systems (e.g., firewalls, anti-malware scanner, intrusion detection system), and (3) systems that provide resources to other systems (e.g., service water, high-pressure air, lubrication oil).

a. performs one or more critical functions,

b. relies on or supports a single or more than one critical function, or

c. adversely affects a critical function(s) if compromised (e.g., a system that is used to scan the portable media for any malware before uploading the software into digital assets that support critical functions).

114. The licensee may perform an analysis that provides justification that a critical function is performed by alternative means. Figure 8 shows the credit for this analysis, which would allow for a licensee to categorize the associated system as "least critical." The AFSA should confirm that the categorization of such a system does not invalidate the analysis of the CEIS or CEAS.

115. The licensee may develop a graded approach (e.g., security degrees or levels) that incorporates the grading depicted in figure 8 with other considerations, such as functions provided by alternative (noncyber, diverse) means, safety defense-in-depth level, or security defense-in-depth level. The licensee should provide an analysis to justify a reduction of protection based on these other considerations.

116. Each system that meets any of the criteria in figure 8 should be considered a critical system. However, the graded approach may be used to inform whether a specific control should be implemented and the stringency with which a control is applied.

117. Each critical system should be located within an area with secure physical and logical boundaries (i.e., computer security zone). The level of security applied for these areas can be graded based on the system categorization (e.g., most critical, least critical).

118. If a graded approach is applied, the DCSA implementation should provide increasing levels of protection for these computer security zones containing critical systems. The zone assigned to a critical system and its location within the DCSA should be commensurate with the level of protection required by the system.

119. The updated DCSA should have multiple layers of diverse and independent measures to prevent adversary access to equipment, detect such access, limit impacts from such access, and provide defense in depth. The DCSA should consider limiting the number of critical systems that can be placed within a zone, as this reduces the potential for common-cause access (i.e., the adversary can access attack vectors for many critical systems based on bypassing or compromising a single boundary) and reduces the complexity of the zone, making detection and response less challenging.

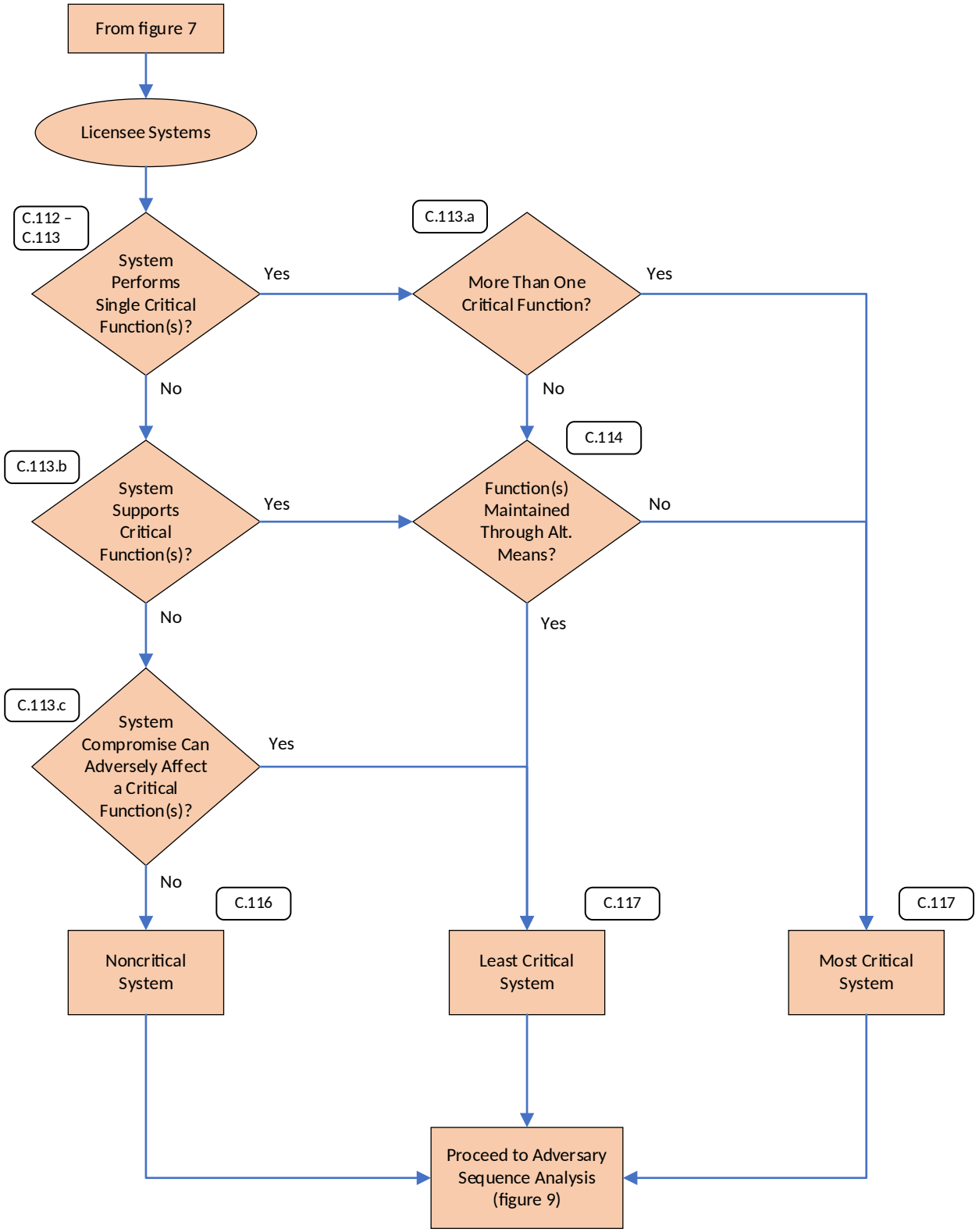


Figure 8. Categorization of Critical Systems

Adversary Technical Sequence Analysis

120. ATSs are associated with potential major consequences and impacts on the functionality of computer systems, which may, directly or indirectly, compromise the safety and security of the facility. For this reason, 10 CFR 73.110(c) requires the licensee to meet the CIA requirements in 10 CFR 73.54(a)(2) for the systems and networks covered by 10 CFR 73.110(b) in a manner that is commensurate with the potential consequences resulting from cyberattacks.

121. The licensee should perform an analysis to determine all controls that are needed for each CEIS and CEAS that has a credible adversary functional scenario. The ATS analysis assumes the protections are in place from the DCSA and CSP implementation.

122. When developing ATSs, the licensee should consider the technological trends and ease of access to attack technologies. In developing preventive measures against cyberattacks, it is very important to understand the nature of the attacks and the potential pathway(s) that an adversary may use to gain relevant information and access to target computer systems. The outcome of the analysis should identify potential impacts of successful cyberattacks on the assessed systems and the corresponding impacts on the facility in terms of the consequences. In addition, CIA requirements should be more thoroughly assessed for critical systems to ensure that required measures are correctly implemented.

123. The ATS analysis includes the following:

    a. identification of all digital assets and networks with zones containing critical systems;

    b. identification and analysis of all routes (e.g., attack pathways) through which digital information transfer can occur, including supply chain;

    c. analysis of CSP and DCSA elements to determine their effects on adversary tactics, techniques, and procedures, including existing countermeasures in preventing adversary access and tactics, mitigating the effects of compromise, and ensuring effective detection and response to cyberattacks targeting the system under consideration; and

    d. concurrent and successive cyberattacks targeting systems needed to protect or mitigate the impacts from radiological sabotage (e.g., EP) or physical intrusion should be analyzed for those CEISs and CEASs in which postattack action may be necessary to minimize the consequences.

124. The ATS analysis has the following outputs:

    a. identification of additional system (or internal zone) controls that are necessary to protect digital assets against cyberattacks associated with a consequence defined in 10 CFR 73.110(a);

    b. information on whether the planned detection and response measures determined by the licensee are sufficient to protect against the adversary compromising the system within a specified time period that allows for progression of the CEIS or CEAS (including AFSA) to completion (these licensee-identified performance measures will be most demanding for the most critical systems); and

    c. statement of applicability with the elements listed in this section.

125. All components within the zone that rely on digital technology (i.e., are susceptible to cyberattack or electronic compromise) within either a development, maintenance, or operational environment should be identified as digital assets, while noncyber assets are excluded.

126. The licensee may conduct an analysis to determine if specific digital assets (1) do not fulfill any of the conditions in section 1133, (2) do not need to be placed in the same zone as the critical system, and (3) do not provide a means for the adversary to access an attack pathway for a critical system. If these conditions are met, then the licensee may exclude such assets from identification.

127. All pathways listed in section 933 and the supply chain attack pathway need to be considered when assessing the potential for compromise of critical systems. The information flow attributes (e.g., type, direction, impact) and the countermeasures that prevent, limit, monitor, or control these information flows should be identified. The information flow and its attributes may indicate the system lifecycle phase(s) where the flow is possible, which may simplify the implementation of countermeasures needed to address specific phase(s).

128. Once all digital assets and information flows have been identified, ATSs should be developed. These ATSs may refer to attack analysis frameworks (e.g., MITRE ATT&CK (Ref. [36]), cyberthreat framework from the Office of the Director of National Intelligence (Ref. [37])) to structure and provide sufficient detail for the sequences. The analysis should cover all credible attacks derived from those applicable publicly disclosed attacks. The licensee may record and update a knowledge base consisting of the set of applicable attacks to ensure adequate coverage.

129. Once a suitable set of ATSs has been developed, the licensee should do the following:

    a. Confirm the effectiveness of existing CSP and DCSA elements in protecting against all or part of an ATS(s).

    b. Identify ATSs that are not addressed by CSP and DCSA elements, especially those focused on controls that detect, control, or recover from cyberattack.

    c. Implement controls to prevent, detect, and respond to any ATS with the potential to lead to a CEAS or CEIS.

    d. Specify performance-based and graded requirements through an analysis that determines the overall detection and response security controls necessary to intercept and interrupt the progression of the sequence to completion if system categorization was performed. The facility scenario analyses inform the overall licensee-identified measures.

    e. Implement all licensee-identified required controls and confirm that the 10 CFR 73.110 performance-based and graded requirements would be met. The set of ATSs should be used to develop tests that are verified in support of this step, and both the test procedures and the test results should be made available upon request for review by the regulatory authority.

130. Figure 9 outlines the process in section C.1299.

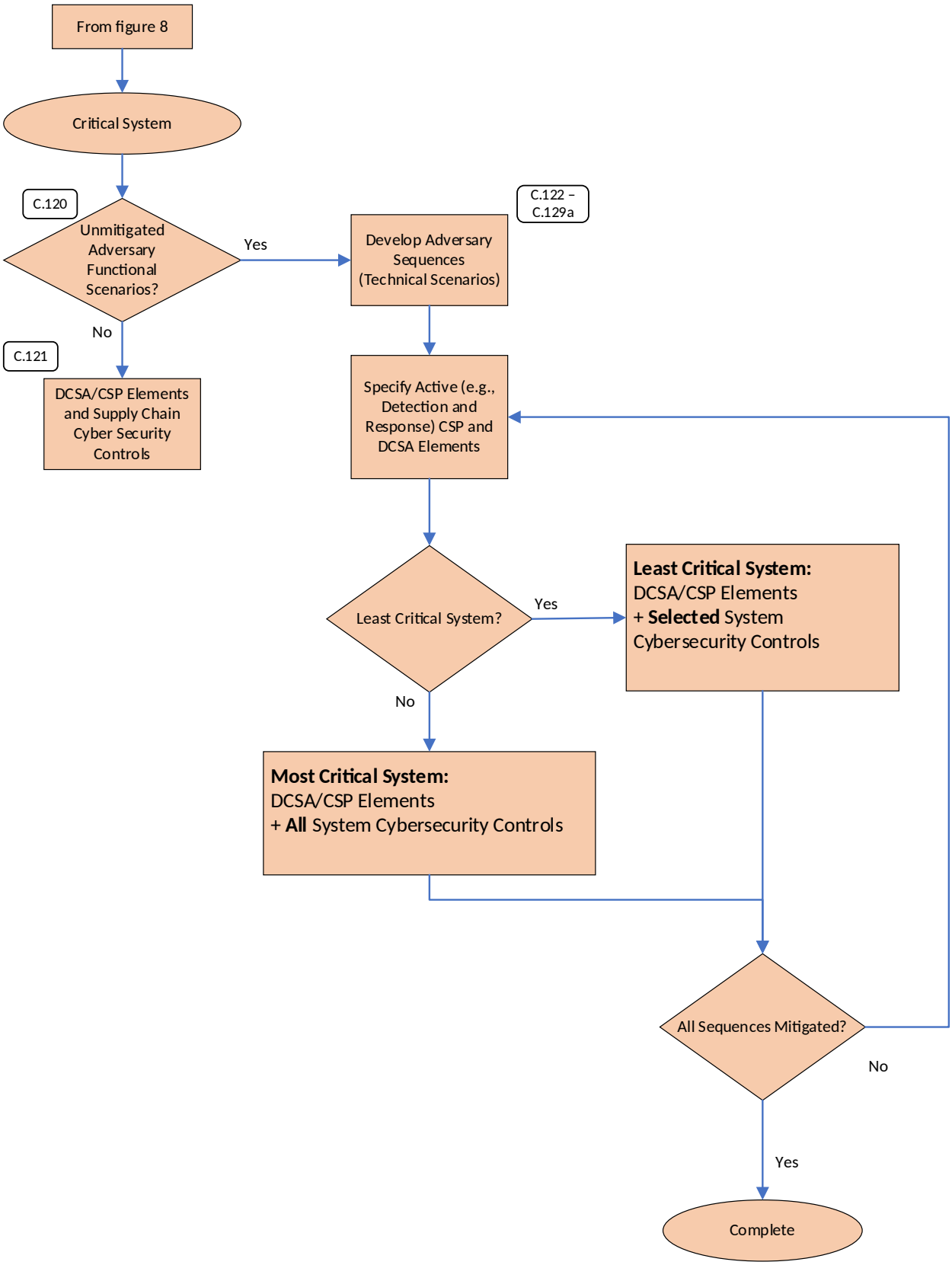


Figure 9. Adversary Technical Sequence Analysis

131. For the ATS analysis, the licensee may use any standard control catalogs (e.g., IEC 63096; RG 5.71, appendices B and C; NEI 08-09, Revision 6, appendices D and E; NIST SP800-53; NIST SP800-82; ISO/IEC 27002) or an organizational specific control catalog. If a customized control catalog is used, the licensee should perform an equivalency evaluation to RG 5.71 to demonstrate that protection is maintained or enhanced.

132. The licensee should compare the cybersecurity controls to the licensee-identified security measures specified within the facility scenario analyses and ATS analysis and confirm that no necessary controls have been omitted. If a graded approach has been used (e.g., IEC 63096), implemented controls can be commensurate with the level of protection required to protect digital assets against cyberattacks associated with a consequence defined in 10 CFR 73.110(a).

133. As part of the CSP development, the licensee should produce a statement of applicability (see Ref. 31) or similar document that contains the following:

    a. the necessary controls,

    b. justification for their inclusion (e.g., detect adversary access to attack pathways as required by adversary scenario),

    c. whether the necessary controls are implemented, and

    d. the justification for excluding any controls (e.g., crediting DCSA protection, which provides the required level of protection).

134. The licensee should periodically demonstrate that the controls are effective in mitigating all ATSs with the potential to lead to a CEAS or CEIS, thereby reducing the risk from these sequences and scenarios to an acceptable level.

135. Sections C.139 through C.141 provide additional guidance on the identification of digital assets.

Elements of a Cybersecurity Plan

136. As required by 10 CFR 73.110(e)(2), a licensee must establish, implement, and maintain a CSP that implements the cybersecurity program requirements in a manner that is commensurate with the potential consequences of cyberattacks. Additionally, the CSP should describe how the licensee will implement the requirements of the regulation, considering site-specific conditions that affect implementation, to provide reasonable assurance that critical functions are protected from cyberattacks in a manner commensurate with the potential consequences resulting from compromise of system functions due to cyberattack.

137. This section lists the necessary elements of a CSP, as required by the rule. For cases in which the potential consequences from a cyberattack for a given commercial nuclear plant design do not lead to the consequences listed in 10 CFR 73.110(a), the CSP would be limited to documenting the risk analysis performed by the licensee in support of reaching such a conclusion.

138. To further guide licensees, appendix A to this RG provides a generic CSP template that can be used to develop a CSP and to establish and maintain a CSP that will comply with this regulation. RG 5.71, section C.2, contains additional information on this topic.

Identification of Digital Assets Associated with Critical Systems

139. As required by 10 CFR 73.110(b)(1), a licensee would identify digital assets that must be protected in a manner that is commensurate with the potential consequences resulting from cyberattacks. This RG provides one acceptable approach a licensee may use to determine which digital assets require cybersecurity controls in a manner that is commensurate with their safety and/or security significance.

140. The outcome of the risk assessment discussed in sections C.19 through C.64 should be used for identifying the digital assets that would be required to be protected in accordance with 10 CFR 73.110. As shown in , a cyberattack that results in the consequence defined in 10 CFR 73.110(a)(1) would require the protection of digital assets associated with critical functions such as safety, security, and EP. EP functions should be included within the scope of the risk assessment because they are essential to mitigating the consequences of radiological sabotage (i.e., they are part of the defense-in-depth strategy). Similarly, a cyberattack that results in the consequence defined in 10 CFR 73.110(a)(2) would require the protection of digital assets associated with security functions. Additional information on this topic can be found in RG 5.71, section C.3.1.3.

141. The BOP systems that are beyond the first intertie[3] with offsite power distribution systems would not be considered to be within the scope of 10 CFR 73.110. All BOP systems and components within this intertie that meet the definition of a digital device are within the scope of the risk assessment discussed in sections C.19 through C.64. The North American Electric Reliability Corporation survey, known as the "Bright-Line Survey," could be reviewed to assist in identifying the physical and logical boundary for BOP systems and components. RG 5.71, section C.3.1.3, and an NRC letter (Ref. [38]) contain additional information on this topic.

Cybersecurity Controls

142. A cybersecurity control contains performance specifications used to inform the measures taken to detect, protect against, or respond to a cyberattack capable of causing a consequence of concern. The performance specification of a cybersecurity control is satisfied by taking measures in a manner that is commensurate with the potential consequences from cyberattacks. To effectively protect digital assets against cyberattacks associated with a consequence defined in 10 CFR 73.110(a), a licensee would establish and maintain cybersecurity controls as required by 10 CFR 73.110(d)(1). As required by 10 CFR 73.110(e)(2), the licensee's CSP would document the cybersecurity controls.

143. Appendices B and C to RG 5.71 provide acceptable lists of technical controls, operational controls, and management controls to address potential cybersecurity risks. Additional control catalogs from recognized U.S. national (e.g., NIST SP800-53, NIST SP800-82) or international standards (e.g., ISO/IEC 27002, IEC 62443 series, IEC 63096) or a customized catalog may be used (with equivalency evaluation). The implemented controls should follow the licensee-identified guidance specified in sections C.65 through C.103 during the facility scenario and ATS analyses by applying a risk-informed, performance-based approach. Additional information on this topic can be found in RG 5.71, section C.3.3.

[3] Electricity interties are transmission lines that connect separate electric grids.

Configuration Management

144. Configuration management processes maintain plant capability for defense in depth (e.g., SeBD, passive features, analog systems, DCSA), as well as ensuring that plant systems are operated and maintained securely. Many vulnerabilities and weaknesses are the results of insecure configurations in the operating, maintenance, or development systems. Configuration management, including quality assurance elements, should include the CSP and DCSA elements that are part of the cybersecurity controls. RG 5.71, section C.3.3, contains additional information on this topic.

Supply Chain

145. Information and cybersecurity are essential to reducing the risk to critical functions from supply chain risks (Ref. 29). Identification and analysis of sensitive information, cybersecurity and information security assurance requirements, CEAS, CEIS, AFSA, ATSs, including controls and information flows are necessary to ensure that the correct contractual requirements are specified. Information security assurance is necessary to ensure the protection of confidentiality (unauthorized information release), integrity (unauthorized information modification), and availability (unauthorized denial of use) of information created, transferred, used, or archived by organizations within the supply chain.

146. Reducing the risk to critical systems that can be compromised through cyberattack targeting the supply chain is essential. The significance of the data or system may require licensee-identified security requirements for supply of products and management throughout the entire procurement process. Appendix C to RG 5.71, section C.12, has more information on supply chain management controls.

147. The supply chain attack vector provides adversaries with increased opportunities to access digital information and systems (e.g., during development, shipment) and to maliciously alter the function (e.g., by altering a digital asset). It is possible that compromise of functions while in development is not observable, and there could be increased opportunities for the adversary to use stealth. These opportunities provide tremendous value to potential adversaries.

148. Supply chain relationships add to risk complexity as suppliers might be relied on to directly provide the function, support the correct operation of the function (e.g., design services, maintenance, inspection), or provide information on which critical attributes of function assignment, performance, or validation depend.

149. Attack pathways not available at the licensee (e.g., prohibited by CSP or prevented by DCSA) may be present at the supplier(s). It will be necessary to identify those attack pathways that may invalidate the facility scenario analysis. In such cases, an additional facility scenario analysis should be performed to identify and specify alternative compensating measures.

150. The concept of supply chain attack surface may be used for the management of information and computer security associated with supply chain relationships. Understanding and minimizing the attack surface and implementation of a DCSA and computer security measures by the acquirer are key to establishing effective risk management and defense in depth to protect both information and digital assets in the supply chain.

151. Security controls can be taken or derived from RG 5.71, section C.12, or from other U.S. national standards on supply chain risk management (e.g., NIST, U.S. Department of Defense) or

international standards (e.g., International Telecommunication Union, ISO/IEC). However, given the consequences defined in 10 CFR 73.110(a), additional measures for critical systems would need to be considered.

Cybersecurity Measures for Critical Systems

152. The following items should effectively manage the risk associated with an item or service that has the potential to compromise critical systems:

a. The type of procurement purchase that is allowed—It is expected that direct commercial off-the-shelf purchases will be restricted. The types of suppliers and their subsuppliers that require cybersecurity (Ref. 27).)

b. The level of cybersecurity system hardening required—The AFSA and ATS analysis may provide insights into key aspects of hardening that should be defined.

c. The applicable or alternative compensating DCSA measures necessary to comply with AFSA and ATS analysis.

d. The importance of establishing a process whereby the supplier provides dedicated support (on site or remote during information and computer security incidents.

e. The mean tolerable outage time for the item or service before the impact is realized (or becomes irreversible)—This may assist in ATS analysis to define performance-based measures for detection and response.

Cybersecurity Measures for Most Critical Systems

153. In addition to the guidance in section C.152, the following measures could effectively manage risk associated with an item or service that has the potential to result in severe impacts:

a. All suppliers are identified and controlled by direct and formal contracts.

b. All CEIS, CEAS, AFSA, and ATS analyses are identified, and measures or countermeasures have been implemented to ensure that regulatory requirements in 10 CFR 73.110 are met.

c. Cybersecurity hardening is performed by all relevant entities before delivery, and the licensee verifies that all devices and systems are hardened:

(1) The licensee should require the vendor or supplier to perform device or system hardening (e.g., by the purchase ordering or requirements document).

(2) The licensee should verify the hardening upon delivery.

d. Licensees work with vendors to ensure that devices and systems are secure. Stringent computer security measures may conflict with end user license agreements or other legal arrangements. For example, a vendor does not permit source code to be subjected to a static code analysis when the source code is deemed intellectual property (sensitive to the vendor) and will not be released (or limited to escrow or in trust release upon certain conditions). Therefore, the vendor will need to perform the tests and provide the "sanitized" results to the licensee for acceptance. An alternative would be the use of nondisclosure agreements that require results, observation, or code review.

Establishing and Implementing a Cybersecurity Program

154. The regulations in 10 CFR 73.110 establish an overall performance-based requirement to ensure that the functions of digital computer and communication systems and networks are protected in a manner that is commensurate with the potential consequences resulting from a cyberattack. One method of complying with these regulations is to implement and maintain a cybersecurity program that consists of a DCSA, described in sections C.156 through C.160, and the security controls described in sections C.104 through C.135.

155. As required by 10 CFR 73.110(b)(2) and 10 CFR 73.110(d), a commercial nuclear plant licensee must establish, implement, and maintain a cybersecurity program that protects digital computer and communication systems and networks associated with the critical functions of a nuclear facility. This RG describes an acceptable method for establishing, implementing, and maintaining a cybersecurity program to comply with the regulations.

Defensive Cybersecurity Architecture

156. An adequate DCSA implementation for effectively protecting against a cyberattack should reflect the following principles:

a. Defensive model: The design of the defensive architecture for digital systems and networks to protect against a cyberattack should establish the logical and physical boundaries between digital assets with similar risks and digital assets with lower security risks. Most critical systems should be located at the highest security levels and protected from lower levels. A formal or semiformal security model may simplify verification and validation of DCSA implementation.

b. Cybersecurity defense in depth: A defense-in-depth protective strategy consisting of complementary and redundant cybersecurity controls should be used to establish layers of protections to safeguard critical digital assets, critical systems, or both. The failure of a single protective strategy or security control should not result in the compromise of functions such as those associated with safety, security, or EP.

c. Least functionality: The design of the digital assets and digital communication systems should incorporate the principle of least functionality. The design should do the following:

(1) Eliminate unused or unnecessary functionality, protocols, ports, and services capable of being used in a stage of a cyberattack.

(2) Disable unused or unnecessary functionality, protocols, ports, and services and protect against enabling and use of the capabilities in a stage of a cyberattack.

(3) Provide protections to prevent the use of unused or unnecessary functionality, protocols, ports, and services in a stage of a cyberattack when eliminating or disabling the capabilities is not practical.

157. Additional considerations for specification of the DCSA may include the following:

a. The definition of logical and physical boundaries for secure areas (e.g., zones) must be clear, concise, and verified with the implementation for critical systems. Most critical systems should be located within zones where the logical and physical boundaries are completely aligned (e.g., the logical network does not extend past the physical boundary). Decoupling devices such as data diodes may be used to limit the logical boundary.

b. Most critical systems should be located in zones that prioritize simplicity. This aids in the implementation of boundaries and measures aimed at preventing, detecting, and responding to cyberattacks. System or network anomalies within simple zones are more readily observable, and subsequent analysis is eased to increase the likelihood of detection and determination of the necessary response activities.

c. Zones containing critical systems should limit the number of functions that are protected by the secure boundaries. Functions and systems that do not require location within the same zone should be considered for placement in other zones.

d. Most and least critical systems should be located in the most secure zones of the DCSA. The DCSA should aim to minimize the number of attack pathways that are accessible. The AFSA and ATS analyses can inform the location of these systems within the DCSA.

158. The DCSA may consider support for a cybersecurity operations center (CSOC) that provides the following:

a. Realtime continuous monitoring aimed at verification that cybersecurity requirements are met: This would fulfill many information security assurance objectives that are required by the licensee-developed baseline CSP, supply chain, and DCSA requirements. Specifically, a CSOC with security information and event management (SIEM) capabilities could verify that the plant is operating securely and complies with necessary requirements and regulations.

b. Improved detection and response capability to meet the performance requirements specified during the licensee-conducted ATS analysis: The CSOC may implement security orchestration, automation, and response capabilities; however, the licensee may require performance of an AFSA and ATS analysis to determine whether the CSOC provides access to attack pathways due to interactions between the monitored systems and the CSOC. Addendum 2, “Cyber Attack Detection, Response and Elimination,” to NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors” issued in 2009 (Ref. [39]), contains additional guidance regarding cyberattack detection and response.

159. Access, control, or monitoring from remote locations may be necessary to perform tasks and activities. In these instances, the licensee-developed DCSA implementation should indicate the conditions and the elements that allow for these tasks and activities to occur. This should include support for CSP elements and implemented controls to provide the appropriate protections. The

provision of remote access and control needs to ensure that attack pathways, specifically those of wired and wireless networks, are not permitted for any stage of a CEAS or CEIS.

160. Additional guidance on this topic appears in RG 5.71, section C.3.

Maintaining the Cybersecurity Program

161. After fully implementing the cybersecurity program by identifying and protecting its critical systems and associated digital assets, the licensee would implement a configuration management system to ensure that changes to the facility are properly evaluated in accordance with 10 CFR 73.110(e). This system ensures that changes (e.g., addition, modification, or removal of devices and equipment) are evaluated before their implementation and that they do not adversely impact the licensee's ability to meet the cybersecurity program objectives. The licensee would document this system in written procedures and can add it to an existing site design, configuration management, or improvement program. As part of this system, the licensee would document the baseline configuration for the system and devices used in the facility. For cases where the potential consequences from a cyberattack for a given commercial nuclear plant design do not lead to the consequences listed in 10 CFR 73.110(a), maintaining such a configuration management system is vital to ensure that any changes do not invalidate the conclusions reached by the licensee as part of the original risk assessment; otherwise, the licensee should take the necessary actions to ensure that the cybersecurity performance objectives defined in 10 CFR 73.110 are met in light of the changes.

162. The configuration management system should establish the appropriate procedures for documenting the evaluation and approval of additions or changes associated with critical systems and associated digital assets. Evaluating additions or changes may be done through a cybersecurity impact analysis (e.g., facility scenario analyses, system-level analyses). When properly implemented, the configuration management system should protect against improper or unintended changes to the CSP. Furthermore, the licensee should consider a sitewide approach by incorporating cybersecurity configuration management into the planning process for the facility.

Cybersecurity Impact Analysis

163. An acceptable way for the licensee to address configuration management for cybersecurity would be to conduct a cybersecurity impact analysis as a part of a proposed change. A cybersecurity impact analysis examines the proposed change to determine whether it could introduce vulnerabilities allowing a cyberattack to result in the consequences in 10 CFR 73.110(a). This impact analysis is supported by the system-level analyses that assist in managing potential vulnerabilities, weaknesses, and risks introduced by changes in the system, network, environment, or emerging threats.

164. The cybersecurity impact analysis should identify adjustments or actions affecting the CSP, DCSA, or other elements as a result of the proposed change. The effort would also determine whether the proposed change would affect or degrade existing alternative means and measures taken to address cybersecurity controls. Additionally, this impact analysis would determine whether adjustments would be required to maintain the effectiveness of the existing detection functions or implementing procedures. Furthermore, this impact analysis would consider the potential effects that the proposed change would have on the CSP, other documentation, or processes.

165. Before making a design or configuration change to a critical system and associated digital assets or when changes to the environment occur, a licensee should, at a minimum, demonstrate that the proposed change (1) does not introduce unaddressed cybersecurity vulnerabilities that would allow a cyberattack to result in unacceptable consequences, and (2) maintains the protection established by the measures taken to address controls, detection schemes, and the availability of alternate means. At the completion of the analysis, a licensee may need to address cybersecurity vulnerabilities identified in the analysis, as required by 10 CFR 73.110(e)(2).

Sitewide Considerations

166. The results of a cybersecurity impact analysis, revisions to implementing procedures, and other applicable considerations should be shared with the appropriate facility design and operations personnel to ensure that the implementing procedures are properly executed. Changes as a result of the procedure should be tested and verified before use in the licensee's production environment when technically feasible. As part of the overall process, critical systems and their associated digital assets should not be considered sufficiently protected until the implementing procedure has been completed and validated and the corresponding measures have been taken to address the performance specifications of the cybersecurity controls.

167. Through the configuration management system, the licensee should implement a process for ensuring that cybersecurity testing, training, and monitoring activities associated with critical systems are properly maintained. The licensee should confirm that these actions continue to be executed in a timely manner and are consistent with the CSP as changes occur to the facility, critical systems, and their digital assets.

168. In accordance with 10 CFR 73.110(e)(4), the licensee must periodically review its CSP. The periodic review serves to evaluate the overall effectiveness of the CSP. An acceptable approach includes an audit of the effectiveness and adequacy of the CSP, including, but not limited to, a review of the following:

    a. purpose, scope, roles, responsibilities, requirements, and management support of the CSP;

    b. changes made to implementing procedures;

    c. measures of performance established through cybersecurity controls and whether the licensee developed, monitored, and reported on the results of these performance measures;

    d. cybersecurity control strategy;

    e. use of alternative compensating measures and DCSA for critical systems;

    f. configuration management system; and

    g. changes made to the operating environment.

169. The licensee should develop and implement procedures to facilitate and maintain the periodic review. Individuals independent of those personnel responsible for CSP management or implementation should complete these reviews.

170. When the review is completed, the licensee tracks in a timely manner and formally documents the findings, deficiencies, and recommendations resulting from the review in a record. This record may take the form of a report that includes management's findings on CSP effectiveness and actions taken as a result of recommendations from prior CSP reviews. The licensee must maintain records in an auditable format and make them available, upon request, for inspection by the NRC. The results of the periodic review may initiate changes to (1) the CSP, (2) the cybersecurity controls or alternate means, or (3) the implementing procedures for critical systems and associated controls.

171. Consistent with 10 CFR 53.1565(d)(4), a change that would result in a decrease in the effectiveness of the CSP, including the cybersecurity controls, would be submitted to the NRC for review and approval before implementation of the change. The licensee may change the CSP without prior Commission approval if these changes do not decrease the effectiveness of the plan.

172. RG 5.71, section C.4, offers additional guidance on this topic.

Event Reporting and Tracking

173. Pursuant to 10 CFR 73.110(e)(1), which references 10 CFR 73.54(d)(4), the licensee must make cybersecurity event notifications in accordance with the provisions of 10 CFR 73.77 for a scenario in which a cyberattack adversely impacts the functions performed by digital assets that prevent the consequences listed in 10 CFR 73.110(a). In addition to the NRC staff, the Cybersecurity and Infrastructure Security Agency of the U.S. Department of Homeland Security and other Federal partners such as the Federal Bureau of Investigation would work with the licensee and conduct, for example, forensic analysis. RG 5.83 contains additional guidance on this topic.

Records Retention and Handling

174. In accordance with 10 CFR 73.110(e)(5), the licensee must retain all records and supporting technical documentation required to satisfy the implementation of this regulation until the Commission terminates the license for which the records were developed. Furthermore, the licensee must maintain superseded portions of these records for at least 3 years after the record is superseded, unless otherwise specified by the Commission. RG 5.71, section C.5, contains additional guidance on this topic.

D. IMPLEMENTATION

The NRC staff may use this regulatory guide as a reference in its regulatory processes, such as licensing, inspection, or enforcement. However, the NRC staff does not intend to use the guidance in this regulatory guide to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 53.1590, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests" (Ref. [40]), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 53, Subpart H, "Licenses, Certifications, and Approvals." The staff also does not intend to use the guidance to support NRC staff actions in a manner that constitutes forward fitting as that term is defined and described in Management Directive 8.4. If a licensee believes that the NRC is using this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfitting or forward fitting appeal with the NRC in accordance with the process in Management Directive 8.4.

GLOSSARY[4]

active measures	Computer security measures that require the time-dependent performance of actions by a person, system, or entity to prevent, detect or delay, respond to, and mitigate the consequences of cyberattacks.
adversary functional scenario	Sequences of adversary accesses to attack pathways that advance CEASs and CEISs through the compromise of functions. These scenarios are based on the threat assessments and reflect the potential effects on facility functions of the compromise of systems performing those functions. These scenarios include those involving radiological sabotage or physical intrusion resulting in unacceptable consequences. Adversary functional scenarios can also be used to identify dependencies between critical functions or systems (Ref. 24).
adversary technical sequence	Sequences of adversary tactics, techniques, and procedures that provide a detailed listing of tasks, series progressions, and impacts. Frameworks such as MITRE ATT&CK can be used to develop ATSs that are consistent and reproducible.
attack tree	A graphical conceptual diagram that represents a set of potential approaches in which systems are penetrated or compromised in a specified way to result in the desired consequences (Ref. [41]).
attack pathways	Types of access to critical systems (and digital assets) that allow for the adversary to launch a cyberattack on the accessed system. The types of access are (1) physical access, (2) portable media/device connectivity, (3) wired communications, (4) wireless communications, and (5) supply chain access (adapted from Ref. 40).
attack vector	Means, method, mechanism, or technique (or combination thereof) used, or that might be used, by an adversary to gain unauthorized access to, exploit a vulnerability in, produce a malicious outcome on, or otherwise cause adverse impact to a digital asset, network, or system (Ref. 11).
availability	Ensuring timely and reliable access to and use of information (Ref. 14).
blended attack	A coordinated attack that uses both cyber and physical aspects in an unauthorized act (Ref. 22).
computer security level	The strength of security protection required for a facility function and consequently for the system that performs that function (Ref. 24).
computer security measures	Policies, procedures, and practices specifying permitted, necessary, and forbidden actions to protect critical systems by providing instructions for actions of employees and of vendors, contractors, and suppliers.
computer security zone	A group of systems having common physical and virtual (logical) boundaries and, if necessary, arranged using additional criteria, that is assigned a common security level to simplify the administration, communication, and application of computer security measures (Ref. 24).
confidentiality	Limiting information access and disclosure and system access to only

[4] RG 5.71 defines terms that do not appear in this glossary but may be used in this RG.

	authorized users, as well as preventing access by, or disclosure to, unauthorized parties (Ref. [42]).
critical function	A function that is associated with a CEAS or CEIS.
critical system	A system that performs or supports a critical function. Critical systems may be categorized as "most critical" or "least critical," allowing for a graded approach to the selection and implementation of measures.
cyberattack	A malicious act that targets sensitive information or sensitive information assets with the intent of stealing, altering, preventing access to, or destroying a specified target through unauthorized access (or actions) to a susceptible system (Ref. 24).
cyber-enabled accident scenario (CEAS)	Postulated accidents that are used to set cybersecurity design criteria and performance objectives. CEASs may be derived from safety analysis and include considerations involving (1) effects of compromise on a function(s) and (2) events resulting from cyberattack. CEAS analysis allows for insights into potential mitigations to cyberattacks associated with the potential to result in unacceptable radiological sabotage consequences.
cyber-enabled intrusion scenario (CEIS)	Postulated physical intrusions that are used to set cybersecurity design criteria and performance objectives for physical protection systems. CEISs may be derived from security analysis and include considerations involving (1) effects of compromise on function(s) and (2) events resulting from cyberattack. CEIS analysis allows for insights into potential mitigations of cyberattacks that could result in unacceptable physical intrusion consequences.
cybersecurity operations center (CSOC)	An installation that provides for the complete and continuous cybersecurity monitoring, assessment, and coordination of cybersecurity incident response team(s) and facility personnel (adapted from Ref. [43]). A CSOC may include Security Information and Event Management (SIEM) and security orchestration, automation, and response (SOAR) technology.
digital assets	Technologies that create, provide access to, process, compute, communicate, store, or control services involving digital information. These systems may be physical or virtual. They include but are not limited to desktops, laptops, tablets and other personal computers, smart phones, mainframes, servers, virtual computers, software applications, databases, removable media, digital I&C devices, programmable logic controllers, printers, network devices, and embedded components and devices (Ref. 24).
function	A coordinated set of actions, processes, and operations associated with a nuclear facility. Their purpose may be, but is not limited to, performing functions important or related to nuclear safety, nuclear security, nuclear material accounting and control or sensitive information management (Ref. 24).
integrity	Guarding against improper information modification or destruction. Integrity includes ensuring information nonrepudiation and authenticity (Ref. 14).

noncyber independent protection layer (IPL)	Computer security measures that do not rely on digital systems and prevent the progression of CEASs or CEISs. IPLs include physical security or mechanical safeguards (such as pressure safety valves) that are in place to reduce the likelihood of a successful cyberattack (adapted from Ref. 18).
passive measures	Computer security measures that do not require action or operation to support capabilities or contribute to the prevention, detection, or delay, response to, and mitigation of the consequences of cyberattacks.
preventive measures	Computer security measures that exclude potential adversaries from access to attack pathways. Preventive measures are generally passive measures (e.g., structure and features) that may be supported by active measures (e.g., physical access control systems) (informed by Ref. [44]).
protective measures	Computer security measures that detect and respond to an adversary's malicious activity. Protective measures are generally active measures (e.g., physical intrusion detection system, alarm communication and display) that may be supported by passive measures (e.g., structure and features providing delay) (informed by Ref. 45).
risk-informed, performance-based	An approach to decision-making in which insights from risk assessments are considered with other sources of insights to inform decision-making that focuses on desired objectives and calculable or measurable observable outcomes, rather than prescriptive processes, techniques, or procedures. Performance-based decisions lead to defined results without specific direction as to how those results are to be obtained. At the NRC, performance-based regulatory actions focus on identifying performance measures that ensure an adequate margin and offer incentives and flexibility for licensees to improve cybersecurity without formal regulatory intervention by the agency (adapted from Ref. 9).
risk treatment	Process to modify risk (Ref. [45]). Risk treatment can involve avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk, taking or increasing risk to pursue an opportunity, removing the risk source, changing the likelihood, changing the consequences, sharing the risk with another party or parties (including contracts and risk financing), and retaining the risk by informed choice. Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation," "risk elimination," "risk prevention," and "risk reduction." Risk treatment can create new risks or modify existing risks (Ref. [46]).
security by design (SeBD)	Consideration of safety and security requirements together in the design process such that security issues (e.g., newly identified threats of terrorist attacks) can be effectively resolved through facility design and engineered security features, and formulation of mitigation measures, with no or minimal reliance on human actions (Ref. 33).
security controls	A safeguard or countermeasure prescribed for a critical system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements (Ref. 14). Operational, management, and technical controls that are implemented to protect critical systems from cyberattack.

	Security controls are generally selected based on the ATS analysis. Appendices B and C to RG 5.71, ISO/IEC 27002, and NIST SP800-53 are security control catalogs.
security information and event management (SIEM)	Technology supports threat detection, compliance, and security incident management through the collection and analysis (both near realtime and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards, and reporting) (Ref. [47]).
security orchestration, automation, and response (SOAR)	Refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies—where incident analysis and triage can be performed by leveraging a combination of human and machine power—help define, prioritize, and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format (Ref. 48).
statement of applicability	Record or records that document the selection and implementation of security controls to assist with compliance requirements.
supply chain	Linked set of resources and processes between and among multiple tiers of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle (Ref. 14).
unacceptable consequences	Any consequence scenario in which the cyberattack leads to offsite radiation hazards that would endanger public health and safety or facilitate physical intrusion.

REFERENCES[5]

[5] Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public website at https://www.nrc.gov/reading-rm/doc-collections/index.html and through the NRC's Agencywide Documents Access and Management System (ADAMS) at https://www.nrc.gov/reading-rm/adams.html. The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or e-mail pdr.resource@nrc.gov.

Copies of the non-NRC documents included in these references may be obtained from the publishing organization.

Publications from the Nuclear Energy Institute (NEI) are available at its website: http://www.nei.org/ or by contacting the headquarters at Nuclear Energy Institute, 1776 I Street NW, Washington DC 20006-3708, Phone: 202-739-800, Fax: 202-785-4019.

Copies of NIST computer security documents may be obtained through its website at http://csrc.nist.gov/publications or by writing the National Institute of Standards and Technology, Attn: Computer Security Division, Information Technology Laboratory, 100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930.

Copies of International Atomic Energy Agency (IAEA) documents may be obtained through its website at https://www.iaea.org/ or by writing the International Atomic Energy Agency, P.O. Box 100, Wagramer Strasse 5, A-1400 Vienna, Austria; telephone (+431) 2600-0; fax (+431) 2600-7; or e-mil at official.mail@IAEA.org.

APPENDIX A

CYBERSECURITY PLAN TEMPLATE

Note: In this appendix, any text shown in brackets is generic example text. The licensee or applicant should replace the example text with appropriate and applicable site-specific text. This cybersecurity plan (CSP) template uses Regulatory Guide (RG) 5.96, "Establishing Cybersecurity for Advanced Reactors," to show one acceptable means of meeting regulatory requirements. If the licensee selects other guidance for the basis of its CSP, it should modify references to RG 5.96 to refer to the licensee-selected guidance.

[SITE] CYBERSECURITY PLAN

A.1 INTRODUCTION

The purpose of this [Licensee/Applicant] cybersecurity plan (CSP, the plan) is to describe how the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.110, "Technology inclusive requirements for protection of digital computer and communication systems and networks" (the rule), are to be implemented to protect digital computer and communications systems and networks associated with the following ***critical*** functions from those cyberattacks, up to and including the design-basis threat described in 10 CFR 73.1, "Purpose and scope":

[Licensee critical functions in accordance with cyber-enabled intrusion scenario (CEIS)/cyber-enabled accident scenario (CEAS) analysis.]

As discussed in RG 5.96, [Licensee/Applicant] must establish, implement, and maintain a CSP. This plan establishes the licensing basis for the [Licensee/Applicant] cybersecurity program (the program) for [Site(s)]. Elements of the program described in this plan are applicable to all sites unless otherwise stated. The [Licensee/Applicant] acknowledges that the implementation of this plan does not alleviate [Licensee/Applicant]'s responsibility to comply with other regulations of the U.S. Nuclear Regulatory Commission (NRC).

The [Licensee/Applicant] will comply with the requirements of 10 CFR 73.110 by following the guidance in RG 5.96. RG 5.96 provides a method that the NRC staff considers acceptable for complying with the regulatory requirements in 10 CFR 73.110. RG 5.96 includes a glossary of terms that are used in this plan.

A.2 CYBERSECURITY ANALYSIS

As discussed in RG 5.96, [Licensee/Applicant] developed and documented the following:

- a facility-level analysis consisting of CEASs, CEISs, and resulting design elements and considerations with justification for inclusion or exclusion;
- a function-level analysis consisting of adversary functional scenario analysis (AFSA) for all unmitigated CEASs and CEISs and resulting passive defensive computer security architecture (DCSA) elements and passive CSP controls with justification for inclusion or exclusion;
- a system-level analysis consisting of adversary technical sequences (ATSs) for all unmitigated AFSAs and resulting active DCSA elements and active CSP controls with justification for inclusion or exclusion; and

- a criticality classification (most critical, least critical, noncritical) for each plant system.

A.3 CYBERSECURITY PLAN

A.3.1 Scope and Purpose

This plan describes how [Licensee/Applicant] establishes/established a cybersecurity program to achieve reasonable assurance that site digital assets or computer and communication systems and networks associated with critical functions, defined here as critical systems (CSs), are adequately protected against cyberattacks up to and including the design-basis threat. The following actions provide reasonable assurance of adequate protection from cyberattacks of systems associated with the above functions:

- implementing and documenting the security controls described in appendix B, "Technical Security Controls," and appendix C, "Operational and Management Security Controls," to RG 5.71, "Cyber Security Programs for Nuclear Facilities," and

- implementing and documenting a cybersecurity program to maintain the established cybersecurity controls through a comprehensive life-cycle approach, as described in section C of this document.

A.3.2 Controls Catalog

The implementation of the security controls listed in appendices B and C to RG 5.71 can be graded as follows:

- Noncritical Systems—Security controls are optional but recommended for enhancing the defense-in-depth posture of the DCSA and should prioritize detection measures.

- Least-Critical Systems—Selected security controls should be applied based on a technical justification that factors in the technical feasibility or other design considerations (e.g., safety, operational performance), with the exception of security controls associated with detection and delay measures, which must always be applied.

- Most-Critical Systems—All security controls must be applied as they provide near realtime assurance that cybersecurity is maintained. Protective measures (response, correction, recovery), active and passive DCSA, and prohibitive CSP measures must be applied to minimize risks identified in scenarios.

A.3.3 Statement of Applicability

As discussed in RG 5.96, the licensee must complete a statement of applicability form for each control in appendices B and C to RG 5.71. The purpose of this form is to communicate the impact of the control on the overall risk of a system and justify its inclusion or exclusion in the CSP.

A.3.3.1 *Statement of Applicability Inputs*

As discussed in RG 5.96, the licensee will assess cybersecurity risks using a tiered risk management approach. The results of the analysis are sets of CEASs, CEISs, AFSA, and ATSs. Scenarios produced at each tier should be used to select and justify controls.

A.3.3.2 *Risk Treatment*

For each scenario in a CEAS, CEIS, AFSA, and ATS, the licensee should consider the appropriate risk treatment option. Risk treatment options include risk modification, risk retention, risk avoidance, and risk sharing. The controls in appendices B and C to RG 5.71 generally apply to risk modification. Controls can provide the following types of protection:

- correction
- elimination
- prevention
- impact minimization
- deterrence
- detection
- recovery
- monitoring and awareness

The licensee should determine which risk modification options to consider based on a qualitative assessment of the control's contribution to the scenario's likelihood (i.e., increasing the difficulty of attack) or consequence.

A.3.3.3 *Control Selection and Justification (Inclusion and Exclusion)*

The licensee should select controls for each scenario in the AFSA and ATS that can provide demonstrable risk reduction based on a qualitative assessment of the control's contribution to the scenario's likelihood (i.e., increasing the difficulty of attack) or consequence. The licensee should cite the applicable cyberattack stage in the scenario and discuss (1) the significance of the stage to the overall scenario and (2) the result of applying the control to that stage.

For most-critical systems, [Licensee/Applicant] must document the reason for exclusion of any security control, alternative compensating measures, and the method by which these measures were validated and determined to provide equivalent protection.

For least-critical systems, [Licensee/Applicant] must document the reason for exclusion and alternative compensating measures taken to otherwise reduce the risk of associated scenarios.

Statement of Applicability Form

Table 1 provides an example of the process of selecting and justifying cybersecurity controls for each system based on the scenarios developed in the function-level and system-level analyses. Controls from [Controls Appendix] should be considered for each system, and the decision to select or omit a control should be informed by threats identified in the AFSA and ATS related to the system.

The control information in columns 1 through 3 (labeled "Control Number," "Heading (Family or Name)," and "Control Requirement or Element (from Appendices B and C to RG 5.71)") can be copied from the associated control description in appendices B or C to RG 5.71.

For column 4 (labeled “Security Control Applicable?”), the licensee documents if the AFSA or ATSs associated with the systems have identified a need for the control. If the need is identified, the licensee documents whether the control is selected for the system. The licensee should consider and document the intent of the control in the context of the scenarios applicable to the system and how the control reduces the scenario risk. This should be a qualitative assessment of the control’s contribution to the scenario’s likelihood (i.e., increasing the difficulty of attack) or consequence. In this column, the licensee either describes how the control will be implemented if selected, or justifies the exclusion of a security control that has been identified as a requirement or recommendation for the scenarios but cannot be feasibly implemented in the system.

Column 5 (labeled “Alternative Compensating Control(s) and Justification [Security Control Applicable but not applied]”) is reserved for instances in which a security control has been identified as recommended by the system-specific ATSs or AFSAs, but the licensee has chosen to exclude the control. In this case, the licensee should consider the intent of the control as documented in column 5 and document compensatory measures meeting the objectives of the control:

- For the most-critical systems, the justification should discuss how the alternative compensating measures provide equal or greater risk reduction relative to the control.

- For the least-critical systems, alternative compensating measures should be documented, but further analysis is not required.

- For noncritical systems, security controls are optional, and alternative compensating measures are not required to be documented.

Table 1: Sample Cybersecurity Controls Selection Documentation

System:	Example System	**Control Requirement or Element (from Appendices B and C to RG 5.71)**	**Security Control Applicable?**	**Alternative Compensating Control(s) and Justification [Security Control Applicable but Not Applied]**
System Criticality:	Example (Most or Least Critical)			
Scenario(s) (if any):	Example (AFSA or ATS #)			
Control Number	**Heading (Family or Name)**			
B.1	**Access Controls**			
B.1.1	Access Controls Policy and Procedure	[Licensee/Applicant] develops, disseminates, and [annually] reviews and updates a formal, documented, CS access control policy …	Description of how control will be implemented if selected, or a justification for excluding a security control.	
		access control rights (i.e., which individuals and processes can access what resources) and access control privileges (i.e., what these individuals and processes can do with the resources accessed)		
		management of CSs...		
		auditing of CSs [annually] or immediately upon changes...		

System:	Example System	**Control Requirement or Element (from Appendices B and C to RG 5.71)**	**Security Control Applicable?**	**Alternative Compensating Control(s) and Justification [Security Control Applicable but Not Applied]**
System Criticality:	Example (Most or Least Critical)			
Scenario(s) (if any):	Example (AFSA or ATS #)			
Control Number	**Heading (Family or Name)**			
		separation of duties…		
B.1.2	Account Management			
		managing and documenting CS accounts…		
		reviewing CS accounts in a manner consistent with the access control list provided…		

APPENDIX B

CYBER-ENABLED ACCIDENT SCENARIO
Analysis and Example of an Adversary Functional Scenario

B.1 INTRODUCTION

The cyber-enabled accident scenario (CEAS) example analyzes the effect of compromise for a major control loop of a high-temperature gas-cooled reactor (HTGR) arising from a cyberattack. The potential consequences of the postulated attack include unanticipated changes in reactivity, fuel temperature, and coolant temperature that may challenge safety margins for key components, result in unanalyzed operational conditions, or exacerbate any concurrent accident conditions.

The same HTGR design is used in the adversary functional scenario example. Figure B-1 shows an example implementation for the conceptual design of the plant. The event sequence that the adversary seeks to exploit is a helium depressurization event initiated by a small helium pressure boundary (HPB) break.

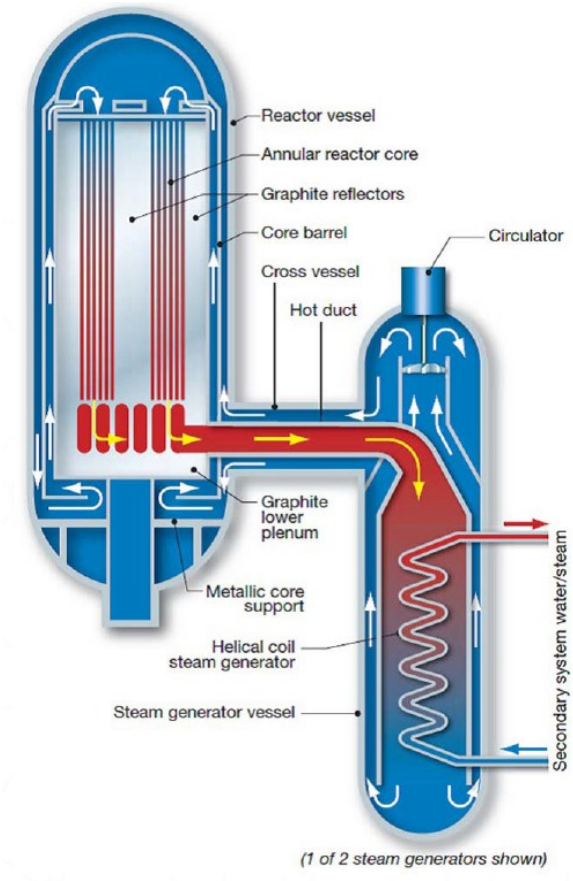


Figure B-1. HTGR Reactor Concept (from Ref. B-[48])

The event tree in figure B-2 models plant capability defense in depth. Each path in the tree is a potential attack sequence leading to a consequence.

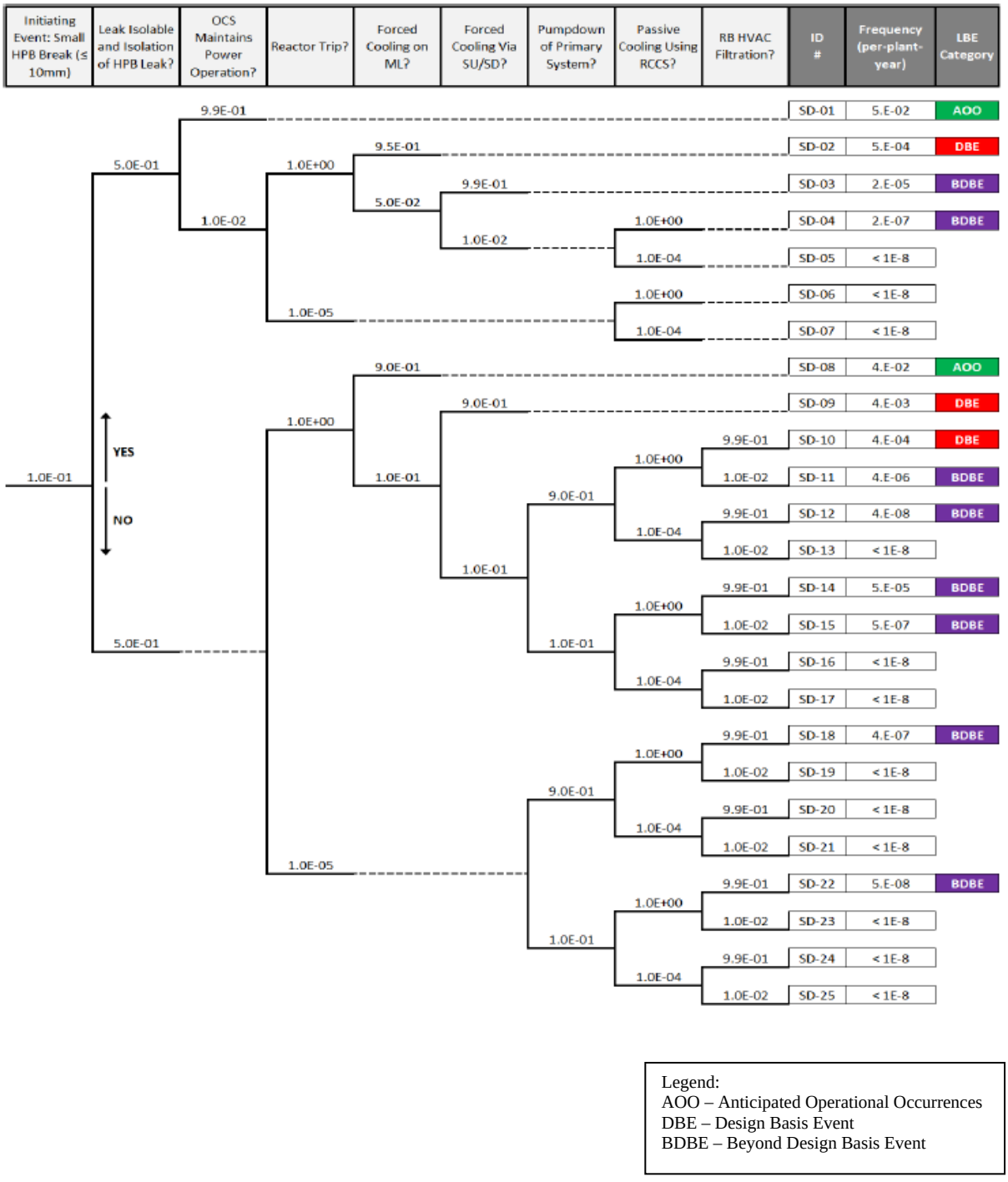


Figure B-2. Helium Depressurization Event Tree (from Ref. B-[49])

HTGR designs are generally helium-cooled, graphite-moderated reactors involving either prismatic or pebble bed core configurations of the fuel and moderator. The target for this example analysis is a representative plant concept derived from the historical modular HTGR design developed with funding

from the U.S. Department of Energy (Ref. B-[50]). For this example, the HTGR involves a Rankine cycle energy conversion system coupled to the primary heat transport system through steam generators. Key information on functions, systems, operational behavior, and safety characteristics for historical and conceptual HTGR plants are documented in gas-cooled reactor instrumentation and control technology summaries generated by Oak Ridge National Laboratory (Ref. B-[51] and Ref. B-[52]) and phenomena identification and ranking tables for the next generation nuclear plant (Ref. B-[53] and Ref. B-[54]).

This CEAS focuses on functions within the plant control system that manage the performance of its heat transfer processes. Figure B-3 presents a simplified view of the gas-cooled reactor functions. Under nominal conditions, the operational control system (OCS) regulates the processes to the specified setpoints of the design. The automated controls adjust for load perturbations, as well as gradual changes in the plant such as fuel burnup, steam generator fouling, or changes in the temperature of the ultimate heat sink. Feedback control is used to regulate temperatures, flows, and pressures within the heat transport system to their setpoints, compensating for all these variations. Feedforward control is used to coordinate feedback control objectives and anticipate coupled response arising from changing grid demands.

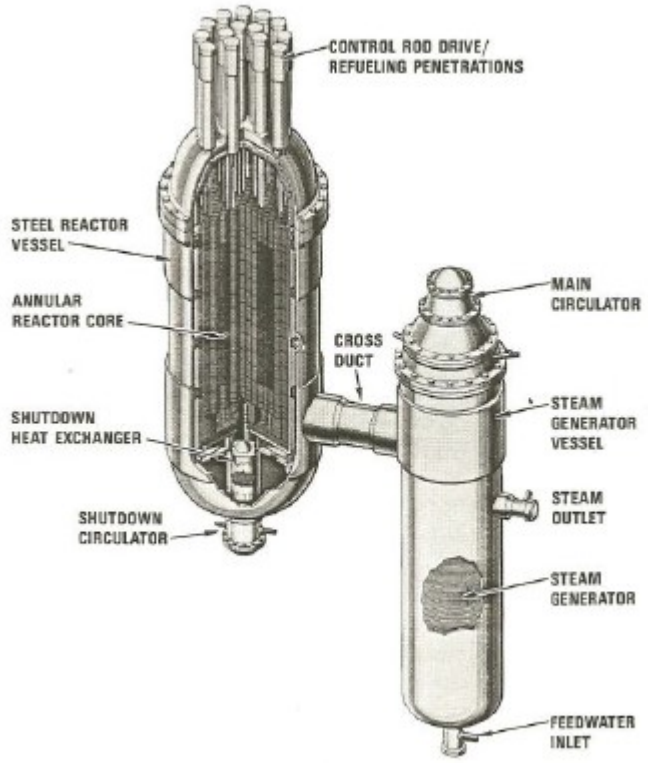


Figure B-3. Gas-Cooled Reactor Functions (from Ref. B-3)

B.1.2 Design Assumptions

Key assumptions of the design necessary for the analysis of the coolant flow control loop include the following:

- All systems and components are digital.
- All measurements and sensors are digital or convert analog to digital.

- The control loop is a proportional-integral-derivative (PID) controller with both feedback and feedforward action.
- The heat transport medium is helium.
- The main control action is to manage the coolant flow rate to ensure removal of core heat by convection and subsequent transport to energy conversion systems (e.g., heat exchanger, steam generator, or gas turbine).
- The OCS and forced cooling system require bidirectional communication.
- The plant state is assumed to be operational.

Figure B-4 shows the simplified coolant flow control loop function.

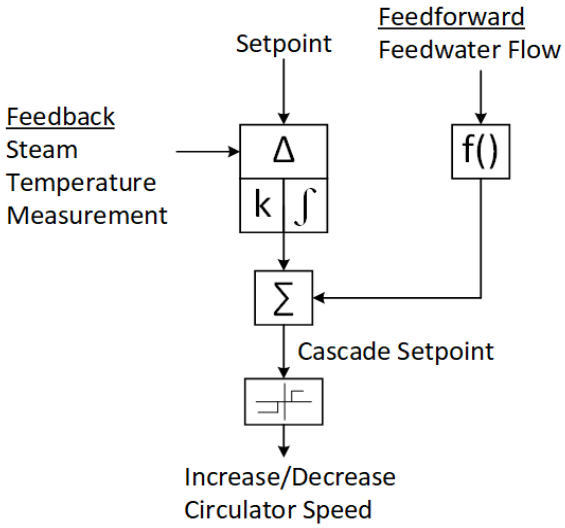


Figure B-4. HTGR Coolant Flow Control Loop (from Refs. B-4 and B-5)

B.1.3 Analysis of Cyber-Enabled Accident Scenario

Initial Assumption: Simplified coolant flow control has no other systems to prevent or protect against a malicious cyberattack resulting in coolant flow change and consequential reactivity and temperature changes.

This analysis determines the design basis and features necessary to prevent or limit the condition(s) that could be initiated by a cyberattack resulting in radiological sabotage (i.e., the consequence specified in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.110(a)(1)).

> *As discussed in sections C.17 through C.18 above, 10 CFR 73.110(a)(1) deals with the radiological sabotage scenario in which a potential cyberattack adversely impacts the functions performed by the digital assets used by the licensee to avoid exceeding the offsite dose values established in 10 CFR 53.210. The risk assessment should identify functions that could contribute to or mitigate the radiological sabotage consequence identified in 10 CFR 73.110(a)(1)*. [section C.43]

Radiological sabotage may involve compromise(s) of function(s) resulting in events such as the following:

a. *loss of reactivity control leading to an unacceptable reactor power increase,*

b. *overpressure event leading to a pressure boundary failure,*

c. *loss-of-coolant event (from a pressure boundary breach) leading to reactor core damage,*

d. *equipment malfunction or failure leading to fire,*

e. *a physical breach resulting from a kinetic event in which control of rotational equipment (e.g., turbine) is altered because of a cyberattack, and*

f. *equipment malfunction or failure resulting from an electrical power system event.* [section C.44]

The condition and assumptions being considered for this analysis are as follows:

Condition (section C.44(a)): Loss of reactivity control leading to an unacceptable reactor power increase.

Assumptions:

- Digital devices and systems perform all measurements and control actions.
- Simplified coolant flow control loop uses a PID controller with both feedback and feedforward action.
- Core power is affected by variation (i.e., increasing, decreasing, loss) of forced coolant flow through reactivity feedback due to temperature changes in the fuel or coolant or both.

For reactor designs that include passive safety features, the licensee provides an analysis of how events such as those listed in section 44 are accounted for when considering the effects of compromise on function(s). The events resulting from function(s) compromised by potential cyberattacks produce CEASs. [section C.45]

The analysis includes postulating the compromise(s) of a measurement/control action as follows:

Compromise #1 (measured input(s) for coolant flow control loop set to arbitrary value): For example, the controller feedback variable “steam temperature” can be set to an incorrect low value. This results in controller action to drive the feedback variable to match the setpoint. In this example, with a compromised measurement, erroneous action by the controller can persist to further increase reactor power and temperatures.

Unsafe Action Resulting from Compromise #1: In the stated example, the coolant flow control loop controller will command an increased circulator speed to transfer more thermal energy from the core through increased coolant flow. The transfer of this additional energy will thereby increase steam temperature in an attempt to match the current setpoint. Concurrently, the fuel temperature will decrease because of increased heat removal, and core reactivity will increase in response to thermal feedback

effects. The undesired consequence is that reactor power increases in the absence of actual demand. Figure B-5 illustrates the progression of phenomenological reactions to the primary action induced by the compromise. This cyber-enabled action can lead to higher nuclear power and temperature rises that could challenge material temperature limits or stress component integrity (e.g., through thermal cycling of steam generator tubes). In the absence of other control or protection functions that manage or limit core power and temperatures, the undesired effects are primarily constrained by the strength of reactivity feedback effects and speed at which thermal energy transfer can be accelerated.

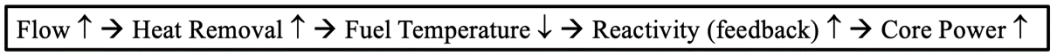


Figure B-5. Progression of Phenomenological Response to Compromise

Design Basis #1: Identify constraints on thermal-hydraulic and neutronic behavior driving the temperature and power response to flow changes. Determine the range and rate of power changes that can result from reactivity feedback effects and assess the magnitude of thermal effects arising from those power changes. Determine whether such effects are bounded by the safety analysis or represent unanalyzed events. Consider the impact of power/temperature cycling, as well as extremes of those variables.

Design Constraint #1 (to address compromise of coolant flow control loop measurement): If the rate of change for power or temperatures resulting from coolant flow changes challenges the safety basis for the reactor, then constrain the rate at which circulator speed can vary. Constraining coolant flow rate changes can limit the rate of reactivity increase that can be achieved by a cyberattack. While this constraint does not eliminate the cyberattack or need for an adversary functional scenario analysis (AFSA) in accordance with sections C.88 through C.103, it would slow down the reactivity increase to allow sufficient time for an operator to intervene (or another function to act).

Design Requirement #1: Include a design requirement to have additional systems implementing functions to prevent unacceptable power increases. Examples of functions that could be effective include protection functions such as reactor trip or runback or control functions such as reactivity or power control. The independence of these functions can also be considered. An AFSA will be needed to assess the effectiveness of such design requirements (see sections C.88 through C.103).

> *To aid in the risk assessment, the licensee should develop adversary functional scenarios to validate assumptions made during the reactor design and implementation. These scenarios should assess whether a radiological sabotage scenario involving compromise(s) of function(s) that results in events such as those listed in section 44 could lead to the consequence identified in* 10 *CFR 73.110(a)(1). A licensee may use existing documentation and analyses (e.g., integrated safety analysis, process hazards analysis, security plans) in support of the risk assessment to (1) determine those events that could lead to the consequence identified in 10 CFR 73.110(a)(1), and (2) subsequently identify the function(s) that may be adversely affected by a potential cyberattack thus leading to the consequence identified in 10 CFR 73.110(a)(1).* [section C.46]

The licensee will need to perform an AFSA in accordance with sections C.88 through C.103 to inform features of the defensive cybersecurity architecture (DCSA) and cybersecurity plan (CSP) elements needed to mitigate the cybersecurity risks associated with the pathways mentioned above. For example, an event tree may be used to simplify the functional analysis with the condition that tier 1 analysis outputs

demands that other systems/functions are considered. Any commonalities among functions (e.g., common input measurements) need to be identified and addressed.

> *The licensee considers events such as the above and evaluates whether cyberattacks can escalate the impacts (i.e., increase the severity) of these events in the accident scenarios (i.e., CEASs) already considered and whether they may create new pathways that result in consequences.* [section C.47]

Power and thermal excursions resulting from a potential cyberattack to the coolant flow control loop are possible through the pathways mentioned above and could contribute significantly to reactivity events causing radiological accidents. However, the licensee needs to perform accident scenario analysis involving the interactions among thermal-hydraulics, reactor physics, and feedback reactivity in preventing unsafe conditions (see Design Basis #1).

> *Those functions that could require or depend on digital technology and have the potential to result in the consequence identified in 10 CFR 73.110(a)(1) if compromised should be identified, including their contribution to the risk, given the applicable adversary functional scenario(s).* [section C.48]

Assuming the coolant flow control loop cannot fully prevent unacceptable reactivity increases, then an AFSA in accordance with sections C.88 through C.103 should be performed.

> *Systems and components that perform or support the functions identified as being associated with CEASs would be considered significant contributors to risk resulting from a cyberattack. Therefore, such systems and components should be protected from a cyberattack using a graded approach as based on the analyses detailed in sections C.65 through C.105 of this RG to ensure their protection not only during operation, but also during their development, simulation, and maintenance environments.* [section C.49]

The CEAS, AFSA, and system-level analyses assume that digital assets and systems support the following control loop functionality:

- coolant flow control loop measurements,
- coolant flow control loop communications, and
- coolant flow control loop computations and commands.

Therefore, digital assets and systems supporting the above functionality need to be identified as they are associated with a CEAS.

Despite the future implementation by the licensee of Design Constraint #1 and Design Requirement #1, this analysis assumes that the coolant flow control loop does not fully prevent unacceptable reactivity increases during a potential cyberattack.

> *Supporting systems, components, and personnel may either reduce or add to the risk from a compromise of the functions associated with a CEAS. For example, interconnected systems may detect precursors or evidence of malicious activity, thus reducing risk; conversely, interconnection of systems may provide for new attack pathways to compromise the function.* [section C.50]

Any supporting systems, components, and personnel will need to be determined before the development of the adversary functional scenario(s) in accordance with sections C.88 through C.103.

> *Independent and diverse systems providing redundant or backup functionality can reduce the contribution of the systems associated with the CEAS to the risk of radiological sabotage.* [section C.51]

Independent and diverse systems that provide the mechanism for attaining a safe and guaranteed shutdown state will need to be analyzed as part of the CEAS analysis and possibly considered within the adversary functional scenario(s) in accordance with sections C.88 through C.103.

> *Independent continuous monitoring of cybersecurity can reduce the potential that compromise from cyberattack will not be detected, further reducing the contribution of the systems associated with the CEAS.* [section C.52]

The use of independent continuous monitoring of cybersecurity for implementing information security assurance activities and systems to confirm that design constraints, design features, and requirements are implemented and effective will need to be analyzed as part of the CEAS analysis and possibly considered within the adversary functional scenario(s) in accordance with sections C.88 through C.103.

B.2 CEAS ADVERSARY FUNCTIONAL SCENARIO

This example of an adversary functional scenario analyzes the attack pathways necessary for an adversary to exploit an unsafe event sequence.

> *If any CEIS or CEAS results in the consequences listed in 10 CFR 73.110(a), then the licensee should perform an AFSA to further assess the potential consequences from such scenarios. This analysis excludes all CEISs and CEASs completely protected by SeBD elements (e.g., noncyber IPLs, analog systems, passive system/barriers).* [section C.88]

The CEAS analysis in section B.1.3 identifies the features necessary to prevent or limit the condition(s) that could be initiated by a cyberattack resulting in radiological sabotage (i.e., the consequence specified in 10 CFR 73.110(a)(1)). The analysis postulated a compromise of the coolant feedback control loop, which would result in an increased circulator speed. Since the proposed design constraints in the CEAS analysis are in place to slow down, but not prevent the adversary, passive design features in this example will focus on mitigative measures for access to the forced cooling system.

In a comprehensive AFSA, multiple attack sequences would be analyzed in depth. In this example, an attack path is considered to be a sequence of plant functions whose collective failure leads to an accident condition. The adversary's attack progression is modeled by all paths leading to consequences in the event tree. This example analysis will follow the path highlighted in red (figure B-6) leading to design-basis event SD-02.

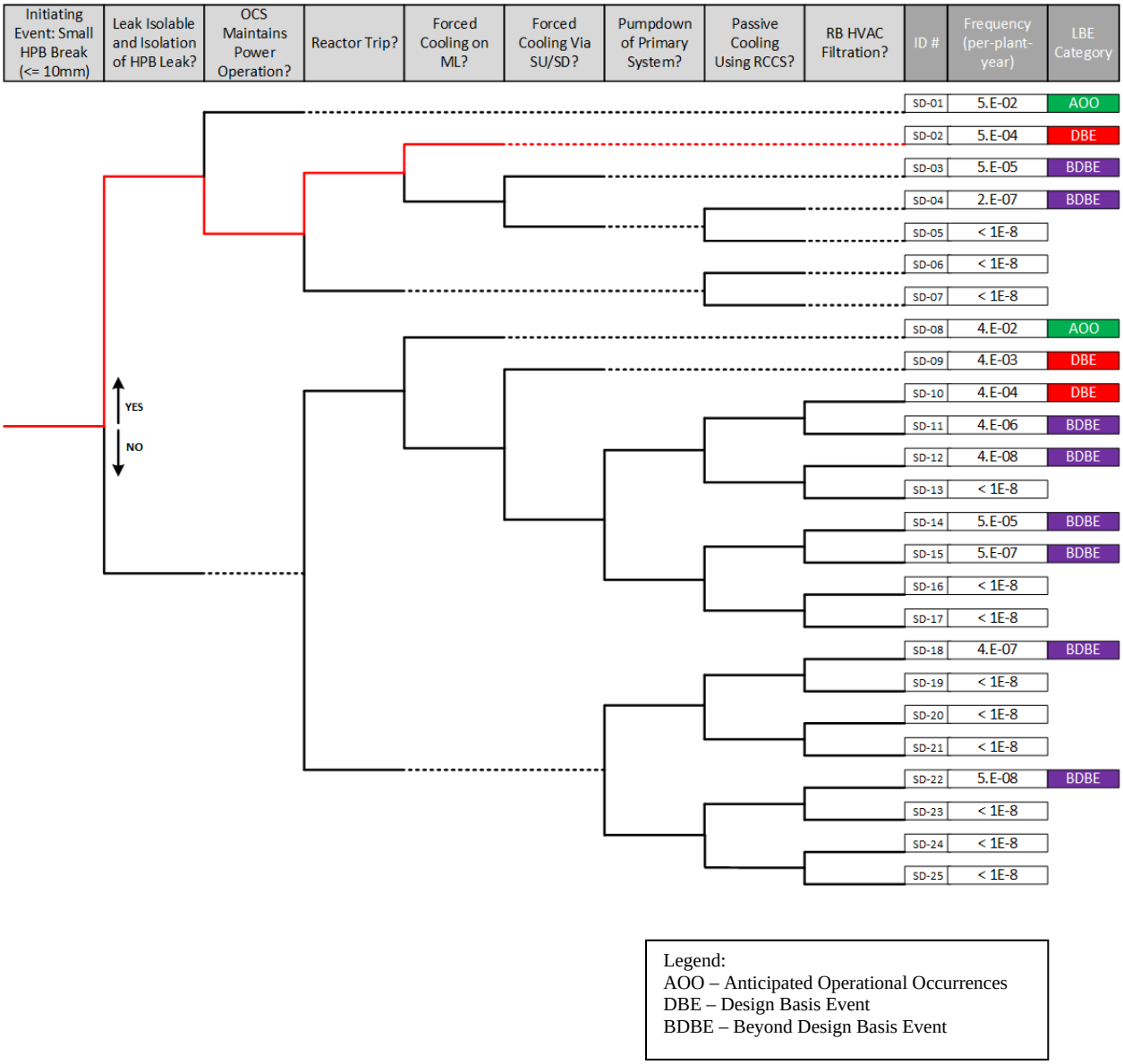


Figure B-6. Attack Path to Be Analyzed (from Ref. B-2]

Event Description: Following the initiating event (IE), the leak is detected and isolated, providing a bypass for the helium gas. The OCS loses power, disabling operator control over valves in the system. The reactor trip system releases control rods in the reactor vessel. Auxiliary pumps and valves initiate forced cooling on the main line (ML).

Assumption: The adversary does not cause the IE. This is assumed to be a random event, and adversary actions occur after the small break event.

Assumption: This analysis assumes an operational plant state.

The AFSA aims to provide plant capability defense in depth by specifying prohibitive CSP elements (e.g., forbid use of wireless communications) and passive, deterministic

DCSA elements to mitigate or control adversary access to attack pathways or eliminate these pathways. Figure 6 describes the AFSA. [section C.89]

No assumptions are made at this point regarding the security or DCSA posture of the systems, components, and networks of the forced cooling system. Initially, all components are assumed to be physically accessible and communication between components required for operation is assumed to be unsecure (e.g., unencrypted, bidirectional). The CSP should document requirements identified in the AFSA.

The essential element of the AFSA is the assumption that the adversary is able to compromise functions in any manner that allows for progression of attack scenarios (i.e., attack success) immediately upon adversary access. [section C.92]

This analysis considers only logical or physical access to system nodes or networks. If access cannot be prevented by passive controls or DCSA elements, the system is further analyzed in the following tier.

For each CEIS and CEAS, the following attack pathways should be considered:

a. physical access,
b. wired communications,
c. wireless communications, and
d. portable media/device connectivity.

For each function, analyze the availability of each attack path. [section C.93]

Leak Isolable and Isolation of Helium Pressure Boundary Break

Design Assumption: This function requires (1) detection of a helium leak along the pressure boundary, and (2) the ability to isolate a small leak and provide a bypass for the gas.

Design Assumption: The HPB exists along the reactor vessel, the steam generator, and the connecting lines. Secondary containment allows the leak detection system to monitor pressure changes with pressure sensors in compartments outside of the HPB. If a leak is identified in a compartment, the system will close the isolation valve upstream of the break and open a bypass valve to allow gas flow while circumventing the break location.

Physical Access: Mitigated—During normal operations, the components that support leak detection and isolation should be in an inaccessible area as they all exist along the HPB. This plant design feature mitigates the threat.

Wired Communication: Mitigated—Data diode prevents access to the network remotely as a DCSA Level 3 or Level 4 (see figure B-7) safety system requirement.

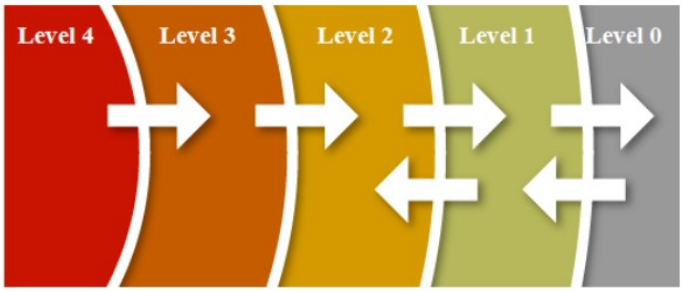


Figure B-7. Cybersecurity Defensive Architecture (from Ref. B-[55])

Wireless Communication: Eliminated—Plant design and CSP requirements prohibit wireless communication.

Portable Interface: Mitigated—The components are inaccessible during operation. Control measures can be put in place to prohibit access during maintenance operations.

Operational Control System Maintains Power Operations

Design Assumption: The OCS requires that sensors be distributed throughout the secondary containment compartments to detect leaks. Valves will need to be manually operated and maintained.

Design Assumption: The operator requires bidirectional communication in the OCS.

Physical Access: Available—Access to the OCS controller is available at the operator control center.

Wired Communication: Mitigated—Systems requiring operator interaction cannot use a data diode. Control and continuous monitoring will be needed.

Wireless Communication: Eliminated—Plant design and CSP requirements prohibit wireless communication.

Portable Interface: Mitigated—Control measures (e.g., blocking ports from physically being accessed by portable media devices) can be implemented but should be continuously monitored for tampering.

Reactor Trip

Design Assumption: The reactor trip system is a digital controller that releases the control rods. The controller is assumed to be kept in a locked compartment in the plant.

Physical Access: Mitigated—The reactor trip system controller is maintained in a locked compartment in the plant. The delay of physical access for the adversary is sufficient to give the plant enough time between the IE and reactor trip. The components of the trip system that release the control rods are inaccessible during plant operation.

Wired Communication: Mitigated—Data diode prevents access to the network remotely as a DCSA Level 3/4 requirement.

Wireless Communication: Eliminated—Plant design and CSP requirements prohibit wireless communication.

Portable Interface: Mitigated—See **Physical Access**.

Forced Cooling through the Main Line

Design Assumption: ML cooling is an auxiliary safety system with components in an auxiliary building.

Design Assumption: ML cooling requires bidirectional communication.

Physical Access: Mitigated—Access to the auxiliary building requires physical security controls.

Wired Communication: Mitigated—Systems requiring operator interaction cannot use a data diode. Control and continuous monitoring will be needed.

Wireless Communication: Eliminated—Plant design and CSP requirements prohibit wireless communication.

Portable Interface: Mitigated—Control measures (e.g., blocking ports from physically being accessed by portable media devices) can be implemented but should be continuously monitored for tampering.

The supply chain attack pathway is addressed separately in sections C.145 through C.151, which provide guidance for mitigating the risk associated with such a pathway that may allow an adversary to compromise the system function(s) in a way that advances the CEAS or CEIS. [section C.94]

Supply chain is not considered in this example.

If the adversary can potentially advance a CEAS or CEIS to completion, the CSP or DCSA may need to include additional mitigation. A necessary attribute of these additional mitigation measures is that they do not require action by licensee personnel or action by a digital system to deny the adversary access to the attack pathway. The following are mitigating measures that can be considered for inclusion:

a. prohibitive CSP elements, such as prohibition of wireless for critical systems, remote access, or other capabilities that allow for adversary to access the attack pathway;

b. location of critical systems within inaccessible or protected locations that will always deny adversary access; and

c. passive and deterministic technical measures needed as part of the DCSA implementation, such as a data diode, or unidirectional taps. [section C.95]

Based on the analysis, the DCSA and CSP implementation should address the following:

a. Eliminate attack vectors. For example, the DCSA implements a deterministic unidirectional communications pathway to eliminate access to wired networks from remote or adjacent networks. Another example is a CSP implementation that forbids wireless communications within critical systems.

b. Mitigate attack vectors using the following means:

(1) Minimize attack vectors. For example, the DCSA implementation places critical systems within the most secure boundaries with supporting CSP implementation of licensee-identified procedures that strictly control physical access to these systems.

(2) Control access to attack vectors. For example, CSP implementation of licensee-identified technical and administrative controls supplements the physical control measures of critical systems.

(3) Detect unauthorized access to attack vectors. This capability will rely on items b(1) and b(2) to increase the likelihood of detecting such access. For example, the CSP implements licensee-identified technical and administrative controls to detect unauthorized access to critical systems. [section C.96]

Figure B-8Error: Reference source not found shows the analysis results. Leak isolation, OCS, and forced cooling all contain at least one attack path that requires controls or is left available to the attacker. The reactor trip function has either mitigated or eliminated all attack paths, and the analysis can take credit for this function being removed from the adversary's attack sequence.

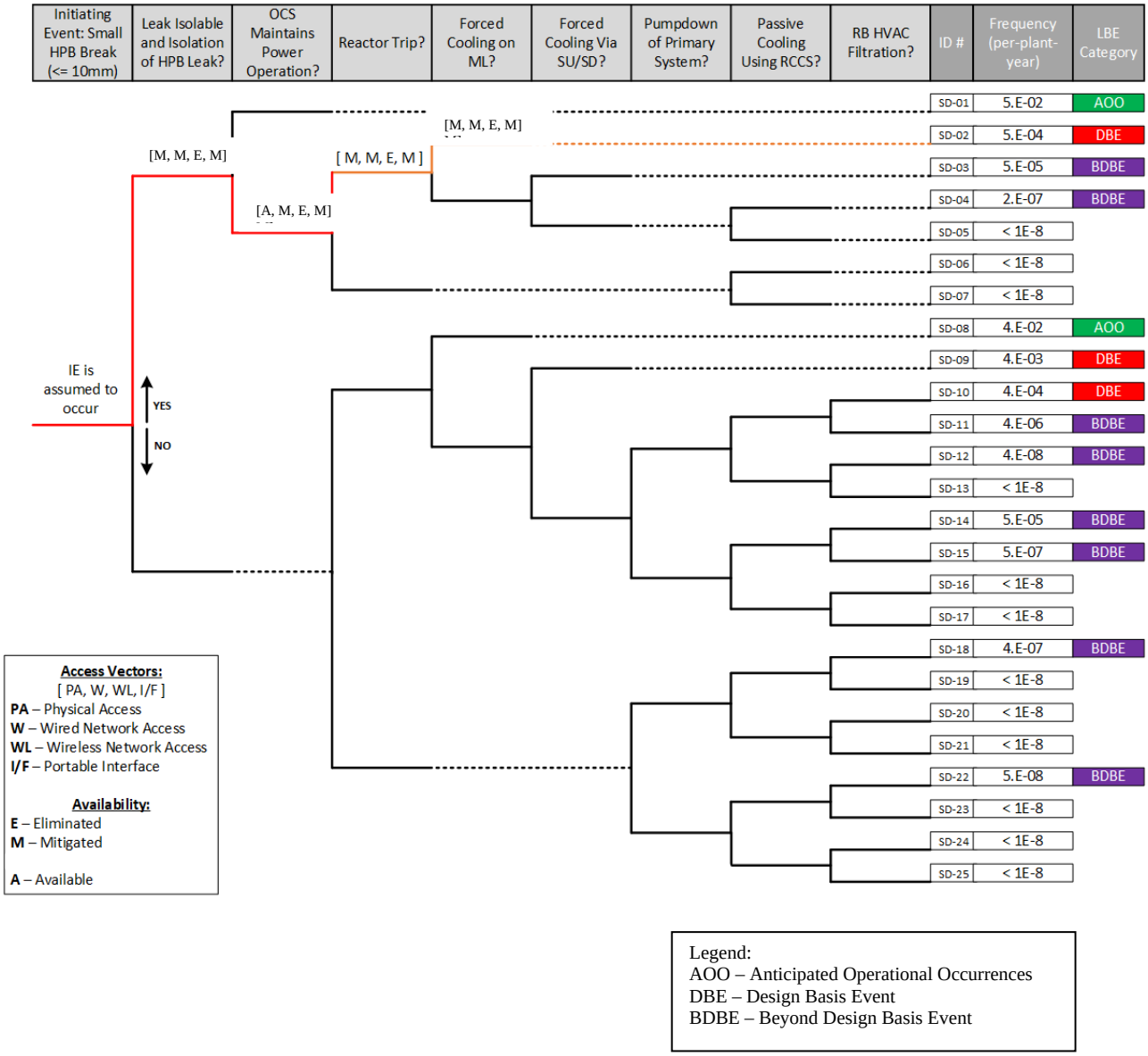


Figure B-8. Analysis for Path Leading to SD-02 (from Ref. B-2)

It may be necessary to bound certain analysis to be valid for specific plant states (e.g., operation, outage, construction) to simplify the analysis. If this is necessary, the licensee should consider all states for which the CSP will be in effect and cover all adversary functional scenarios that could occur during the specific plant states. [section C.97]

The licensee may specify multiple DCSAs based on different considerations such as the following:

a. type of system(s) (e.g., physical protection, safety, EP, BOP),

b. plant lifetime stage (e.g., design, construction, commissioning, operation, decommissioning), and

c. other considerations (e.g., security/trust model, organization). [section C.98]

The licensee should perform the following:

a. Document the AFSA associated with each analyzed CEIS or CEAS.

b. Identify the mitigation measures (e.g., prohibitive CSP elements, locations, DCSA elements) and PPS elements that provide the capability to mitigate or eliminate adversary access to attack pathways. (Special attention by the licensee will be required to manage potential cybersecurity supply chain risks for these mitigations and quality assurance based on their contribution to preventing cyberattacks). [section C.99]

If the AFSA demonstrates that adversary access to the attack vectors necessary to complete a CEIS or CEAS scenario is prevented, then the licensee should do the following:

a. Implement the baseline cybersecurity program, baseline DCSA, and cybersecurity supply chain risk management in accordance with sections C.145 through C.151 to protect those functions identified in the analysis.

b. Implement additional protective measures and mitigations as identified in section C.99 above.

c. Incorporate measures for periodic review and validation of the AFSA within the licensee's management system. [section C.100]

Each CEAS or CEIS where attack vectors are still available for each stage in the scenario progression should result in further system-level analysis in accordance with sections C.104 through C.105 below. These analyses include the following:

a. system analysis to identify critical functions confirming the CEAS and CEIS analysis at the system level (figure 7),

b. categorization of systems allowing for the application of a graded approach (figure 8), and

c. ATS analysis for each adversary functional scenario that could result in the CEIS or CEAS (figure 9). [section C.101]

As shown in Figure B-8, the forced cooling system has three controlled access pathways that require tier 3 analysis. However, such an analysis is beyond the scope of this appendix; but could be included as part of this RG development if deemed useful by its future users.

APPENDIX B REFERENCES

APPENDIX C

CYBER-ENABLED INTRUSION SCENARIO
Analysis and Adversary Functional Scenario Example

C.1 INTRODUCTION

This example of a cyber-enabled intrusion scenario (CEIS) analyzes the effect of compromise of the physical protection system (PPS) for a high-temperature gas-cooled reactor (HTGR) arising from a cyberattack. The outputs from the analysis include a set of functions that require protection, insights for potential updates to the design basis or PPS design, and security engineering insights for the cybersecurity plan (CSP) and defensive cybersecurity architecture (DCSA). The analysis also informs implementation of the CSP, cybersecurity supply chain, and periodic review, and any other licensee-identified actions.

> *The CEIS analysis would aim to eliminate physical intrusion scenarios enabled by potential cyberattacks that would adversely impact the functions performed by digital assets used by the licensee for implementing the physical security requirements that would be established in 10 CFR 53.860(a).* [section C.80]
>
> *CEISs may be used to validate assumptions made during the PPS design and implementation. The assumptions made in developing a set of CEISs should include at a minimum the following:*
>
> *a.* *loss of detection performed by digital technology with no indication of failure;*
>
> *b.* *failure of one or more of the detection, delay, response, or recovery capabilities; and*
>
> c. *unexpected behaviors or actions of digital equipment concurrent with the start of a physical intrusion.*[section C.39]

C.1.2 Design Assumptions

The following are key assumptions of the design necessary for the PPS analysis:

- site location is approximately 4 square kilometers (km^2) (2 x 2 km)
- 19.9% High-Assay Low-Enriched Uranium (HALEU) fuel
- 10 kilograms (kg) or more uranium-235 (both unirradiated and irradiated fuel) (Ref. C-[56])
- all systems and components are digital
- combinations of unirradiated and irradiated fuel exists at the site

C.1.3 Analysis of Cyber-Enabled Intrusion Scenario

In this physical intrusion scenario, as described in section C.34, “a potential cyberattack adversely impacts the functions performed by digital assets used by the licensee for implementing the physical security requirements 10 CFR 53.860(a).”

> *PPSs are used for the protection of special nuclear material, source material, and byproduct material. A licensee would be permitted to rely on the use of digital assets for*

implementing the PPS functions that would be required to meet the 10 CFR 53.860(a) requirements. Therefore, this consequence deals with a scenario in which, for example, a cyberattack adversely impacts the digital assets and associated security functions used by the licensee to meet the 10 CFR 53.860(a) requirements. Security digital assets include those used for nuclear material control and accounting. Such a consequence would not be applicable to commercial nuclear plant designs that do not rely on the use of digital assets for implementing the security functions required for meeting the 10 CFR 53.860(a) requirements. [section C.34]

Security digital assets to be assessed as part of consequence 10 CFR 73.110(a)(2) include those used for nuclear material control and accounting. Such a consequence would not be applicable to commercial nuclear plant designs that do not rely on the use of digital assets for implementing the security functions required for meeting the 10 CFR 53.860(a) requirements. [section C.35]

For each CEIS that has the potential to result in a 10 CFR 73.110(a)(2) consequence, one of the following may be chosen:

a. *Update the design basis or the PPS to prevent CEISs resulting in a 10 CFR 73.110(a)(2) consequence.*

b. *Accept the risk as unavoidable and apply additional cybersecurity measures to protect against the CEIS, as discussed in sections C.88 through C.103 and follow-on sections.*[section C.84]

Initial design-basis assumptions include a 4 km^2 area with three internal areas: owner-controlled area (most external; 0.7 km long); protected area (0.5 km long); and access-controlled area (0.1 km long). Figure C-1 depicts this information.

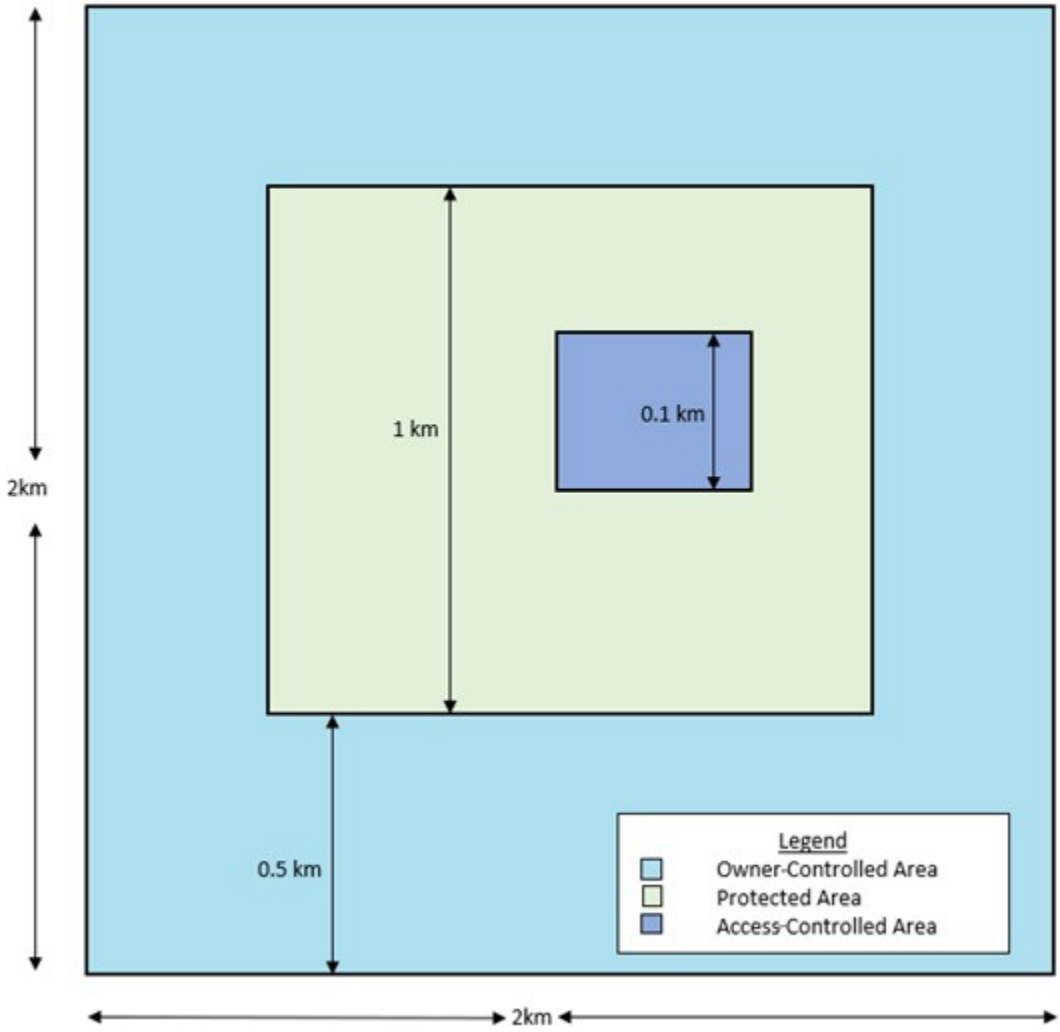


Figure C-1. Depiction of Facility Design Assumptions (Not to Scale)

This analysis determines the design basis and features necessary to prevent or limit the condition(s) that may be initiated by a cyberattack that supports a subsequent physical intrusion leading to theft of nuclear material. The functions considered in this analysis are "detection," "delay," and "response." This is not a complete analysis of these functions. The following are specifically covered:

- detection at the area boundaries,
- delay of removal of material from inner area, and
- response of offsite forces after detection.

Note that this analysis does not consider access control, and no credit is taken for access control measures.

The passive features that support the analysis are listed in the initial assumptions and include three areas:

(1) owner-controlled area—single fence with gates allowing pedestrian and vehicular traffic; normal and emergency gate access for vehicles and personnel

(2) protected area—two fences creating a “clear zone”; normal and emergency gate access for vehicles and personnel

(3) access-controlled area—sheet metal structure with an interior fenced area

Compromise of Detection Function: Compromise of the detection function would allow adversaries to breach boundaries without triggering detection by human operators.

Design Basis #1: Central alarm station (CAS) staff/security staff is on site to allow for detection of explosive breaches into inner areas. Human operator detection of explosive breaches to inner areas is required, as remote offsite personnel would depend entirely on digital means for detection.

PPS Requirement #1: Specific detection elements in the clear zone and inner areas shall be analog. Diversity (noncyber detection) in sensors increases the challenges for potential adversaries attempting to avoid or bypass digital and noncyber sensors. Some of these sensors may include sensors across roads to detect vehicle traffic, especially at the emergency gates.

Impacts to Delay Function: Without detection, no delay can be credited. Additionally, delay features are related to the boundaries of the areas and the entry control points. Credit for delay at the entry control points is not within the scope of this analysis, but delay may be credited to fuel size, shape, and quantity.

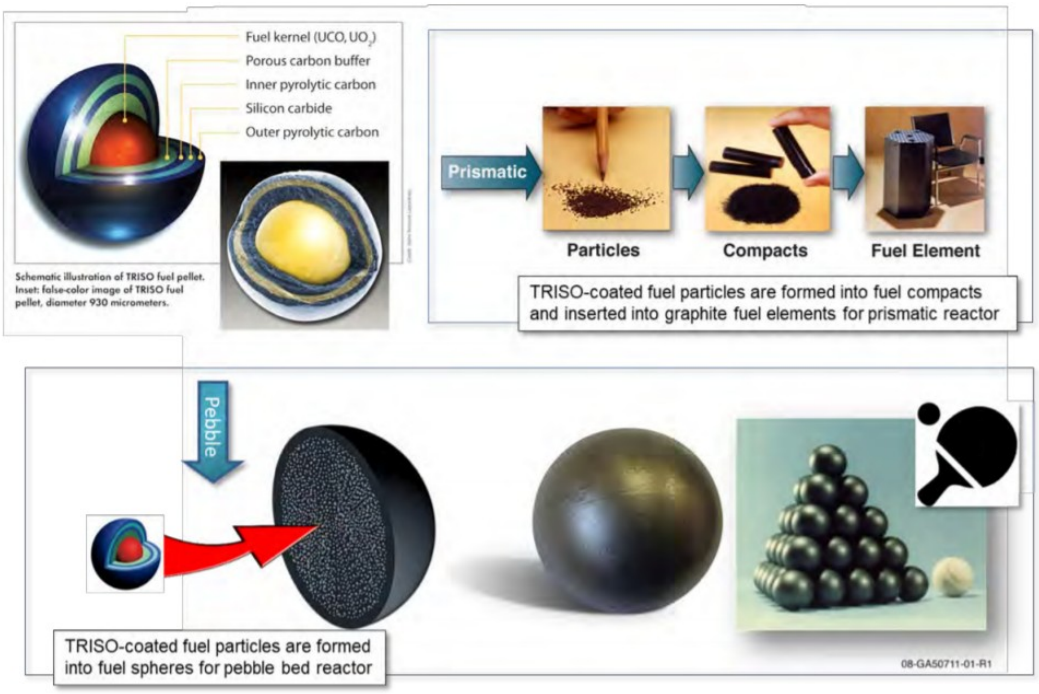


Figure C-2. Depiction of TRISO Fuel Pebbles (from Ref. C-[57])

Design Basis #2: TRISO fuel pebbles are 60 millimeters (mm) in diameter (see figure C-2) and contain 7 grams (China’s High Temperature Gas-Cooled Reactor - Pebble-bed Module (HTR-PM)) of uranium at 19.5 percent enrichment (Ref. C-[58]). Assuming an area packing of a cube (as spheres will result in gaps of air between the pebbles), each pebble takes up an area of 0.00216 cubic meters (m^3). Additionally, the adversary needs to remove 10 kg of uranium-235. This would mean that the adversary had to remove twenty-nine 55-gallon drums of pebbles to obtain 10 kg of uranium-235 and would need motorized transport to remove the material. Table C-1 below contains detailed information.

Table C-1. Material and Container Information

	Items/Containers					
Material	U-235 mass/ Total mass of items	Container Tare Mass (kg)	Mass of Material (kg)	Total Mass (kg)	U Mass (kg)	U-235 Mass (kg)
Finished Pebbles (loose)	0.0054	n/a	0.202	n/a	0.007	0.0011
Finished Pebbles in 55-Gallon Shipping Container	0.0054	177.0	64.32	241	2.24	0.352

Design Basis #3: The inner area will not provide the means for motorized transport (or cranes) to move greater than 0.5 m^3 of pebbles or material per minute. This will provide a delay of about 6 minutes for the adversary to load or move the material outside of these areas. Table C-2 shows an estimate of the time required for theft.

Table C-2. Estimated Timeline

Adversary Step	Time (min):(sec)	Cumulative Time (min):(sec)
Disembark from truck	0:10	0:10
Unload tools, explosives, pallet mover	0:20	0:30
Blast through door	0:10	0:40
Blast through inner door	0:10	0:50
Transit to pebble storage area	1:00	1:50
Cut through fence	0:30	2:20
Load pallet onto pallet mover	0:45	3:05
Transit pallet to loading dock door	2:00	6:05
Load drums into truck using hand carts	3:00	9:05
Transit to pebble storage area	1:00	10:05
Load 2 pallets onto pallet movers	0:45	10:50
Transit pallets to loading dock door	2:00	12:50
Load 8 drums into truck using hand carts	3:00	15:50
Transit to pebble storage area	1:00	16:50
Load 2 pallets onto pallet movers	0:45	17:35
Transit pallets to loading dock door	2:00	19:35
Load 8 drums into truck using hand carts	3:00	22:35
Transit to pebble storage area	1:00	23:35
Load 2 pallets onto pallet movers	0:45	24:20
Transit pallets to loading dock door	2:00	26:20
Load 8 drums into truck using hand carts	3:00	29:20
Exit site	**1:15**	**30:35**

PPS Requirement #2: The inner area will not provide the means for mechanized transport to enter or move within the building unless alternative compensating measures are put in place (e.g., guards positioned at entry points or vehicle access areas; spike strips).

PPS Requirement #3: Response forces shall be positioned off site and target a response time of less than 30 minutes from detection at the access-controlled area boundaries (Ref. C-[59]).

C.1.4 Summary of Cyber-Enabled Intrusion Scenario

Critical Detection Point for PPS: The critical detection point (CDP) is at the boundary of the inner area. Onsite staff will detect explosive breaches; however, gate crashing of the emergency gates may not be detected under certain environmental conditions (e.g., thunderstorm). Compromise of the entry control point and access control systems result in no provision of delay, but vehicular or motorized cranes are limited by passive features (narrow entry points) and nondigital means (spike strips; crane limits/governor) and credited for a delay of 6 minutes.

> *To determine the scope of the CSP and additional protective measures, the licensee should perform an AFSA in accordance with sections C.88 through C.103 if any CEIS could result in 10 CFR 73.110(a)(2) consequences.* [section C.87]

Delay cannot be credited unless the malicious act is detected and correctly assessed. The design of the detection system to incorporate noncyber independent protection layers, notwithstanding an access control analysis, is necessary to ensure that detection can occur at a point during the attack to allow for effective response. Detection and assessment should occur at or before the inner area boundaries. Detection at this point would allow 6 minutes for the response to occur.

Given the delay time and effort required by the adversary, the CEIS is probable only if detection at the CDP is avoided and the CAS onsite staff do not alert to the adversaries crashing the emergency gates for access to the owner-controlled and protected areas. An adversary functional scenario evaluation will be required.

C.2 CEIS ADVERSARY FUNCTIONAL SCENARIO

This example of an adversary functional scenario analyzes the attack pathways necessary for an adversary to use a cyberattack to steal nuclear material.

> *If any CEIS or CEAS results in the consequences listed in 10 CFR 73.110(a), then the licensee should perform an AFSA to further assess the potential consequences from such scenarios. This analysis excludes all CEISs and CEASs completely protected by SeBD elements (e.g., noncyber IPLs, analog systems, passive system/barriers).* [section C.88]

The CEIS analysis in section C.1 of this appendix determined that features necessary to prevent or limit the condition(s) may be initiated by a cyberattack resulting in radiological theft. The analysis reviewed a hypothetical situation in which an adversary was able to infiltrate a nuclear facility to remove 10 kg of uranium-235 (category II nuclear material). The analysis suggested a compromise of the detection function within the PPS, which may ultimately give an adversary unfettered access to nuclear material(s).

Event Description: An adversary conducts a cyberattack targeting the detection function of the alarm communication and display (AC&D) system, which allows the adversary to evade detection completely or after the CDP necessary for offsite forces to respond.

Scenario Assumption: An adversary crashes through emergency vehicle gates at the owner-controlled area and protected area. There are no guards and limited means of detection at these specific boundary crossings.

Assumption: The detection function relies on the generation of data by the sensor (i.e., alarm), communication of the data to equipment that processes the data, and then for presentation of the data, to an entity that assesses the sensor data. Figure C-3 shows the detection function broken down into its key subfunctions.

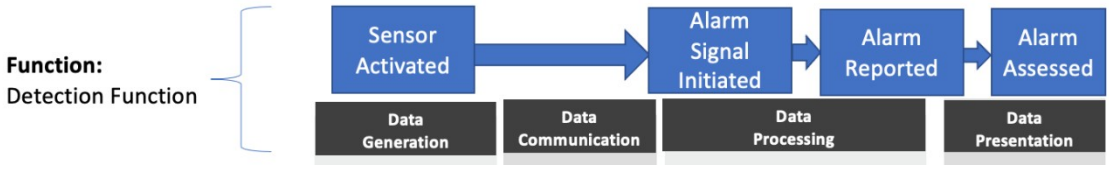


Figure C-3. Detection Function (information flows and subfunctions)

PPSs are used for the protection of special nuclear material, source material, and byproduct material. A licensee would be permitted to rely on the use of digital assets for implementing the PPS functions that would be required to meet the 10 CFR 53.860(a) requirements. Therefore, this consequence deals with a scenario in which, for example, a cyberattack adversely impacts the digital assets and associated security functions used by the licensee to meet the 10 CFR 53.860(a) requirements. Security digital assets include those used for nuclear material control and accounting. Such a consequence would not be applicable to commercial nuclear plant designs that do not rely on the use of digital assets for implementing the security functions required for meeting the 10 CFR 53.860(a) requirements. [section C.34]

C.2.2 Preliminary Analysis

Compromise #1: Compromise of data generation function to not provide an alarm.

Compromise #2: Compromise of data communication to not transmit the alarm for data processing.

Compromise #3: Compromise of data processing that "hides" the alarm condition from the data presentation subfunction and thus from the operator.

While the above does not represent a complete set, it lists some of the significant impacts of compromise on the detection function and subfunctions.

Pursuant to 10 CFR 73.110(d)(2), a licensee would need to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, delay, respond to, and recover from cyberattacks capable of causing the consequences identified in 10 CFR 73.110(a). [section C.36]

C.2.3 Preliminary Design Considerations

Design Consideration #1 (Compromise #1): Sensors at the CDP will need to implement a noncyber independent protection layer that provides a signal that does not require digital generation.

Design Consideration #2 (Compromise #2): An alternative analog signal is necessary to ensure that sensor data will be received even if the data communication function is compromised by a cyberattack. This design requirement will reduce the likelihood that the entire detection function will be degraded, but may decrease the performance of the function.

Design Consideration #3 (Compromise #3): A single point of failure in the data processing subfunction should not be implemented as it would not meet the implementation of a defense-in-depth strategy pursuant to 10 CFR 73.110(d)(2). The use of an independent and redundant system for implementing this subfunction is recommended.

Design Consideration #4 (All): A DCSA implementation is required to separate detection functions at required boundaries or internal to structures.

DCSA Requirement #1: The PPS requires a DCSA that consists of two zones, one for a normal AC&D system and the other for security critical (SC) AC&D system monitoring sensors, providing communications and processing for display at the CAS. The event tree in figure C-4 below takes into account this initial DCSA requirement.

A comprehensive AFSA should thoroughly analyze multiple attack sequences. For the purposes of this example, only one sequence is analyzed. In this example, an attack path is a sequence of PPS functions whose collective failure will lead to nuclear material theft. The adversary's attack progression is modeled by all paths leading to consequence in the event tree depicted in figure C-4.

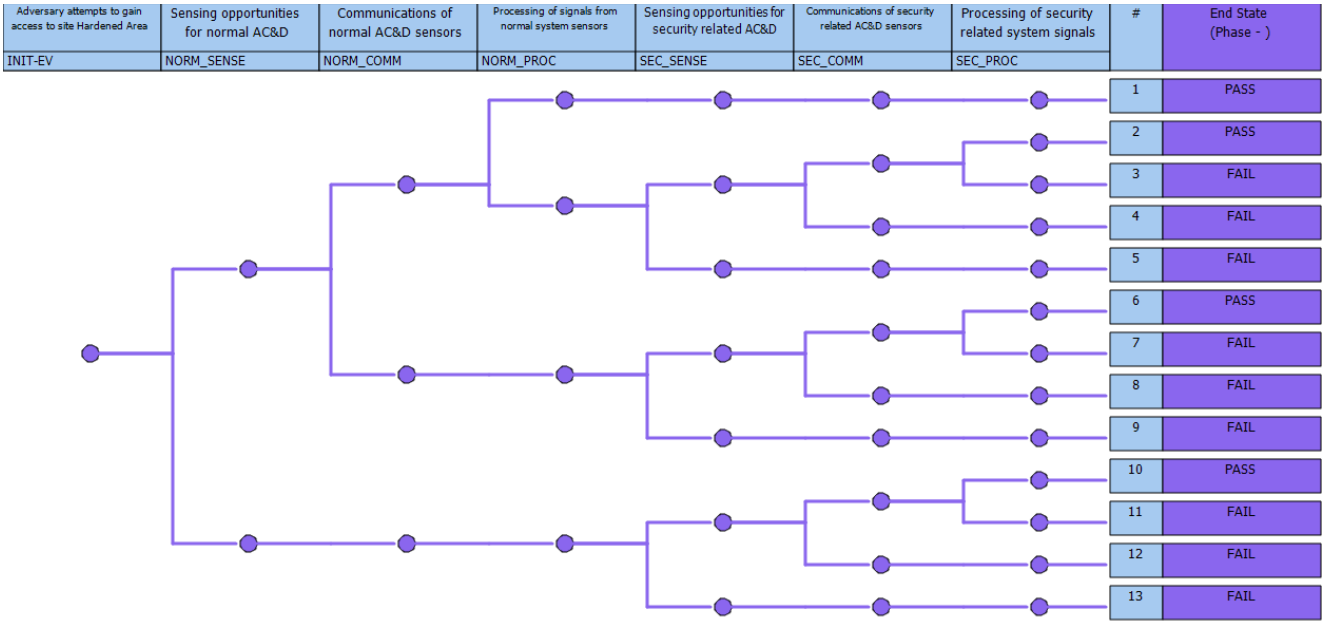


Figure C-4. AC&D Event Tree

The AFSA aims to provide plant capability defense in depth by specifying prohibitive CSP elements (e.g., forbid use of wireless communications) and passive, deterministic DCSA elements to mitigate or control adversary access to attack pathways or eliminate these pathways. Figure 6 describes the AFSA. [section C.89]

CSP Requirement #1: Prohibition of wireless communications within the AC&D (normal and SC) systems.

No assumptions beyond the above two requirements are made at this point regarding either the security or DCSA posture of the systems, components, and networks of the PPS. Initially, all components are assumed to be physically accessible and communication between components required for operation is assumed to be insecure (e.g., unencrypted, bidirectional). Requirements identified in the AFSA should be documented in the CSP.

> *The essential element of the AFSA is the assumption that the adversary is able to compromise functions in any manner that allows for progression of attack scenarios (i.e., attack success) immediately upon adversary access.* [section C.92]

This analysis considers only logical or physical access to system nodes or networks. If access cannot be prevented by passive controls or DCSA elements, the system is further analyzed in the following tier.

> *For each CEIS and CEAS, the following attack pathways should be considered:*
>
> *a. physical access,*
> *b. wired communications,*
> *c. wireless communications, and*
> *d. portable media/device connectivity.* [section C.93]

For each function, analyze the availability of each attack path.

The normal AC&D and SC AC&D systems provide the detection function. The functional analysis will use the event tree in Figure C-4.

C.2.4 Pathway Analysis

> *If the adversary can potentially advance a CEAS or CEIS to completion, the CSP or DCSA may need to include additional mitigation. A necessary attribute of these additional mitigation measures is that they do not require action by licensee personnel or action by a digital system to deny the adversary access to the attack pathway. The following are some mitigating measures that can be considered for inclusion:*
>
> > *a. prohibitive CSP elements, such as prohibition of wireless for critical systems, remote access, or other capabilities that allow the adversary to access the attack pathways,*
> >
> > *b. location of critical systems within inaccessible or protected locations that will always deny adversary access, and*
> >
> > *c. passive and deterministic technical measures needed as part of the DCSA implementation, such as a data diode, or unidirectional taps.* [section C.95]
>
> *Based on the analysis, the DCSA and CSP implementation should address the following:*
>
> *a. Eliminate attack vectors. For example, the DCSA implements a deterministic, unidirectional communications pathway to eliminate access to wired networks*

from remote or adjacent networks. Another example includes a CSP implementation that forbids wireless communications within critical systems.

b. Mitigate attack vectors using the following means:

(1) Minimize attack vectors. For example, the DCSA implementation places critical systems within the most secure boundaries with supporting CSP implementation of licensee-identified procedures that strictly control physical access to these systems.

(2) Control access to attack vectors. For example, CSP implementation of licensee-identified technical and administrative controls supplements the physical control measures of critical systems.

(3) Detect unauthorized access to attack vectors. This capability will rely on items b(1) and b(2) to increase the likelihood of detecting such access. For example, the CSP implements licensee-identified technical and administrative controls to detect unauthorized access to critical systems. [section C.96]

C.2.4.1 *Normal AC&D Analysis*

The wireless pathway is eliminated for all stages by the CSP prohibition of its use in the normal AC&D system.

Sensing Opportunities (e.g., microwave, pressure sensors, vibration sensors)

Physical Access: Mitigated—The component devices that support sensing opportunities are in locations difficult to access without detection (e.g., accessible only during authorized maintenance).

Wired Communication: Mitigated—Wires and cables are inaccessible either by being in secure conduit or buried.

Endpoints: Mitigated—Above-ground cabling is located within secure conduit or secured field distribution boxes (FDBs) with physical locks and keys.

Portable Media/Mobile Devices (PMMDs): Controlled—PMMDs may have port blockers installed or additional locks with physical keys.

Communications

Physical Access: Mitigated—The components are located in locked FDBs.

Wired Communication: Mitigated—Wires and cables are inaccessible either by being in secure conduit or buried.

***Endpoints*:** Mitigated—Above-ground cabling is located within secure conduit or secured FDBs with physical locks and keys.

PMMDs: Mitigated—PMMDs may have port blockers installed or additional locks with physical keys.

Data Processing/Presentation

Physical Access, Wired Communication, PMMD Pathways: Mitigated—Because these pathways are located in the CAS and network equipment room, only authorized staff have access. The two-person rule and strict access control will be applied.

C.2.4.2 ***Security Critical AC&D Analysis***

Sensing Opportunities (e.g., microwave, pressure sensors, vibration sensors)

Physical Access: Mitigated—The component devices that support sensing opportunities are in locations difficult to access without detection (e.g., only accessible during authorized maintenance). Access-controlled areas will provide enhanced detection in areas not requiring routine personnel traffic.

Wired Communication: Mitigated—Wires and cables are inaccessible either by being in secure conduit or buried.

Endpoints: Mitigated—Above-ground cabling is located within secure conduit or secured FDBs with physical digital locks requiring two-factor authentication and detection of FDB access.

PMMDs: Eliminated—Devices are designed with no externally accessible interfaces for PMMDs or irreversible methods for port blocking (e.g., resin, making inoperable, removal of interfaces).

Communications

Physical Access: Mitigated and Minimized—The components are located in locked FDBs requiring two-factor authentication with detection of FDB access.

Wired Communication: Mitigated—Wires and cables are inaccessible by either being in secure conduit or buried.

PMMDs: Eliminated—Devices designed with no externally accessible interfaces for PMMDs or irreversible methods for port blocking (e.g., resin, making inoperable, removal of interfaces).

Data Processing/Presentation

Physical Access, Wired Communication, PMMD Pathways: Mitigated—Because these pathways are located in the CAS and network equipment room, only authorized staff have access. The two-person rule and strict access control will be applied. SC AC&D pathways are not accessible during normal use, and display is available only to indicate alarms at the CDP. Maintenance activities are strictly controlled.

PPS Requirement #1 (Analog Sensor and Communication to CAS): To address Design Considerations #1 and #2, an alternative analog sensor and communications are needed on the pathway to the emergency gates to the owner-controlled and protected areas. This analog sensor will be outputted to an alarm within the CAS (noncyber/digital) to ensure detection if the adversary can compromise both AC&D systems.

> *The supply chain attack pathway is addressed separately in sections C.145 through C.151, which provide guidance for mitigating the risk associated with such a pathway that may allow an adversary to compromise the system function(s) in a way that advances the CEAS or CEIS.* [section C.94)]

A supply chain attack pathway is not considered as a part of this functional example.

APPENDIX C REFERENCES

[1]. *U.S. Code of Federal Regulations* (CFR), "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants," Part 53, Chapter I, Title 10, "Energy."

[2]. CFR, "Physical Protection of Plants and Materials," Part 73, Chapter I, Title 10, "Energy."

[3]. U.S. Nuclear Regulatory Commission (NRC), Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," Washington, DC, February 25, 2002. (Agencywide Documents Access and Management System (ADAMS) Accession No. ML020510635)

[4]. NRC, Order EA-03-086, "Design Basis Threat for Radiological Sabotage," Washington, DC, April 29, 2003. (Safeguards information)

[5]. NRC, SRM-COMWCO-10-0001, "Staff Requirements—COMWCO-10-0001—Regulation of Cyber Security at Nuclear Power Plants," Washington, DC, October 21, 2010. (ADAMS Accession No. ML102940009)

[6]. NRC, Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Washington, DC. (ADAMS Accession No. ML102870022)

[7]. NRC, RG 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licensees, Certifications, and Approvals for Non-Light-Water Reactors," Washington, DC. (ADAMS Accession No. ML20091L698)

[8]. Nuclear Energy Institute, NEI 18-04, Revision 1, "Risk-Informed Performance-based Guidance for Non-Light Water Reactor Licensing Basis Development," Washington, DC, August 2019. (ADAMS Accession No. ML19241A472)

[9]. NRC, Draft Regulatory Guide (DG) 5076 (proposed new RG 5.97), "Guidance for Technology Inclusive Requirements for Physical Protection of Licensed Activities at Commercial Nuclear Plants," Washington, DC.

[10]. NRC, DG-5061, Revision 1 (proposed Revision 1 to RG 5.71), "Cyber Security Programs for Nuclear Power Reactors," Washington, DC, February 2022. (ADAMS Accession No. ML21095A329)

[11]. NRC, RG 5.83, "Cyber Security Event Notifications," Washington, DC. (ADAMS Accession No. ML14269A388)

[12]. CFR, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," Part 37, Chapter I, Title 10, "Energy."

[13]. National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations," Gaithersburg, Maryland, April 2013.

[14]. NIST SP800-82, Revision 2, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, Maryland, May 2015.

[15]. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002:2013, "Information technology—Security techniques—Code of practice for information security controls," Geneva, Switzerland, October 2013.

[16]. IEC 63096:2020, "Nuclear power plants—Instrumentation, control and electrical power systems—Security controls," Geneva, Switzerland, October 2020.

[17]. IEC 62443-3-3:2013, "Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels," Geneva, Switzerland, August 2013.

[18]. Information Systems Audit and Control Association, “Control Objectives for IT 2019 (COBIT 2019),” Schaumburg, Illinois, November 2018.

[19]. NRC, “Nuclear Regulatory Commission International Policy Statement,” *Federal Register*, Vol. 79, No. 132, July 10, 2014, pp. 39415–39418.

[20]. NRC, Management Directive (MD) 6.6, “Regulatory Guides,” Washington, DC. (ADAMS Accession No. ML18073A170)

[21]. International Atomic Energy Agency (IAEA), Nuclear Security Series No. 42-G, “Computer Security for Nuclear Security,” Vienna, Austria, July 2021.

[22]. IAEA, Nuclear Security Series No. 23-G, “Implementing Guide for Security of Nuclear Information,” Vienna, Austria, February 2015.

[23]. IAEA, Nuclear Security Series No. 17-T, “Computer Security Techniques at Nuclear Facilities,” Vienna, Austria, September 2021.

[24]. IAEA, Nuclear Security Series No. 33-T, “Computer Security of Instrumentation and Control Systems at Nuclear Facilities,” Vienna, Austria, May 2019.

[25]. IAEA, Nuclear Energy Series Technical Report NR-T-3.30, “Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants,” Vienna, Austria, December 2020.

[26]. IAEA, Nuclear Energy Series No. NP-T-3.21, “Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities,” Vienna, Austria, September 2016.

[27]. IAEA, Nuclear Energy Series Technical Report NP-T-1.13, “Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants,” Vienna, Austria, November 2015.

[28]. IAEA, Non-Serial Nuclear Security Publication, IAEA-TDL-011, “Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain,” Vienna, Austria, December 2022.

[29]. IEC, 62645:2019, “Nuclear power plants—Instrumentation, control and electrical power systems—Cybersecurity requirements,” Geneva, Switzerland, November 2019.

[30]. ISO/IEC, 27001:2013, “Information technology—Security techniques—Information security management systems—Requirements,” Geneva, Switzerland, October 2013.

[31]. IEC, 62859:2016+AMD1:2019 CSV, “Consolidated version Nuclear power plants—Instrumentation and control systems—Requirements for coordinating safety and cybersecurity,” Geneva, Switzerland, October 2019.

[32]. IEC, 62443 Series, “Industrial communication networks—IT security for networks and systems,” Geneva, Switzerland, from November 2010 to June 2020.

[33]. NRC, “Policy Statement on the Regulation of Advanced Reactors,” *Federal Register*, Vol. 73, No. 199, October 14, 2008, pp. 60612–60616.

[34]. NRC, Advanced Reactor Stakeholder Public Meeting, Washington, DC, August 26, 2021. (ADAMS Accession No. ML21237A463)

[35]. NIST, SP800-37, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” Gaithersburg, Maryland, December 2018.

[36]. MITRE Corporation, “MITRE ATT&CK for Industrial Control Systems: Design and Philosophy,” McLean, Virginia, March 2020.

[37]. Office of the Director of National Intelligence, “Cyberthreat Framework,” accessed from https://www.dni.gov/index.php/cyber-threat-framework on November 14, 2021.

[38]. NRC, “Response to NEI White Paper, ‘Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with the Balance of Plant,’” Washington, DC, August 14, 2020. (ADAMS Accession No. ML20209A442)

[39]. NEI 08-09, Revision 6, “Cyber Security Plan for Nuclear Power Reactors,” Washington, DC, April 2010. (ADAMS Accession No. ML101180437)

[40]. NRC, MD 8.4, “Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests,” Washington, DC. (ADAMS Accession No. ML18093B087)

[41]. Committee on National Security Systems Glossary, April 2015, available at https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.

[42]. NIST, NISTIR 7864, “The Common Misuse Scoring System (CMSS): Metrics for Software Feature Misuse Vulnerabilities,” Gaithersburg, Maryland, July 2012.

[43]. IAEA, Nuclear Security Series No. 13, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities,” Vienna, Austria, January 2011.

[44]. IAEA, Nuclear Security Series No. 8-G, “Preventive and Protective Measures Against Insider Threats,” Vienna, Austria, January 2020.

[45]. ISO, Guide 73:2009, “Risk management—Vocabulary,” Geneva, Switzerland, November 2009.

[46]. ISO/IEC, 27000:2018, “Information technology—Security techniques—Information security management systems—Overview and vocabulary,” Geneva, Switzerland, February 2018.

[47]. Gartner, Gartner Glossary, https://www.gartner.com/en/information-technology/glossary, 2022.

[48]B-. H.D. Gougar, “High Temperature Gas-Cooled Reactor—History, Physics, Design Features,” Idaho National Laboratory, Idaho Falls, Idaho, July 2019.

[49]B-. B.Waites et al., “Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors. High Temperature Gas-Cooled Pebble Bed Reactor Licensing Modernization Project Demonstration,” Document Number SC-29980-200, Southern Company, 2018.

[50]B-. U.S. Department of Energy, “Conceptual Design Summary Report, Modular HTGR Plant, Reference Modular High-Temperature Gas-Cooled Reactor Plant,” DOE-HTGR-87-092, Bechtel National, Inc., under subcontract to Gas-Cooled Reactor Associates, Contract DE-AC03-7, Reston, Virginia, September 1987.

[51]B-. Oak Ridge National Laboratory, “Advanced Control and Protection System Design Methods for Modular HTGRs,” ORNL/TM-2012/170, Oak Ridge, Tennessee, May 2012. (Agencywide Documents Access and Management System (ADAMS) Accession No. ML12194A344)

[52]B-. Oak Ridge National Laboratory, “Task 1—Control and Protection Systems in VHTRS for Process Heat Applications,” LTR/NRC/RES/2010-001, Oak Ridge National Laboratory, Oak Ridge, Tennessee, September 2010. (ADAMS Accession No. ML12194A354)

[53]B-. U.S. Nuclear Regulatory Commission, “Next Generation Nuclear Plant Phenomena Identification and Ranking Tables (PIRTs)—Volume 1: Main Report,” NUREG/CR-6944, Vol. 1 (ORNL/TM-2007/147, Vol. 1), Washington, DC, March 2008. (ADAMS Accession No. ML081140459)

[54]B-. U.S. Nuclear Regulatory Commission, “Next Generation Nuclear Plant Phenomena Identification and Ranking Tables (PIRTs)—Volume 2: Accident and Thermal Fluids Analysis PIRTs,” NUREG/CR-6944, Vol. 2 (ORNL/TM-2007/147, Vol. 2), Washington, DC, March 2008. (ADAMS

Accession No. ML081140460)

[55]B-. U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, Revision 0, “Cyber Security Programs for Nuclear Facilities,” Washington, DC, January 2010. (ADAMS Accession No. ML090340159)

[56]C-. International Atomic Energy Agency, IAEA Nuclear Security Series No. 13, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities” (INFCIRC/225/Revision 5), Vienna, Austria, 2011.

[57]C-. D. Yurman, “TRISO Fuel Successfully Fabricated in Canada,” April 17, 2021. [Online]. Available: https://neutronbytes.com/2021/04/17/triso-fuel-successfully-fabricated-in-canada.

[58]C-. P.A. Demkowicz, B. Liu, and J.D. Hunn, “Coated Particle Fuel: Historical Perspectives and Current Progress,” Oak Ridge National Laboratory, Oak Ridge, Tennessee, 2018.

[59]C-. A.S. Evans and M.J. Parks, “U.S. Domestic Small Modular Reactor Security by Design,” Sandia National Laboratories, Albuquerque, New Mexico, 2020.