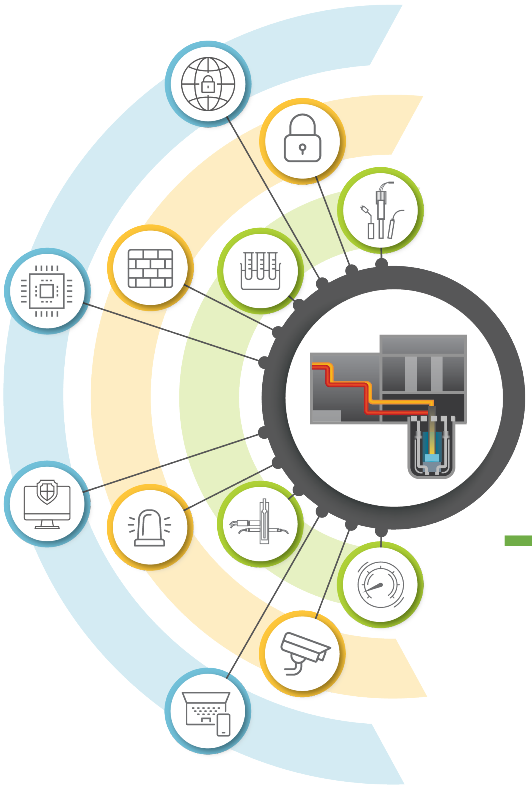

Advanced Reactor Safeguards and Security

Proposed Classifications of Remote Operations for Nuclear Reactors Based on Physical and Cybersecurity Considerations

Prepared for
US Department of Energy

Joseph Oncken
Idaho National Laboratory

Christopher Chwasz
Idaho National Laboratory

Shannon Eggers
Idaho National Laboratory

Thomas Ulrich
Idaho National Laboratory

August 2025
INL/RPT-25-06057, Rev. 0

DISCLAIMER

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

INL/RPT-25-06057, Rev. 0

Advanced Reactor Safeguards and Security

Proposed Classifications of Remote Operations for Nuclear Reactors Based on Physical and Cybersecurity Considerations

Joseph Oncken
Idaho National Laboratory
Christopher Chwasz
Idaho National Laboratory
Shannon Eggers
Idaho National Laboratory
Thomas Ulrich
Idaho National Laboratory

August 2025

Idaho National Laboratory
Advanced Reactor Safeguards and Security
Idaho Falls, ID 83404

https://energy.sandia.gov/arss

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy Under DOE Idaho Operations Office
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

EXECUTIVE SUMMARY

The incorporation of remote operations into reactor operations is a topic of high interest among advanced and small modular reactor (A/SMR) vendors, with some considering it essential to the success of their business models. However, remote operations are a concept novel to the nuclear industry. While various technical aspects of remote operations have been explored, a significant gap remains in understanding the security implications of integrating remote operations into reactor designs, particularly concerning the security requirements for remote-operations facilities and infrastructure.

This report aims to address this gap by first defining classes of remote operation based on the extent of remote access to reactor control systems and grounded in the existing regulatory framework with compatible terminology. Secondly, the report outlines the physical and cybersecurity requirements applicable to remote-operations facilities and infrastructure at each defined class. These requirements are based on existing licensing frameworks provided by 10 Code of Federal Regulations (CFR) Part 50 and 10 CFR Part 52, as well as the upcoming A/SMR licensing framework in the proposed Part 53. The assessment focuses specifically on security regulations, such as 10 CFR Part 73, which includes provisions for both cybersecurity (§ 73.54) and physical security (§ 73.55).

This report proposes five classes of remote reactor operations. Class 1 involves remote monitoring only, with no control over reactor systems. Class 2 allows for the remote issuance of allowlisted commands to the reactor facility. Class 3 extends control to non-safety-significant, non-safety-related, or not important to safety systems and equipment. Class 4 permits remote control of safety-significant systems. Finally, Class 5 allows remote control of safety-related systems. It is important to note that these classes were defined purely with functionality in mind, without considering the practicality or feasibility of implementation for each class under current or upcoming regulatory guidance. The intention behind this approach is to enable an assessment of which security requirements apply to each class, allowing readers to evaluate the implementation possibilities for their specific use cases.

Following the definition of remote-operation classes, the report assesses the specific physical and cybersecurity requirements applicable to the remote-operations facility and infrastructure within each defined class. This includes defining the types and locations of operators that are possible at each class of operation and, based on operator type and location, as well as functionality within each class, outlining the physical and cybersecurity requirements. By detailing the security requirements by class, the report provides readers with the information needed to determine the type of security program they may need to implement for their desired concept of operation.

The next contribution of this report was to assess the practicality of implementing each proposed class of remote operations based upon the security requirement assessment. In short, three of the five proposed remote-operation classes were found to possibly have a practical path forward to implementation under the U.S. regulatory framework. Class 1 remote operations are currently in use in the U.S. while Class 2 and 3 remote operations may be logistically possible to implement under the U.S. regulatory framework. The final two Classes, 4 and 5, would likely be logistically difficult, if not infeasible to implement within the current U.S. physical- and cybersecurity regulatory framework.

Given the results of the feasibility assessment, an example architecture is proposed for both Class 2, remote allowlisted commands, and Class 3, remote control of non-safety systems as well as security implication assessments of each architecture. These example implementations are not meant to be prescriptive in terms of how Class 2 or Class 3 remote operations should be deployed; instead, they are intended to be informative to stakeholders on how Class 2 or Class 3 could potentially be applied in order to inform their system design. An example architecture for Class 1 remote monitoring was not provided as Class 1 in already in use in U.S. nuclear operations. Example architectures for Class 4 and Class 5 were not provided due to their assessment of being likely infeasible to implement.

The final contribution is an assessment of the physical- and cybersecurity implications of introducing autonomous operations into an A/SMR. What was found was that the security implications can be separated into two cases. Autonomous operations supported by SSCs located only at the reactor site, and autonomous operations supported by SSCs outside of the reactor site. For the first case, the introduction of autonomous systems will likely not change the facility's requirement to comply with existing cyber and physical security regulations. The largest impact would be the increased complexity of evaluating these systems for compliance with regulation due to the increased complexity of an autonomous system. The second case exists as autonomous systems may require offsite support due to large computing and data-storage requirements of autonomous systems. In this situation, the autonomous system becomes a remote operation system and requires the application of the remote operations framework proposed in this report.

Overall, this report serves to elucidate the impact that remote and autonomous operations will have on the security programs and design of A/SMRs. It provides a structured framework to categorize different concepts of remote operations, the applicable security requirements associated with remote and autonomous operations, and potential implementation avenues for remote and autonomous operations. Reactor vendors can use this information to make informed decisions about the implementation of secure remote operations for their reactor designs.

ACKNOWLEDGEMENTS

The authors would like to thank and acknowledge Zachary Dalton and Kreg Roenfeldt for their respective contributions on critical infrastructure threat analysis and network architecture.

Page intentionally left blank

CONTENTS

EXECUTIVE SUMMARY v

ACKNOWLEDGEMENTS v

ACRONYMS xi

1 INTRODUCTION 1

1.1 Motivation for Remote Operations of Nuclear Power Reactors 1

1.2 Regulatory Context and Considerations 2

1.3 Overview of Current Physical-Protection Practices 2

1.4 Overview of Current Nuclear-Cybersecurity Practices 3

1.5 Report Structure 5

2 PROPOSED CLASSES OF REMOTE OPERATIONS FOR NUCLEAR REACTORS 6

2.1 Class 1: Remote Monitoring Only 7

2.2 Class 2: Remote Allowlisted Commands 7

2.3 Class 3: Remote Control of Non-Safety Systems 8

2.4 Class 4: Remote Control of Safety-Significant and Important-to-Safety Systems and Equipment 8

2.5 Class 5: Remote Control of Safety-Related Systems and Equipment 9

3 SECURITY CONSIDERATIONS FOR REMOTE OPERATIONS CLASSES 9

3.1 Class 1: Remote Monitoring Only 10

3.1.1 Reactor Operations 10

3.1.2 Physical Protection 11

3.1.3 Cybersecurity 13

3.2 Class 2: Remote Allowlisted Commands 13

3.2.1 Reactor Operations 13

3.2.2 Physical Protection 14

3.2.3 Cybersecurity 15

3.3 Class 3: Remote Control of Non-Safety-Significant, Not Important to Safety, or Non-Safety-Related Systems and Equipment 15

3.3.1 Reactor Operations 15

3.3.2 Physical Protection 16

3.3.3 Cybersecurity 17

3.4 Class 4: Remote Control of Safety-Significant Systems 17

3.4.1 Reactor Operations 17

3.4.2 Physical Protection 18

3.4.3 Cybersecurity 18

3.5 Class 5: Remote Control of Safety-Related Systems 19

3.5.1 Reactor Operations 19

3.5.2 Physical Protection 19
3.5.3 Cybersecurity 19
4 IMPLEMENTATION PATHWAYS FOR REMOTE OPERATIONS 20
4.1 Remote-Operation Implementation Background Information 20
4.1.1 Defensive Computer Security-Architecture Framework 20
4.1.2 Secure Remote Connections 22
4.2 Class 1: Remote Monitoring Only 24
4.3 Class 2: Remote Allowlisted Control 24
4.3.1 Remote Allowlist Control Implementation 25
4.3.2 Allowlist Cybersecurity Regulatory Considerations 30
4.3.3 Allowlist Physical Security Considerations 31
4.4 Class 3: Remote Control of Non-Safety Systems 31
4.4.1 Remote Non-Safety Control Implementation 32
4.4.2 Non-Safety Cybersecurity Consideration 35
4.4.3 Non-Safety Physical Security Considerations 36
4.5 Class 4: Remote Control of Safety-Significant and Important-to-Safety Systems 36
4.6 Class 5: Remote Operation of Safety-Related Systems 37
4.7 Non-Regulatory Cyber Security Implications of Remote Operations 37
4.7.1 Current and Recent Threat Landscape 37
4.7.2 Cyberattack Impact on Proposed Class 2 and Class 3 Architectures 39
5 AUTONOMOUS OPERATIONS AND THE RELATION TO REMOTE OPERATIONS 39
5.1 Autonomous Systems Contained Within Plant Boundary 39
5.2 Autonomous Systems with External Support 40
6 CONCLUSIONS 40
7 REFERENCES 42

FIGURES

Figure 1. Proposed hierarchical remote operation classes defined by the supported level of remote access and control. 7
Figure 2. Characterization of each remote activity class for DAs located at a nuclear facility 10
Figure 3. Example of a DCSA [16]. 21
Figure 4. Allowlisted command structure basic information flow. 25
Figure 5. Defensive cybersecurity architecture for the proposed remote allowlisted-command implementation. 27
Figure 6. Network diagram for the remote-operations center to reactor-facility connection for allowlisted control. 28

Figure 7. Defensive cybersecurity architecture for the proposed non-safety control implementation. 33

Figure 8. Network diagram for the remote operations center to reactor facility connection for non-safety control. 34

TABLES

Table 1. CDA categories as outlined by NEI 13-10, Revision 7 [12]. 4

Table 2. Recommended remote monitoring and access and control capability by categorization of reactor facility systems and remote operations class where M = monitoring and C = access and control. 7

Table 3. Physical Security of a Class 2 Remote Operations Facility with GLROs. 15

Table 4. Implementation practicality of each class of remote operations. 20

Table 5. Example mapping of security levels to functions and systems. 22

Table 6. Example mitigations for increased defense in depth for remote allowlisted operations. 29

Table 7. Example remote allowlist control functions. 29

Table 8. Example mitigations for increased defense in depth for remote non-safety control operations. 34

Table 9. Example non-safety functions that could be controlled from the remote operations center. 35

Page intentionally left blank

ACRONYMS

A/SMR	Advanced or small modular reactor
BOP	Balance of plant
CDA	Critical digital asset
CFR	Code of Federal Regulations
DA	Digital asset
DCSA	Defensive computer security architecture
DMZ	Demilitarized zone
DOE	U.S. Department of Energy
DOE-ID	U.S. Department of Energy-Idaho Operations Office
EP	Emergency preparedness
EPRI	Electric Power Research Institute
FERC	Federal Energy Regulatory Commission
GLRO	Generally licensed reactor operator
I&C	Instrumentation and control
IAEA	International Atomic Energy Agency
IDS	Intrusion-detection and assessment system
IPS	Intrusion prevention system
INL	Idaho National Laboratory
IT	Information Technology
LAN	Local area network
MCR	Main control room
MFA	Multifactor authentication
MPLS	Multiprotocol Label Switching
NEI	Nuclear Energy Institute
NIST	Nation Institute of Standards and Technology
NLO	Non-licensed operator
NPP	Nuclear power plant
NRC	Nuclear Regulatory Commission
OT	Operational technology
PA	Protected area
PLC	Programmable logic controller
PR	Protected area
PWR	Pressurized water reactor

RG	Regulatory Guide
SNM	Special nuclear material
SSC	Structures, systems, and components
SIEM	Security-incident and event monitoring
SSEP	Safety, important to safety, security, and emergency preparedness
U.S.	United States
VBIED	Vehicle-borne improvised explosive device
VA	Vital area
VPN	Virtual private network

Page intentionally left blank

Proposed Classifications of Remote Operations for Nuclear Reactors Based on Physical and Cybersecurity Considerations

1 INTRODUCTION

1.1 Motivation for Remote Operations of Nuclear Power Reactors

Advanced or small modular reactors (A/SMR) can provide significant cost savings for remote and limited-infrastructure locations. Envisioned applications include remote mining sites, remote communities, or remote oil and gas industries—use cases in which traditional power generation, reliant on fossil fuels, and the logistics of supply incur significant energy costs. However, traditional reactor operations and maintenance strategies may be cost prohibitive to a remotely deployed reactor due to logistical complexity and costs to post highly trained individuals in these remote locations. Thus, the economics associated with traditional onsite-staffing strategies are simply too costly to support A/SMRs sited in remote and infrastructure-limited locations. Remote operations are proposed as a potential solution to achieve a viable business case in which strategic site selection for remote-operations facilities can be done based on construction costs and workforce availability while the reactor itself can be deployed where thermal and electric energy are required. For the context of this report, remote operations are defined as the ability to monitor, manage, or control reactor-facility functions from outside the reactor-facility boundary. Realizing the economic benefits of remote operations requires minimizing staffing at the reactor site while maintaining safe and effective operations. Onsite-staffing reductions imply less local human oversight, control, and protection over the reactor while compensating for this onsite reduction through remote control of the reactor, automated or autonomous control of the reactor, or a combination of both. Other industries, such as oil and gas and wind energy, have successfully implemented remote monitoring and operation, demonstrating the feasibility of this approach for nuclear power.

The wind-energy industry, for example, has grown rapidly, driving a constant push to reduce the costs of operating and monitoring wind turbines. To reduce costs, most wind farms use centralized controllers to adjust the overall power output and the power level of individual turbines. These controllers distribute active-power references among the turbines, comprising central and local control levels. The wind industry employs condition-monitoring systems to detect and predict faults and failures with sufficient time margin to minimize maintenance downtime. This methodology for remote monitoring and predictive maintenance is especially beneficial for offshore wind farms, despite the substantial costs associated with condition-monitoring systems' design and installation [1]. The wind-power industry continues to improve remote-monitoring and control methodologies, offering valuable insights for developing similar frameworks in the nuclear industry.

The oil and gas industry has employed remote networks for monitoring and controlling processes across upstream, midstream, and downstream sectors for many years. These networks enable remote facilities to detect and report such abnormal events as leakages, corrosion, or other damage. They also allow for remote control of assets, including offshore entities controlled from a remote onshore control room [2]. The remote locations of most oil- and gas-refinement sites, often with hostile terrain and harsh weather, make remote operations crucial for cost reduction. This reasoning aligns with motivations for remote operations of A/SMR facilities.

In summary, while remote-operation applications exist in other industries, they have not been extensively pursued in the nuclear industry. Maturing A/SMRs and their near-term deployment require the development of safe and cost-effective remote-operations strategies. There are many different remote-operation paradigms that could be adopted differentially to address the diversity in reactor designs and use-case applications. Here we provide an analysis of the key elements germane to remote operations and evaluate those as they impact physical and cybersecurity issues. This report proposes a functionally defined remote-operations hierarchy to classify physical- and cybersecurity requirements, based on the amount of access to reactor structures, systems, and components (SSCs), with the intent to provide guidance for those considering remote operations in their A/SMR deployment plans. The development of this hierarchy and the classification of physical- and cybersecurity issues associated with different levels of remote-operation access are also detailed to provide the operational context associated with the hierarchical classifications.

1.2 Regulatory Context and Considerations

Commercial nuclear reactors are regulated under Title 10 in the Code of Federal Regulations (CFR), Part 50 [3] and Part 52 [4]. At present, A/SMRs and any supporting remote operations must meet the existing regulations established for the current generation of large light-water reactors. The proposed 10 CFR Part 53 [5] provides a technology-neutral framework for the licensing and regulation of commercial nuclear reactors, including A/SMRs, with the potential to be supported by remote operations. The proposed Part 53 does not contain explicit regulations and guidance on remote operations, but it does address other elements that have implications on possible concepts of deployment and operation relating to remote operation, to include operator licensing and control-room staffing. The commercial-reactor licensing frameworks reference the applicable physical- and cybersecurity regulations found in 10 CFR Part 73 [6], specifically §73.54 [7] and §73.55 [8].[a]

1.3 Overview of Current Physical-Protection Practices

In the United States (U.S.), commercial nuclear power plant licensees are required to protect against the design-basis threat of radiological sabotage, as defined by 10 CFR Part 73 [6]. Section 73.55 gives the requirements for a physical-protection program with the objective of providing: “high assurance that activities involving special nuclear material (SNM) are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety” [6, 8]. Commercial nuclear power licensees are required to have a physical-protection system that is designed to protect against the threat of radiological sabotage, which for light-water reactors is defined as significant core damage and spent-fuel sabotage. The Nuclear Regulatory Commission (NRC) has proposed rulemaking to revise the performance goal for small modular and non-light-water reactors with respect to the prevention of a significant release of radionuclides from any source. These performance goals are further defined within Regulatory Guide (RG) 5.81, Rev. 1 [9], and draft RG 5.81, Rev. 2 [10], to delineate target sets as the minimum set of equipment that, if prevented from performing their safety functions by an adversary, would result in the licensee’s not meeting the performance goal—through, for example, core damage, spent-fuel sabotage, or significant radionuclide release. Target sets are the defined adversary targets that a physical-protection program must be designed to protect against compromise, destruction, or being rendered non-functional.

Target sets may include safety-related and non-safety SSCs. Target sets may be similar to probabilistic risk assessment cut sets, comprised of failure combinations of safety SSCs that result in an undesirable end state, with each piece of equipment or operator action defined as a target element of a given target set. Target elements may include plant safety equipment and the associated instrumentation and control (I&C), power, cooling, working-fluid supply equipment, radionuclide barriers, structures, and required operator actions. It is through these target sets that cybersecurity considerations for digital assets (DAs) become relevant. These target sets may specifically include critical digital assets (CDAs), which

[a] The nomenclature for referring to 10 CFR and related documents uses the term Part to reference a part in its entirety, and the section symbol (§) or section term designation is used to reference subsections.

are DAs that perform or support safety-related, important-to-safety, security, and emergency-preparedness functions, within the cybersecurity analysis. A thorough definition of CDA is provided in Section 1.4 as part of the overview for current nuclear-cybersecurity practices. CDA target elements may be included within target sets due to the safety-function CDA role within the facility-safety analysis or if the compromise of the CDA through (malevolent) misuse could endanger the safety of radiological materials. The protection of target sets establishes the performance goal for the physical-protection system and the basis upon which the protective strategy is determined.

Commercial nuclear power plant licensees must also comply with deterministic physical-security requirements, such as:

- Insider mitigation
- Physical barriers (protected areas, vital areas, vehicles)
- Access control
- Searches
- Detection and assessment
- Communications
- Staffing.

These deterministic requirements are specific and apply to any part of the facility with components that meet established regulatory definitions. The deterministic requirements and protective strategy provide successive layers of defense against the design-basis threat of radiological sabotage. Layers of the security program may apply to a remote-operation facility according to the significance of the remote facility in a graded approach, ranging between a minimal number of layers to all layers applied and representing the full security program and regulatory requirements found in traditional commercial reactors.

1.4 Overview of Current Nuclear-Cybersecurity Practices

Commercial nuclear-power reactors in the U.S. must provide reasonable assurance that DAs providing or supporting safety-related, important-to-safety, security, and emergency-preparedness (SSEP) functions are adequately protected [7, 11]. Nuclear power plant licensees are subjective to “the Cyber Rule,” which is codified under 10 CFR §73.54, “Protection of Digital Computer and Communication Systems and Networks” [7]. Guidance documents by the NRC, Nuclear Energy Institute (NEI), and Electric Power Research Institute (EPRI) are used both domestically and internationally to develop and implement cybersecurity programs at nuclear power plants [11-15]. Additionally, the International Atomic Energy Agency (IAEA) provides international guidance for implementing a computer-security program [16-19]. For small modular reactors, microreactors, and advanced reactors, the NRC has proposed a new draft regulatory guide, DG-5075 (proposed Regulatory Guide 5.96), establishing cybersecurity programs for commercial nuclear plants licensed under 10 CFR Part 53 [20].

CDAs are defined as digital computers, communication systems, or networks (1) that perform SSEP functions or (2) are support assets which, if compromised, would adversely impact SSEP functions. Both the NRC and IAEA provide examples of defense-in-depth architectures in which a graded approach for different security levels provides more stringent protection for safety-related CDAs and less-stringent requirements for non-safety CDAs. It is important to note that NRC RG 5.71, Rev. 1 [11], uses Levels 0 to 4, with Level 4 as the most stringent, and IAEA NSS 17-T, Rev. 1, uses Levels 1 to 5, with Level 1 as the most stringent [16]. For purposes of clarity, the remainder of this paper will use the IAEA security-level designations.

For both NRC and IAEA defensive computer architectures, it is recommended to only allow one-way outbound digital communications from the most-stringent (e.g., safety-related functions) to a less-stringent level (e.g., IAEA Security Levels 1 and 2) using a unidirectional boundary device (e.g., a data diode). Depending on the assignment of SSCs within levels, one-way communication may also be required between subsequent less-stringent levels to prevent inbound circumventions through other segments of subsequent less-stringent levels (e.g., IAEA Security Levels 2 and 3). NSS 17-T Rev. 1 further defines security zones in the defensive architecture as logical and/or physical grouping of DAs with common cybersecurity requirements within security levels [16]. Communication between zones within a given security level may be unidirectional or bidirectional, depending on security requirements of each zone.

RG 5.71, Rev. 1, defines remote access as the “ability to access a CDA, computer, node, or network resource within an identified defensive level” from a device that is physically located in a less-secure level. It also currently establishes that remote access to CDAs located in the highest defensive level (e.g., IAEA Security Level 1) should be prevented [11]. While RG 5.71, Rev. 1, precludes the capability for remote control for IAEA Security Level 1 or 2 CDAs, remote monitoring of these CDAs is still available through data-forwarding and use of tools, such as data historians and security incident and event monitoring (SIEM) systems. Alternatively, DG-5075 states that, when access, control, or monitoring from remote locations is necessary to perform tasks and activities, then the defensive architecture should include appropriate protections, and the licensee should ensure that attack pathways are not available for any stage of a cyber-enabled accident scenario or intrusion scenario leading to radiological sabotage or physical intrusion [20].

NEI 13-10, Revision 7, which the NRC deems acceptable for use, provides CDA scoping criteria to streamline the process of applying cybersecurity controls. Descriptions of each CDA category are provided below in Table 1. A DA is defined as “a programmable device that uses any combination of hardware, firmware, and/or software to execute internally stored programs and algorithms, including numerous arithmetic or logic operations, without operation action” [12].

Table 1. CDA categories as outlined by NEI 13-10, Revision 7 [12].

Category	**Description**
Digital Asset	DA that does not perform or support an SSEP function and that does not fall under the scope of 10 CFR 73.54.
Emergency Preparedness (EP) CDA	CDAs associated with a licensee’s performance of required EP functions where an independent and diverse method to perform the function does not exist.
Balance of Plant (BOP) CDA	CDAs that can result in the generated megawatts being reduced to zero within 15 minutes for facilities with LOW impact on the bulk electric system, as designated by the Federal Energy Regulatory Commission (FERC).
BOP-Scram/Trip	BOP CDAs for FERC-designated medium- or high-impact facilities, as described by NEI 13-10, and BOP CDAs outside the protected area that are not air-gapped or isolated by a deterministic isolation device.
Indirect CDAs	CDAs that cannot have an adverse impact on safety or security functions prior to the detection of their compromise or failure and implementation of compensatory measures.
Direct CDAs	CDAs that are not EP, BOP, or indirect CDAs.

RG 5.71 Rev. 1 and NEI 08-09, Revision 7, provide a set of security measures used to protect CDAs from cyberattacks. These measures are classified as administrative (e.g., policies, procedures), technical (e.g., defensive architecture, authentication, encryption), and physical (e.g., locked doors, locked cabinets, located in protected or vital areas, tamper devices) controls.

1.5 Report Structure

The primary purpose of this report is to propose a framework for classifying remote operations of nuclear power plants defined based on the functions they provide and the access to the different types of SSCs needed to achieve that functionality. The framework also presents protections specific to each class and associated SSCs to meet physical- and cybersecurity regulatory requirements. Thus, the existing physical protection and cybersecurity practices presented in the previous Sections 1.3 and 1.4, respectively, establish the current regulatory context. By grounding the framework within the existing context, the proposed framework is compatible with current regulations.

Five classifications of remote operation are proposed; these cover the range of envisioned concepts for remote control and remote access to control systems that could be deployed in a remote concept of operation. Each remote-operations class, starting from 1, provides a greater level of access to reactor control SSCs from the remote operations center. The five proposed classes are:

1. Class 1: Remote Monitoring Only
2. Class 2: Remote Allowlisted Control
3. Class 3: Remote Control of Non-Safety Systems
4. Class 4: Remote Control of Safety-Significant and Important-to-Safety Systems
5. Class 5: Remote Control of Safety-Related Systems.

The five classes are hierarchically structured such that each subsequent, lower numerical-designation, class is less important to ensure safety and safeguards and therefore requires less-stringent protections. At a fundamental level the framework provides a structured manner to develop an informed remote concept of operations based on operational and security tradeoffs. Specifically, the framework provides mechanisms to evaluate the balance between the level of remote functionality for operational goals and the increased required protections needed to support access to SSCs required for that functionality. The classes of SSC are based, in part, on existing NRC cybersecurity classification schemes and are thus compatible to the existing physical and cybersecurity practices currently followed by the U.S. fleet of commercial reactors. Chapter 2 provides a detailed description for the five classifications and serves as a framework definition.

Chapter 3 presents the five classes of remote operations from the perspective of their security implications and relevant regulatory documents. This chapter aims to provide regulatory context with rationale for the classification groupings based on how SSCs are governed by physical- and cyber-regulations.

The framework is comprehensive in its classifications for all possible cases of remote operations. However, some of the classes of remote operations would likely incur significant potential risk and substantial costs of protections to mitigate those risks. Thus, within the bounds of existing communication- and control-system technologies, and with considerations for A/SMR safety characteristics, Chapter 4 presents a potential implementation strategy. This practical implementation follows industry best practices with regulatory compliance for current regulations. Broadly speaking, the implementation strategy recommends against remote-operation Classes 4 and 5. Class 2 and 3 remote operations may be possible, but there are nuances regarding how SSCs are categorized that must be considered and protected or avoided as appropriate. Class 1 is readily achievable and currently in practice in the U.S.

Last, Chapter 5 presents considerations for autonomous operations within the context of remote operations. The focus is on autonomous digital control-system functions which, by design, should be isolated to fulfill their intended purpose to maintain plant operations and stability without outside intervention. Autonomous systems may introduce additional external access needs through potential external high-performance computing requirements and high-frequency model updates. Within these remote-access conditions, the classes of the remote-operations framework can be applied to autonomous systems with no special considerations.

2 PROPOSED CLASSES OF REMOTE OPERATIONS FOR NUCLEAR REACTORS

Despite widespread adoption in other industries, the concept of remote operations is new to the commercial nuclear power industry. Proposed A/SMR technologies that rely on inherent behaviors and passive safety systems to respond to safety events have enabled the discussion of possible remote operation of these conceptual reactor facilities. The NRC has provided a licensing pathway for the control of such passively safe reactor sites as "self-reliant mitigation facilities" in the proposed Part 53 framework. Reactor developers have expressed interest in varying levels of remote operation for new reactor designs from the current use of remote monitoring to full control of a reactor from a remote facility, as evidenced by NRC pre-application document filings and developer-produced literature [21]. Definite plans for the licensing of a remote-controlled reactor facility are stymied by a lack of regulatory clarity and challenges in meeting regulatory requirements for both the safety and security of the reactor. Specifically, A/SMR developers plan to rely on the passive safety of their designs for remote operation, but have not fully characterized the applicable security challenges that such a deployment concept presents.

To highlight these remote-controlled nuclear-facility security challenges, this report structures remote nuclear operations into hierarchical classes, with corresponding security-measure requirements to provide a common platform to hold discourse on how to design, incorporate, and regulate remote operations for nuclear reactors. Proposed in this report are five classes of remote operation, each distinguished by the degree of remote control and remote access to SSCs classified by regulatory requirements within the reactor facility. Categorizing remote-operation activities into classes defined by regulatorily defined SSC classifications establishes a common framework to distinguish what measures of both physical- and cybersecurity are necessary for each class of remote-operation activity.

Five classes of remote operation are proposed; these cover the range of envisioned concepts for remote *control* and remote *access* to control systems that could be deployed in a remote concept of operations. Each class, starting from 1, provides a greater amount of access to reactor-control systems from the remote-operations center. It should be noted that each increasing class contains all of the functionality of each lower class. These classes should also only be interpreted as a sorting of functionality; viability of each class from a regulatory or practicality perspective was not considered in creation of the class and is the subject of Section 3.

Class 1 is defined as exclusively remote monitoring and represents the class with the most-restrictive access to control systems from the remote-operations facility. Only one-way communication is allowed out of the reactor facility to the remote-operations center. Class 2 introduces two-way communication, where a set of allowlisted commands are permitted to be sent from the remote-operations center to the reactor facility in addition to remote monitoring of data. Class 3 expands control capability with remote control of reactor-facility *non-safety-significant, or not important to safety*[b] SSCs. Class 4 introduces the capability to remotely control reactor facility *safety-significant* SSCs and *important to safety* CDAs. The final class, Class 5, adds remote control of reactor-facility safety-related SSCs. Figure 1 and Table 2 present the remote operation classes and their respective recommended access and control capability to reactor facility systems.

[b] By definition, non-safety significant and non-important to safety SSCs do not include safety-related SSCs.

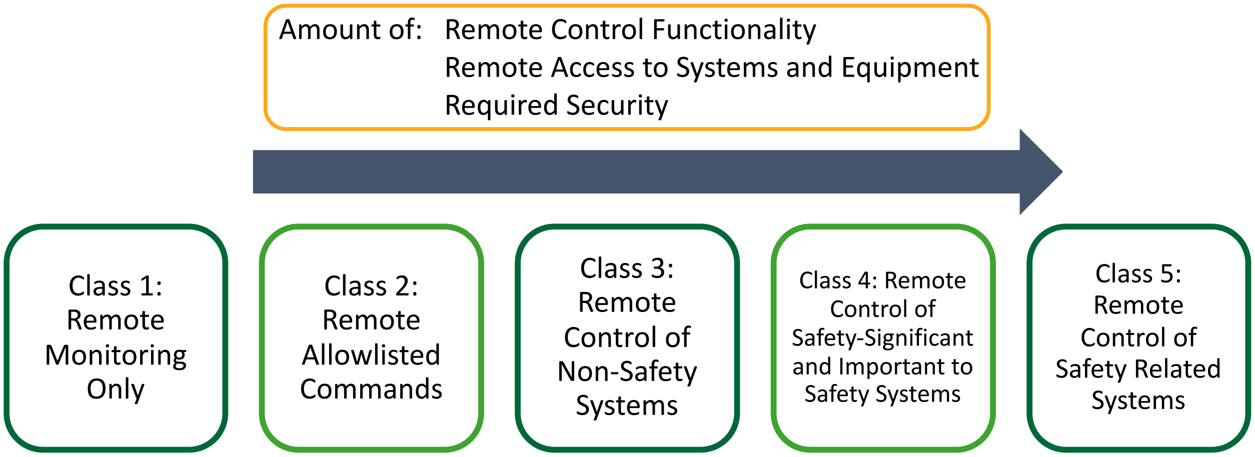
Amount of: Remote Control Functionality
Remote Access to Systems and Equipment
Required Security
Class 1: Remote Monitoring Only
Class 2: Remote Allowlisted Commands
Class 3: Remote Control of Non-Safety Systems
Class 4: Remote Control of Safety-Significant and Important to Safety Systems
Class 5: Remote Control of Safety Related Systems

Figure 1. Proposed hierarchical remote operation classes defined by the supported level of remote access and control.

Table 2. Recommended remote monitoring and access and control capability by categorization of reactor facility systems and remote operations class where M = monitoring and C = access and control.

Categorizations of Reactor Facility Systems	Remote Operations Class				
	Class 1	Class 2	Class 3	Class 4	Class 5
Non-Safety Systems	M only	M only	M, C	M,C	M,C
Safety Significant and Important to Safety Systems	M only	M only	M only	M,C	M,C
Safety Related Systems	M only	M only	M only	M only	M,C

The use of the SSC safety-classification scheme to define the remote-operation classes enables the clearest link between safety and security requirements for the prevention of radiological sabotage. The security requirements for both physical- and cybersecurity are directly tied to the safety SSC classifications and roles those SSCs play in operations and in responding to plant events.

2.1 Class 1: Remote Monitoring Only

The first class of the remote-operations hierarchy is conceptually defined as remote monitoring only. Remote monitoring is defined as the one-way transmission of plant and reactor operational data to a geographically distinct monitoring facility for plant- and reactor-performance observation, with no remote-control functionality or response requirements. In this scheme, reactor-facility data are sent to the remote-operations center using one-way outbound communication accomplished by the use of a unidirectional boundary device, e.g., data diode. Remote monitoring is currently an acceptable practice across the nuclear-power industry; therefore, Class 1 remote operations are already uniquely supported in the existing regulatory frameworks. Examples include the U.S. NRC Emergency Response Data System [22], a required system in the U.S. that provides real-time data from nuclear-plant computers to the NRC Operations Center and regional incident-response centers in the case of an emergency at a plant and the IAEA’s use of remote and unattended monitoring and transmission of safeguards-relevant data to the IAEA [23].

2.2 Class 2: Remote Allowlisted Commands

Class 2 remote operations introduce restrictive, inbound communication for two-way communication between the reactor and remote-operations facility to support a level of remote-control functionality. The inbound communication permits allowlisted commands from the remote-operations center to the reactor.

This is in addition to the allowance for sending remote-monitoring data given in Class 1. Allowlisting is a common cybersecurity practice in which only selected authorized programs are granted run permissions on managed devices. In the context of a remotely operated nuclear reactor, an allowlisted command architecture restricts the remote-operations facility to actuate locally predefined, verified, and validated control programs at the reactor site. For example, allowlisted commands could be reactor-power setpoints, such as 80, 90, or 100% power. Upon receipt of the command, the control system screens the allowlisted program against the current reactor condition to verify its execution maintains the reactor within safe operational boundaries for which the program was designed, then the corresponding allowlisted program executes on the control system to maneuver the reactor to the target setpoint. A central characteristic of the control in this class is that no allowlisted commands are required for safety, meaning that no allowlisted commands are required from the remote-operations center in order for the reactor to maintain a safe state. Any and all safety actions are taken by systems or personnel local to the reactor facility while remote-control functionality is purely for non-safety operational control of the reactor.

2.3 Class 3: Remote Control of Non-Safety Systems

Class 3 remote operations adds control functionality for those systems at the reactor facility that are not required to maintain reactor safety. These include:

- Non-Safety Related Systems
- Non-Safety Significant Systems
- Not Important-to-Safety Systems

In this report, non-safety-significant and non-safety-related SSCs are defined as all plant systems that do not meet NRC definitions of safety related [24] or safety significant [25]. Not important-to-safety systems are defined those systems that do not meet the NEI 10-04, Rev. 3, definition of “important to safety”. Typically, BOP CDAs and BOP-Trip/SCRAM CDAs (as defined in NEI 13-10 Rev. 7) and EP systems would fall under this class. However, it is possible for a BOP or EP CDA to be identified as important to safety. If this is the case, these SSCs would be excluded from this class.

Class 3 can be characterized most basically as remote-control access allowed from the remote-operations center for all SSCs that do not directly or indirectly impact reactor safety or facility security. Control of SSCs within Class 3 adds a higher level of access than Class 2 because individual commands can be executed from the remote-operations facility such that direct control of individual, non-safety-related actuators and control parameters can be manipulated. For example, a Class 3 command might send a control signal to energize a pump in a non-safety-related flow loop, such as a circulating water loop. Class 2 would not allow individual control of the pump because the control of the pump would be handled only by the allowlisted program, locally operating on the circulating water-loop control system. Similar to Classes 1 and 2, Class 3 commands are not required for safety, meaning that no commands are required from the remote operations center in order for the reactor to maintain a safe state. All safety actions are controlled by systems located at the reactor facility, and no action taken from the remote-operation facility can impact reactor safety.

2.4 Class 4: Remote Control of Safety-Significant and Important-to-Safety Systems and Equipment

Class 4 remote operations increase the remote-control functionality to include safety-significant systems and important-to-safety CDAs. For this report, the following NRC definition of “safety significant” is used, where safety significant “... identifies that object as having an impact on safety, whether determined through risk analysis or other means, that exceeds a predetermined significance criterion” [25]. The definition of “important to safety” used in this report originates from NEI 10-04, Rev. 3: “Important to safety equipment is non-safety-related equipment that is used to meet the current licensing basis commitments to assure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition" [13]. The intention in this framework for the use of safety significant and important to safety SSCs is to capture those safety SSCs from the Part 50, 52, and proposed A/SMR framework under Part 50 and 53, that may fall within the scope of the security program to protect, but are not defined as "safety related" and, thus, would not require additional security controls as vital equipment. In contrast to Class 3, which allows remote control of systems with no safety impact, the purpose of Class 4 is to provide remote control to systems that may impact safety, but do not directly impact safety. Commands are permitted to be sent from the remote-operations facility directly to individual actuators and control parameters at the reactor facility of non-safety-related SSCs, as is also the case for Class 3. Class 4 also allows the remote-operations center to send commands directly to individual actuators and control parameters for safety-significant SSCs or important-to-safety CDAs at the reactor facility. An example of a Class 4 function is the remote actuation of the reactivity-control mechanism, such as control rods or drums. Movement of the control rods or drums could be considered a non-safety-significant action if actuation of the rods cannot create a safety incident themselves and are separate from a diverse safety-related reactor-shutdown system. In the case of an electromagnetically clutched control rod, often the safety function is the release of the rod upon a reactor trip signal while the movement of the rod for reactor power manipulation is not a safety function.

2.5 Class 5: Remote Control of Safety-Related Systems and Equipment

Class 5 remote operations represents the class with the greatest remote-control authority and functionality. Class 5 includes the functionality of the prior four classes and adds remote-control functionality for safety-related SSCs. The NRC definition of "safety related" is used in this report: "systems, structures, components, procedures, and controls (of a facility or process) that are relied upon to remain functional during and following design-basis events. Their functionality ensures that key regulatory criteria, such as levels of radioactivity released, are met" [24]. An example of Class 5 remote operation is the ability to remotely control the reactor-protection system or emergency core-cooling system from the remote-operations center.

3 SECURITY CONSIDERATIONS FOR REMOTE OPERATIONS CLASSES

The different classes of remote operation proposed in Chapter 2 require differing amounts of physical- and cybersecurity protections for the remote-operations facility and infrastructure, depending on the amount of control authority the remote-operations facility has over the reactor facility. This section provides a summary of the physical- and cybersecurity requirements that would be applicable to the remote-operations facility and infrastructure based on the 10 CFR Part 50 and Part 52 and proposed 10 CFR Part 53 reactor-licensing frameworks. Providing relevant stakeholders—e.g., A/SMR vendors, suppliers, and researchers with an interest in remote operations—with this information affords informed decision making on what remote-operations framework designs and remote-operations research directions to pursue to ensure sufficient security. Included in each class are the physical-security requirements that are relevant to the remote-operations facilities and infrastructure in that class, as well as the cybersecurity requirements for the remote-operations facility and infrastructure in that respective class.

Prior to introducing the security requirements for each remote-operations class, some discussion regarding cybersecurity of DAs is required. Figure 2 depicts the anticipated types of DAs that fall within each class. In Class 1, the capability exists to remotely monitor all DAs (both CDAs and non-CDAs) at the reactor facility. Because these classes build upon each other, Class 2 includes the capability for monitoring all DAs, as well as the capability to remotely launch allowlisted programs locally on non-CDA DAs. Class 3 includes all Class 2 capabilities, as well as capabilities to remotely control BOP-Trip/SCRAM CDAs, BOP CDAs, and EP CDAs. Further, Class 4 includes all Class 3 capabilities, as well as the capability to remotely control indirect CDAs. Class 5 adds the capability to remotely control security and direct CDAs.

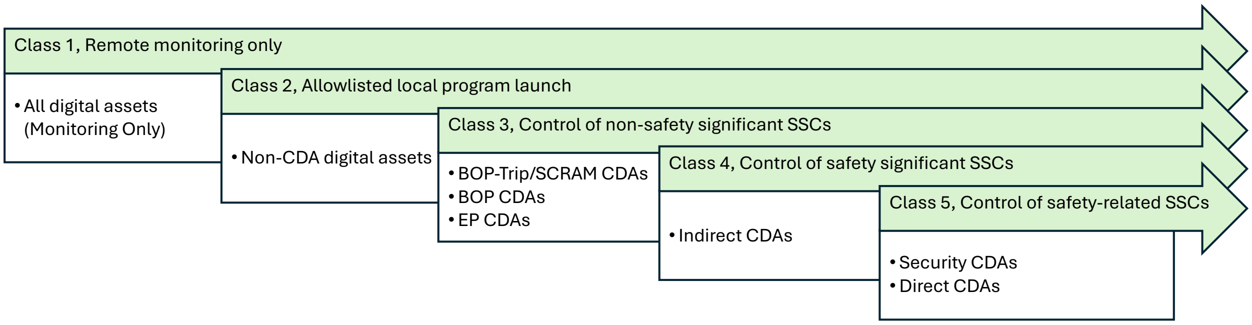
Class 1, Remote monitoring only
• All digital assets (Monitoring Only)
Class 2, Allowlisted local program launch
• Non-CDA digital assets
Class 3, Control of non-safety significant SSCs
• BOP-Trip/SCRAM CDAs
• BOP CDAs
• EP CDAs
Class 4, Control of safety significant SSCs
• Indirect CDAs
Class 5, Control of safety-related SSCs
• Security CDAs
• Direct CDAs

Figure 2. Characterization of each remote activity class for DAs located at a nuclear facility.

When establishing cybersecurity requirements for remote monitoring and operation, there are two contexts to consider with regards to protecting DAs.

1. **Reactor Facility Context: Digital assets located at the reactor facility**

   For power reactors in the U.S., licensees are required to identify SSEP CDAs (see Table 1 for CDA definitions) at the reactor facility as part of their cybersecurity program. Security controls are then applied based upon CDA designation. In the current U.S. regulatory environment, prescriptive requirements and security controls may or may not allow the capabilities of monitoring and/or control at each remote-control class defined in this report. These prescriptive precluding requirements and controls are referenced specifically as applicable within each of the remote-control classes.

2. **Remote Operations Facility Context: Digital assets located at the remote facility**

   Depending on the desired level of remote monitoring and control, it may be necessary to apply security controls not only to the local CDAs at the reactor facility, but also to the DAs located at the remote facility and along the entire digital pathway to ensure regulatory compliance. The application of these security controls may or may not be technically possible and/or acceptable by the regulator.

3.1 Class 1: Remote Monitoring Only

3.1.1 Reactor Operations

Class 1 remote-operations adopt an operations framework in which any operator control action takes place at the local reactor facility while being monitored, through a one-way connection, from a remote facility called the remote-operations center. The reactor facility uses a reactor main control room (MCR) staffed with operators, consistent with the requirements of §50.34, §50.54, and §50.54 (i–m) [3], or §53 (f) [5], which may include generally reactor licensed operators (GLROs) as defined in the proposed Part 53 rulemaking.

The GLRO is a new Class of NRC reactor-operator license proposed in Part 53. GLROs have reduced operations responsibility relative to licensed reactor operators or senior reactor operators. GLROs are only able to operate a reactor designated a self-reliant mitigation facility which requires no human action to maintain its safety basis. As such, GLROs have no role in event mitigation, which is not the case for licensed reactor operators or senior reactor operators. The full definition of a GLRO and self-reliant mitigation facility can be found in Part 53.8 [5].

3.1.2 Physical Protection

The physical protection of the reactor facility is defined by the regulations in Part 73 [6]. For the purposes of this analysis for Classes 1–5 remote operations, it is assumed a licensee will need to comply with the requirements under §73.55 [8] for the protection of power reactors against radiological sabotage, and it is unnecessary to protect against theft, or that alternative physical-security requirements would apply.

3.1.2.1 Reactor Facility

The physical security of the reactor site under Class 1 operations will resemble the security stance of currently licensed commercial-nuclear facilities because the reactor site will need to comply with several prescriptive and performance-based requirements detailed in §73.55 to protect against the design-basis threat of radiological sabotage [8], as described in the subsequent subsections.

Physical-Protection Program

The licensee will be required to prevent a "significant release of radionuclides from any source." Target sets are defined as the SSC combinations that, when all SSCs are prevented from performing or accomplishing their intended safety function, would likely result in a significant release of radionuclides from any source. Target sets are the safety SSCs of a facility that an adversary seeks to destroy to cause a release to the environment. The reactor site would contain target-set SSCs that the physical-protection program would be required to defend against adversary actions. The protection of target-set equipment is accomplished through combinations of prescriptive requirements listed below, and execution of a protective strategy to detect, delay, and neutralize adversarial forces.

Access Authorization

The reactor site shall have an access-authorization program consistent with the requirements of §73.56, to "provide high assurance" that specified individuals "are trustworthy and reliable, such that they do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage." The access-authorization program would be composed of background checks, psychological assessments, behavioral observation, and self-reporting, and apply to at a minimum, from §73.56(b) [26]:

> *(i) Any individual to whom a licensee intends to grant unescorted access to nuclear power plant-protected or vital areas or any individual for whom a licensee or an applicant intends to certify unescorted-access authorization;*
>
> *(ii) Any individual whose duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact the licensee's or applicant's operational safety, security, or EP;*
>
> *(iii) Any individual who has responsibilities for implementing a licensee's or applicant's protective strategy, including, but not limited to, armed security-force officers, alarm-station operators, and tactical-response team leaders; and*
>
> *(iv) The licensee or applicant access-authorization program reviewing official or contractor or vendor access-authorization program reviewers.*

Insider Mitigation Program

The reactor site will need an insider-mitigation program to monitor the trustworthiness of individuals granted access to protected or vital areas and apply defense-in-depth methods to minimize the effects of possible insider actions on the physical-protection program goal of prevention of significant releases of radionuclides.

Physical Barriers

Bullet resisting. The reactor site will need several areas to be bullet-resisting, as specified by regulation, to include the reactor control room, the security central-alarm station, security secondary-alarm station, and the last access-control location for protected-area access.

Protected-area barrier and isolation zone. The reactor site will be encircled by a protected-area (PA) barrier, with an isolation zone immediately adjacent, monitored with intrusion-detection equipment to meet §73.55(i) [8], and designed to limit access to the facility, with all penetrations secured and monitored.

Vital areas. The reactor site will have one or more vital areas (VA)within the protected area, such that entry to each vital area must require passage through two physical barriers. Vital areas include the reactor MCR, used-fuel storage, and security central- and secondary-alarm stations. Vital equipment—defined as any equipment, system, device, or material the failure, destruction, or release of which could directly or indirectly threaten public health and safety by exposing them to radiation, or which is required to function to protect public health and safety after such an event—must be situated within a vital area. In addition, the secondary-power supplies for alarm systems and non-portable communications equipment must be located within a vital area.

Vehicle-control measures. The reactor site will require active and passive vehicle-control measures to prevent the significant release of radionuclides from a possible design-basis threat of radiological sabotage vehicle-borne improvised explosive device (VBIED).

Access Control

The reactor site will require access control for each barrier system to control vehicles, personnel, and materials, as required by regulation and the physical-protection program. Access control will work in concert with the physical-protection, access-authorization, insider-mitigation, and cybersecurity programs and will meet the requirements of the applicable barriers. Access control will also require search programs and escorts, as necessary.

Detection and Assessment Systems

The reactor site will be encircled by an intrusion-detection and assessment system (IDS) to detect an adversary before they breach the PA barrier. IDS equipment will also be placed on unattended security barriers throughout the facility as needed, to include vital areas. The IDS will annunciate and display concurrently in the central- and secondary-alarm stations. Illumination shall be provided where required to support assessment. The alarm hardware, including transmission lines, are tamper indicating, and both alarm stations cannot be disabled with a single act. Security patrols will conduct surveillance and monitor barriers, IDS equipment, and vital areas, and make random patrols of locations that contain target-set equipment to identify indications of tampering.

Communication

The reactor site will require communication between the on-duty security personnel, command-and-control personnel, the alarm stations, and offsite-response organizations. The alarm stations must have continuous radio or microwave communications and two-way telephone communication with local law enforcement, and a system for communication with the MCR.

Personnel

The reactor site must have sufficient staff to satisfy the physical-protection program requirements and protective-strategy goals, with a minimum of ten armed responders available to act, within the protected area at all times.

3.1.2.2 Remote-Operations Facility

The postulated remote-operations facility that receives information only for monitoring purposes would not need to meet physical-protection system requirements as defined by the NRC. The remote-monitoring facility may choose to enact corporate security protocols for the protection of employees and company data. The exception would be if the remote-monitoring facility collected facility information that was considered safeguards information, as defined by §73.1 and regulated by §73.21 and §73.22 [6], or classified information, as regulated under 10 CFR Part 95 [27].

3.1.3 Cybersecurity

Class 1 "monitoring only" of all DAs at a nuclear facility should be possible at a remote facility from a regulatory cybersecurity perspective if certain secure architecture requirements are met. Notably, the use of data diodes or other one-way deterministic devices would be necessary for certain nuclear facility assets to ensure that information flow is only out of the nuclear facility to the remote facility. From a U.S. regulatory perspective (e.g., §73.54), DAs at the reactor facility may not require data diodes to send data from non-CDA DAs to the remote facility; however, they are considered best practice. For the remote-operations facility context, the DAs used at the remote-operations facility to acquire, transform, and/or display information for monitoring purposes should be classified as non-CDAs. Notably, there is precedence for this class of remote operations. For example, it is currently common practice in the U.S. nuclear industry to send information from security CDAs to corporate-level security operation centers for remote monitoring.

Cybersecurity objectives typically include the protection of confidentiality (e.g., privacy of sensitive information), integrity (e.g., accurate and complete information), and availability (e.g., no disruption in system or functions). In operational technology (OT) at nuclear facilities, the protection of integrity and availability are generally considered more important than the protection of confidentiality as it is more important to ensure continued operation with accurate and truthful information. In Class 1, the protection of integrity and availability will still be maintained at the reactor facility, but the protection of confidentiality may be more difficult along the information pathway (i.e., remote-operations facility and infrastructure).

3.2 Class 2: Remote Allowlisted Commands

3.2.1 Reactor Operations

Class 2 remote operations support monitoring and include the ability to send allowlisted commands from a remote-operations facility to the reactor facility. The reactor facility uses a reactor control room staffed with licensed operators, consistent with the requirements of §50.34, §50.54, and §50.54 (i–m) [3], or Part 53 Subpart F [5], which may include GLROs. A separate remote-operations facility exists that has the capability to send allowlisted commands to the reactor facility. The allowlisted commands are considered disconnected and segmented from the reactor-protection system to prevent non-allowlisted commands from being received by the safety systems. The reactor operations for this class may fall into two general concepts.

3.2.1.1 Remote Facility with Non-Licensed Operators

The concept of operation will have licensed reactor operators at the reactor facility in the designated MCR, which may include required operator actions to permit the allowlisted commands to be executed, similar to current in-plant operator supervision and permission of non-licensed operator (NLO) actions under §50.54(j) [3]. NLOs at the remote-operations facility have the capability to send allowlisted commands to the reactor facility, which would be executed by permission and under the supervision of licensed operators in the reactor-facility MCR.

The NLO is a licensee-defined position, trained in accordance with the requirements of §50.120 [3], and authorized in accordance with the site license to carry out duties, to include licensed operator permitted and supervised reactivity manipulations.

3.2.1.2 Remote Facility with Generally Licensed Reactor Operators

If this postulated reactor facility uses a high degree of automation and meets the requirements of a self-reliant mitigation facility, as defined in Part 53.8 [5], and the remote facility plays no role in the safety of the reactor aside from offsite response, the MCR may be located at the remote-operations facility, and GLROs may be used in the MCR, pursuant to Part 53, Subpart F [5].

3.2.2 Physical Protection

The physical protection of a commercial reactor with remote operation will depend on the possible actions that can be executed from the remote location. The allowlisted commands for this class are assumed to have no possible impact on the safety of the reactor. This would define the applicable physical-security requirements.

3.2.2.1 Reactor Facility

The reactor facility that receives allowlisted commands would not have requirements applied different from a traditional reactor's physical-security program, as detailed in Section 3.1.2.1. The reactor facility would still contain the safety equipment required to be protected. The facility may choose to apply greater security controls on the SSCs that receive the signals from the remote facility to address security threats from external adversaries or insiders.

3.2.2.2 Remote-Operations Facility

3.2.2.3 Remote Facility with Non-Licensed Operators

This concept-of-operation description is predicated on the inability to compromise the allowlist command system to impact the reactor safety. Therefore, the SSCs associated with the remote-operations facility would not be required to be protected under §73.55 [8], unless required to under the cybersecurity program. The NLOs, by the nature of their employment and responsibilities, may be required by the licensee to fall under the access-authorization and insider-mitigation programs.

3.2.2.4 Remote Facility with Generally Licensed Reactor Operators

A remote-operations facility that employs GLROs would be designated the MCR for the licensed reactor facility for this concept of operation. Though the remote control room may not play a meaningful role in the safety of the reactor, several security requirements are applied to the oversight, defense-in-depth, access, and communication functionalities of the control room, including protection as a vital area. Table 3 summarize the applicability of physical security elements to the remote facility.

Table 3. Physical Security of a Class 2 Remote Operations Facility with GLROs.

Physical Protection System Element	Applicability to Remote Operations Facility—Class 2 Remote Operation
Physical Protection	None required, no defined target sets at the remote facility.
Access Authorization	Yes, for personnel with access to the protected area and vital areas at remote facility.
Insider Mitigation	Yes, for personnel with access to the vital areas at remote facility.
Physical Barriers	Bullet resisting: Yes, for access control point, MCR, and central alarm station/secondary alarm station. Protected Area: Yes, as MCR is a VA. Vital Areas: Yes, at minimum MCR is a VA. Vehicle control measures: Yes, as required for PA (but not VBIED).
Access Control	Yes, as required by the PA and VAs.
Detection and Assessment	Yes, as required by the PA and VAs.
Communication	Yes, between the remote facility and central alarm station/secondary alarm station. If the central alarm station or secondary alarm station is located at the remote facility, communication will also need to be established between the remote facility and response forces at the reactor site.
Personnel	Yes, access-control security personnel will be required at the remote facility.

3.2.3 Cybersecurity

Remote-operations Class 2 provides the ability to launch allowlist programs or commands at the reactor facility from the remote-operations center. This is considered feasible from a U.S. regulatory perspective (e.g., 10 CFR 73.54) for non-critical DAs located at the reactor facility. Because these activities are performed on non-critical DAs, the information pathway and the DAs used to send the "launch" signal at the remote-operation facility will also not be CDAs.

It is important to note that the logical pathway is considered when identifying whether a DA is a CDA. For instance, a DA connected to a CDA along a logical pathway could be an attack pathway for an adversary; thus, that DA must be protected commensurate with the connected CDA. Therefore, it is important to ensure that any flow path to the local asset at the nuclear facility does not extend beyond it. The local asset receiving the launch signal must be segmented or segregated from the remainder of the OT architecture using defense-in-depth and security controls, such as secure architecture design and boundary devices, to ensure that an adversary cannot pivot to another system or DA.

Because this launch signal flows from the remote facility to the nuclear facility, there is a potential for disruption or compromise of this signal along the pathway. Based on the design of the allowlist functionality, adversarial or non-adversarial action could either start or stop the local program when not intended (i.e., an integrity attack) or delay or prevent the signal from reaching the local device, causing the program to start or stop too late or out of sequence (i.e., an availability attack). However, because a requirement of this class is that the local program is bounded by rigorous design on a non-critical DA and function, any maloperation should not result in an adverse impact to a CDA or an SSEP function.

3.3 Class 3: Remote Control of Non-Safety-Significant, Not Important to Safety, or Non-Safety-Related Systems and Equipment

3.3.1 Reactor Operations

Class 3 remote operations expand the remote-control functions to include remote control of non-safety-related and non-safety-significant SSCs, and non-safety CDAs (e.g., BOP-Trip/SCRAM, BOP, or

EP CDAs) in addition to allowlisted commands and remote monitoring. The reactor facility employs a reactor control room local to the reactor and staffed with operators, consistent with the requirements of §50.34, §50.54, and §50.54 (i–m) [3], or Part 53 Subpart F [5] which may include GLROs. Additionally, a separate remote-operations facility can transmit allowlisted commands as well as manipulate non-safety-related, non-safety-significant equipment, non-safety CDAs, and non-critical DAs.

3.3.1.1 Remote Facility with Licensed Operators and No Target Elements

The concept of operation will have licensed reactor operators at the reactor facility in the designated MCR, and licensed reactor operators at the remote-operations facility with the capability to control non-safety-significant SSCs and transmit allowlisted commands to the reactor facility with no possibility to contribute to radiological sabotage.

3.3.1.2 Remote Facility with Generally Licensed Reactor Operators

If this postulated reactor facility uses a high degree of automation and meets the requirements of a self-reliant mitigation facility, as defined in Part 53.8 [5], and the remote facility plays no potential role in the safety of the reactor aside from offsite response, the MCR may be located at the remote-operations facility, and GLROs may be used in the MCR, pursuant to Part 53, Subpart F [5].

3.3.1.3 Remote Facility with Licensed Operators and Target Elements

The SSCs, controlled by licensed operators, as designed or as compromised by an adversary in the remote-operations facility, have the potential to contribute to radiological sabotage and would be defined as target elements.

3.3.2 Physical Protection

The physical protection of a commercial reactor with remote operation will depend on the possible actions that can be executed from the remote location. The allowlisted commands for this class are assumed to have no possible impact on the safety of the reactor, and the remote-operations facility would only have control of non-significant systems. This would define the applicable physical-security requirements.

3.3.2.1 Reactor Facility

The reactor facility that receives allowlisted commands or manipulation of non-safety-significant SSCs has no different or additional requirements beyond a traditional reactor's physical-security program, as detailed in Section 3.1.2.1. The reactor facility would still contain the safety equipment required to be protected. The facility may choose to apply greater security controls on the SSCs that receive the signals from the remote facility to address security threats from external adversaries or insiders.

3.3.2.2 Remote Operations Facility

Remote Facility with Licensed Operators and No Target Elements

Class 2 remote operations ensure any compromise to the allowlist-command system will not impact reactor safety. Similarly, Class 3 allows control of non-safety-significant systems from the remote facility may not have an impact on reactor-facility safety and will not qualify as target elements. Thus, the SSCs associated with the remote facility require no specific physical protections under §73.55, unless by the cybersecurity program. The licensed operators, by the nature of their employment and responsibilities, may be required by the licensee to fall under the access-authorization and insider-mitigation programs.

Remote Facility with Generally Licensed Reactor Operators

A remote-operations facility that employs GLROs would be designated the MCR for the licensed reactor facility for this concept of operation. This physical security requirements would be similar to that described in 3.2.2.2 for reactor facilities with GLROs.

~~Remote Facility with Licensed Operators and Target Elements~~

~~A remote operation facility that has licensed operators that can directly control safety-related equipment would have requirements applied similar to a traditional reactor physical-security program, as detailed in Section 3.1.2.1. The remote facility would contain SSCs that qualify as target elements; thus, the physical-protection program must consider the protection of target-set elements, including the necessary instrumentation-and-control transmission equipment between the remote facility and reactor systems. Target-set equipment not located within a protected area must be documented and considered within the protective strategy, as required by §73.55(f)(3).~~

3.3.3 Cybersecurity

Class 3 remote operations provides for the ability to control non-safety-significant CDAs, which include BOP-Trip/scram CDAs, BOP CDAs, and EP CDAs at the reactor facility. Starting at Class 3 and higher, operational control of any CDA at the reactor facility will require commensurate protection of the DA used for the operation at the remote-operations facility. Cybersecurity requirements include protection of the logical pathway (the communication path), regardless of the type (e.g., hardwired, wireless) and topology (e.g., point-to-point, hybrid, cloud-based) of the pathway. This DA would likely also be classified as a non-safety-significant CDA.

Because a cybersecurity incident could result in loss of integrity and/or availability of digital systems and assets at the reactor facility and/or the remote-operations facility, leading to adverse impact to BOP or EP functions, administrative, technical, and physical-security controls are needed to provide reasonable assurance that a cyberattack will not adversely impact these functions. However, because the required controls may be less burdensome than protecting security, indirect, or direct CDAs, it may be possible to implement an acceptable solution to meet current U.S. regulatory requirements in §73.54. For example, NEI 13-10, Rev. 7, which is acceptable for use by the NRC, allows for different treatment of low-consequence CDAs, such as BOP and EP CDAs when compared to high consequence CDAs [12]. One method could be to implement allowlists for these functions (as described in Class 2) to limit the potential impacts of a compromise. This design would require significant evaluation to determine whether it is allowable under a licensee's cybersecurity plan.

3.4 Class 4: Remote Control of Safety-Significant Systems

3.4.1 Reactor Operations

Class 4 remote operations adds the capability to remote control safety-significant/important-to-safety SSCs and CDAs from the remote-operations facility. The reactor facility may employ a reactor control room local to the reactor and staffed with operators, consistent with the requirements of §50.34, §50.54, and §50.54 (i–m) [3], or Part 53, Subpart F [5] which may include GLROs. Additionally, a separate remote-operations facility can transmit allowlisted commands, as well as manipulate non-safety-related but safety-significant equipment and important-to-safety CDAs. The role of operators at the remote facility in the safety of the reactor precludes the use of GLROs.

3.4.1.1 Remote Facility with Licensed Operators and No Target Elements

The concept of operation will have licensed reactor operators at the remote-operations facility (which may be the designated MCR) with the capability to control safety-significant SSCs and transmit allowlisted commands to the reactor facility, but with no possibility of contributing to radiological sabotage. As such, there are no target elements located at the remote operations facility.

3.4.1.2 Remote Facility with Licensed Operators and Target Elements

The SSCs in the remote-operations facility, controlled by licensed operators, have the potential to contribute to radiological sabotage and would be defined as target elements. This postulated remote facility is not anticipated to be required to protect public health and safety and would not contain vital equipment or have designated vital areas.

3.4.2 Physical Protection

3.4.2.1 Reactor Facility

The reactor facility that receives allowlisted commands or manipulation of safety-significant SSCs would not have different requirements applied than a traditional reactor physical-security program, as detailed in Section 3.1.2.1. The reactor facility would still contain the safety equipment required to be protected. The facility may choose to apply greater security controls on the SSCs that receive the signals from the remote facility to address security threats from external adversaries or insiders.

3.4.2.2 Remote Control Facility

Remote Facility with Licensed Operators and No Target Elements

Class 2 remote operations are described in this report as not having the ability to compromise the allowlist command system to impact the reactor safety. Similarly, Class 3 control of non-safety-significant systems from the remote facility may not have the possibility of impacting the reactor-facility safety and may not qualify as target elements. This class, Class 4, adds the ability to control safety-significant SSCs, but if these SSCs cannot contribute to radiological sabotage, the SSCs would not be designated as target elements. Thus, the SSCs associated with the remote facility would not be required to be protected under §73.55, unless by the cybersecurity program. The licensed operators, by the nature of their employment and responsibilities, may be required by the licensee to fall under the access-authorization and insider-mitigation program. If the MCR is located in the remote facility, it will be designated a vital area and would be required to be located within a protected area, and this would require the necessary physical-security hardware and programs associated with vital and protected areas.

Remote Facility with Licensed Operators and Target Elements

A remote operation facility that has licensed operators that can directly control safety-significant equipment would have requirements applied similar to a traditional reactor physical-security program, as detailed in Section 3.1.2.1. The remote facility would contain SSCs that qualify as target elements; thus, the physical-protection program must consider the protection of target-set elements, including the necessary I&C transmission equipment between the remote facility and reactor systems. Target-set equipment not located within a protected area must be documented and considered within the protective strategy, as required by §73.55(f)(3).

3.4.3 Cybersecurity

Remote operations Class 4 allows the remote-operations center to remotely control and operate important-to-safety indirect CDAs. However, it will likely be more difficult to meet current U.S. cybersecurity regulatory requirements in §73.54. Not only are the reactor-facility indirect CDAs protected to a higher degree, but the pathway and DAs at the remote-operations facility will also be considered indirect CDAs, requiring additional security measures at the remote facility and the pathway between the remote-operations facility and the reactor facility.

However, similar to Class 3, it may be possible to reduce the required security controls by using allowlists to control these CDAs. For example, consider the desire for remote load-following operation of a pressurized water reactor (PWR). Reactor power is adjusted in a PWR by raising or lowering regulating control rods using the control-rod drive system. This system, and the SSCs required to perform this function in the system, are typically identified as non-safety related. However, the DAs that perform the function may be classified as safety-significant or indirect CDAs because they impact reactivity. Developing and implementing allowlists to raise or lower power based on predefined settings (as described in Class 2) may reduce the need to classify the pathway and DAs at the remote facility as indirect CDAs. Care must be taken to evaluate whether this is acceptable under a licensee's cybersecurity program. (NOTE: The safety-related function for control rods in a PWR is the reactor-trip function, in which power is removed from the control-rod breakers, resulting in control rods' dropping into the reactor core. Aside from the rods themselves, the SSCs in the reactor-trip system and control-rod-drive system are separate and classified independently.)

3.5 Class 5: Remote Control of Safety-Related Systems

3.5.1 Reactor Operations

Class 5 remote operations provide the remote control of all SSCs at the reactor facility, including safety-related and safety-significant SSCs and all CDAs. This implementation may look similar to the remote shutdown panel at existing plants, except the functionality is provided at the remote-operations center. The reactor facility may or may not employ a reactor control room local to the reactor and staffed with operators, consistent with the requirements of §50.34, §50.54, and §50.54 (i–m) [3], or §50.53 (f) [5], which may include GLROs. Additionally, a separate remote-operations facility can transmit allowlisted commands as well as manipulate safety-related and safety-significant equipment and all CDAs. The role of operators at the remote facility in the safety of the reactor precludes the use of GLROs.

The concept of operation will have licensed reactor operators at the remote-operations facility with the capability to control safety-related and safety-significant SSCs and transmit allowlisted commands to the reactor facility with the same capabilities of a control room located at the reactor facility and may or may not have licensed reactor operators at the reactor facility. The designated MCR may be located at either the reactor facility or the remote-operations facility. The SSCs in the remote-operations facility, controlled by licensed operators, have the potential to contribute to radiological sabotage and would be defined as a target element. The remote-facility control room and associated infrastructure for the transmission of safety-related I&C would qualify as vital equipment.

3.5.2 Physical Protection

3.5.2.1 Reactor Facility

The reactor facility that receives allowlisted commands or manipulation of safety-related SSCs would not have applied requirements different from a traditional reactor physical-security program, as detailed in Section 3.1.2.1, unless the reactor facility does not possess the MCR. The reactor facility would still contain the safety equipment required to be protected. The facility may choose to apply greater security controls on the SSCs that receive the signals from the remote facility to address security threats from external adversaries or insiders.

3.5.2.2 Remote-Control Facility

A remote operation facility that has licensed operators that can directly control safety-related equipment would have requirements applied similar to a traditional reactor physical-security program, as detailed in Section 3.1.2.1. The remote facility would contain SSCs that qualify as target elements; thus, the physical-protection program must consider the protection of target-set elements, including the necessary I&C transmission equipment between the remote facility and reactor systems. Target-set equipment not located within a protected area must be documented and considered within the protective strategy, as required by §73.55(f)(3). The physical-protection program would also need to protect the remote control room, and the necessary support and transmission SSCs, as vital equipment and locate them within a designated vital area.

3.5.3 Cybersecurity

Within a cybersecurity context, Class 5 remote operations provide the ability to remotely control and operate security and direct CDAs from the remote-operation facility. This level of access is difficult, if not impossible to achieve under the current U.S. cybersecurity regulatory requirements in §73.54.

Similarly to Class 4, not only are the reactor-facility CDAs classified at the highest-protection rating, but the pathway and DAs at the remote-operations facility will also be considered direct CDAs; therefore, they require the same level of protection. From a physical security-controls standpoint, requirements could extend beyond the need for locked cabinets and locked doors to the need for a defined protected or vital area, which generally requires additional physical-security protections and a security-response force. As a result, it is unlikely that an A/SMR would adopt a remote-operating paradigm at Class 5 due to the large risk and high cost of protection and cybersecurity controls.

4 IMPLEMENTATION PATHWAYS FOR REMOTE OPERATIONS

Chapter 2 provided a framework for characterizing remote operations of nuclear power plants based on the controllable functions and amount of access to SSCs at the reactor facility from the remote-operations facility. However, some of proposed classes are impractical to implement, nor is there an industry desire for remote operations of more critical classes. This chapter will provide context into which classes of remote operation may be possible to implement both from a physical- and cybersecurity perspective, as well as examples of network architectures that could be used to implement remote operations within certain classes.

Chapter 2 proposed five classes of remote operation for nuclear reactors based upon the amount of remote access to plant functions and systems while Chapter 3 outlined the physical- and cybersecurity considerations that would apply at each class of remote operation. What was not provided was any analysis as to the practicality of implementing each class of remote operation. This chapter provides an assessment of the practicality of implementing each proposed class based upon the requirement assessment provided for each class in Chapter 3. A summary of these findings is provided in Table 4. In short, three of the five proposed remote-operation classes may have a practical path forward to implementation under the U.S. regulatory framework. Class 1 remote operations are currently in use in the U.S. while Classes 2 and 3 remote operations may be logistically possible to implement under the U.S. regulatory framework. The final two classes, 4 and 5, would likely be logistically difficult, if not infeasible to implement within the current U.S. physical- and cybersecurity regulatory framework.

Table 4. Implementation practicality of each class of remote operations.

Remote Operation Class	Currently Implemented	Practical to Implement	Infeasible to Implement
1: Remote Monitoring	X	X	
2: Allowlist Control		X	
3: Non-Safety Control		X	
4: Safety-Significant and Important-to-Safety Control			X
5: Safety-Related Control			X

4.1 Remote-Operation Implementation Background Information

4.1.1 Defensive Computer Security-Architecture Framework

The example remote operation architectures in the following sections are adapted from the IAEA's example of a defensive computer security architecture (DCSA). As shown in Figure 3, IAEA Nuclear Security Series No. 17-T Revision 1 provides an example DCSA that incorporates security levels and zones to segregate and isolate systems based on the significance of critical functions and system interaction requirements [16]. Critical functions requiring the greatest security (e.g., reactor protection system) would typically be located in the most-stringent security level (e.g., Security Level 1). Within a security level, the complexity of security zones may be correlated based on physical location and logical size. Between each security level and zone, boundary devices (e.g., data diode, firewall, antivirus scanner, malware detection, etc.) are used to monitor and restrict communication flow, which makes lateral movement and pivoting between systems more difficult for an adversary. Typically, a unidirectional, deterministic boundary device, such as a data diode, is used to limit digital-information flow to one direction to protect critical functions (e.g., only one-way authorized communication is allowed from Security Level 1 to Security Level 2). Data diodes are useful throughout the DCSA wherever it is optimal from a security standpoint to limit bi-directional digital information flow. This may be between levels or between zones.

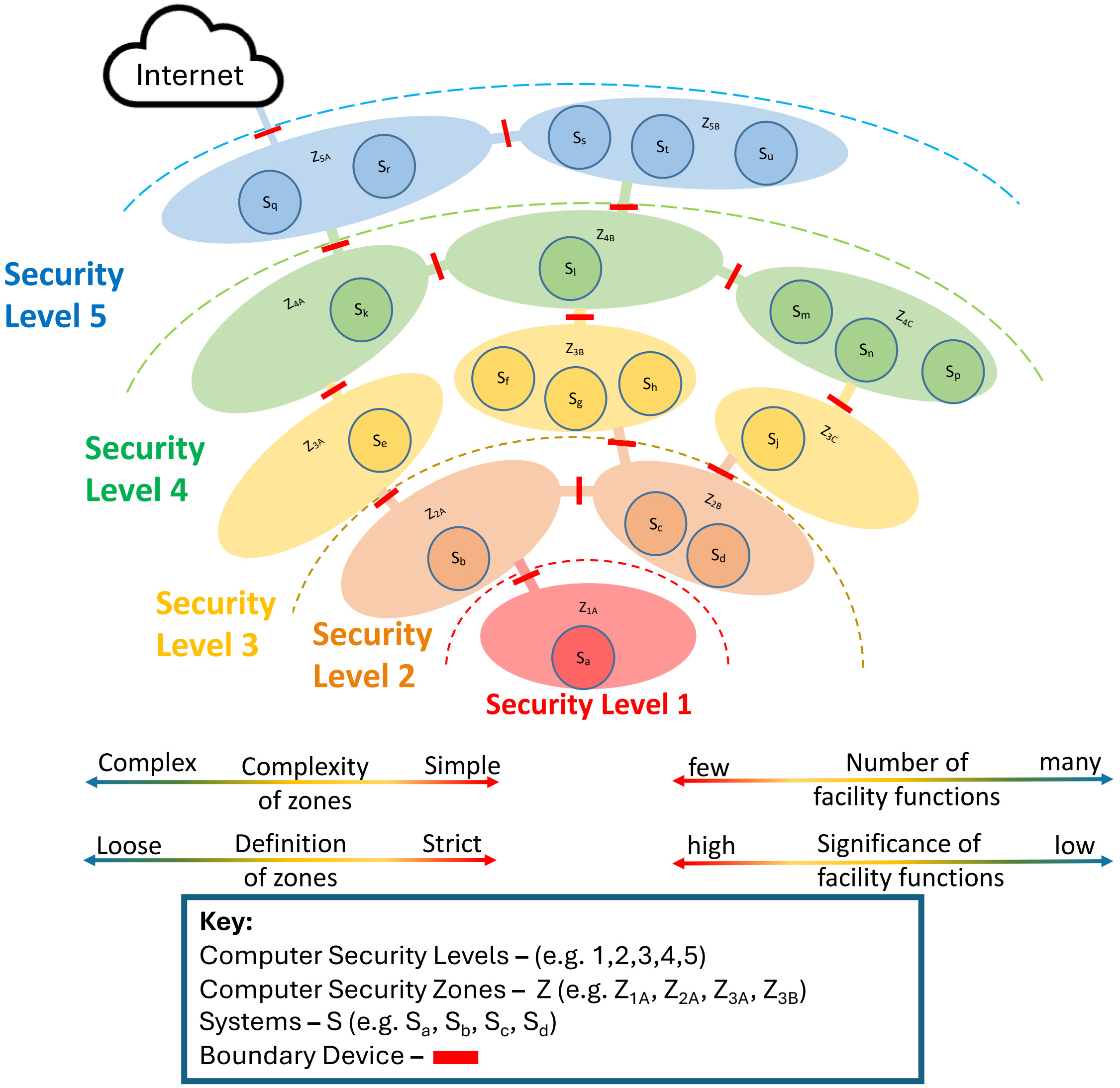

Figure 3. Example of a DCSA [16].

For the context of this document and the following remote-operation architecture examples, Table 5 provides an example mapping of common plant systems to Security Levels 1–5, as shown in Figure 3. Security Level 1 will typically contain digital safety-related SSCs—such as a reactor protection system, engineered-safety-features actuation system, and decay-heat system—that could lead to radiological consequences if compromised. Security Level 2 will typically contain digital SSCs that are classified as physical protection, emergency response, and important to safety DAs, including those related to reactivity control. Security Level 3 will typically contain digital SSCs that will not lead to radiological or physical protection consequences if compromised, but that may have an impact on plant operation. In this paper, Security Level 4 is designated as the local area network at the NPP that is used for business computing, and Security Level 5 is designated as the wide area network for the larger organization that extends externally from the NPP to other corporate locations. In this example, DAs that are not defined as CDAs are located in Security Level 3 but they are not required to have the same robustness in security controls that are required for Security Level 3 CDAs. Note that this notional hierarchy is for example purposes only; the DCSA for a reactor facility will be much more complex and may follow a different security level scheme.

Table 5. Example mapping of security levels to functions and systems.

Security Level	**Systems**
5	Corporate Network
4	Facility Business Network
3	Non-Safety SSCs and CDAs
2	Safety-Significant and Important-to-Safety SSCs and CDAs
1	Safety-Related SSCs

4.1.2 Secure Remote Connections

Not covered yet in this report is how secure remote connections are made between two geographically distinct facilities—in the context of this report, a reactor facility and a remote operations center. Before providing implementation examples of the proposed classes of remote operations for nuclear reactors, this section provides a baseline of knowledge of how secure remote connections for OT systems are made for those readers not familiar with this topic [28]. While not an exhaustive review of all possible methods, two common implementations of a secure remote connection are provided.

Site-to- Site Virtual Private Network over Public Network

A virtual private network (VPN) is a conventional approach for establishing remote access. A VPN creates a private tunnel through public networks to provide a secure connection between authorized endpoints. The Client-to-Server model uses a VPN server housed at a static location that continuously listens for connections from authorized personnel who are moving around at different remote locations. Authorized users access the VPN server using unique credentials such as a password and multi-factor authentication (MFA). This is a common approach used for providing access to corporate networks for individuals who are travelling or teleworking so that they can connect back to work at the office as if they were physically present. However, for the proposed applications of remote operations for nuclear reactors, a Client-to-Server VPN does not provide the strategy desired for the remote access objective. Since the proposed implementations of remote operation limit remote access to the reactor facility from only the remote operations center and no other locations, a different VPN approach should be considered, specifically the more restrictive, Site-to-Site VPN.

A Site-to-Site VPN creates a private connection between two static locations with network traffic still traversing the Internet. Unlike the Client-to-Server VPN implementation, neither end of the connection represents an individual user. Instead, Site-to-Site VPNs are restricted to communication only between specific endpoints, with authentication occurring between the two endpoints instead of an authorized user and an end point. Since a Site-to-Site VPN does not provide a mechanism for access to the VPN from anywhere other than the two static endpoints, it significantly reduces the risk of unauthorized entry to the VPN when compared to the Client-to-Server model.

While there are different protocol choices for implementing a Site-to-Site VPN, IPsec is a common and robust choice [29]. IPsec is a protocol that is standardized and fully supported on enterprise grade equipment. Endpoint devices of a Site-to-Site VPN (e.g., workstations) do not require special software to utilize the link. IPsec enables firewall rules, access control lists, and network segmentation to be natively implemented by network architects. Because IPsec is supported as a standard, its deployment is broadly adopted across vendors enabling cross platform support.

A well-secured Site-to-Site VPN solution should also be paired with the following defense-in-depth measures:

- Access Control and Allowlisting
  - The VPN is restricted to the specific IP address of each terminating side
  - Internal networks are limited to specific workstations and jump servers
- Security Certificates
  - Certificates ensure the link only authenticates to the correct device
  - Identity of the terminating sides is verified, not just by IP or a passphrase
  - An expiration date is issued to ensure certificates are renewed
- Logging and Monitoring
  - IDSs and intrusion-prevention systems (IPSs) are deployed to monitor all traffic
  - Logs are collected and sent to a security incident and event monitoring SIEM system
- Compliance
  - Well accepted standards, such as Nation Institute of Standards and Technology (NIST) SP 800-series, are followed.

A Site-to-Site VPN is a solution for providing a secure connection between two remote facilities when it is deployed using a secure protocol such as IPsec layered with the additional security measures listed above to provide a defense in depth.

Private Carrier Circuit

Service providers can offer privately dedicated circuits to link two remote locations. These paths do not have physical connection to the Internet. The circuit is an dedicated, offline, physical link that is established for use only by the customer. A protocol often used for this service is Multiprotocol Label Switching (MPLS) [30, 31]. MPLS is typically outsourced, managed by service providers who provide dedicated lines to the customer and guarantee network performance, quality, and availability. Because MPLS is essentially a private network, it is considered reliable and secure but is also expensive. If a service provider has available infrastructure available between two remote locations (e.g., the remote operations center and the reactor facility), MPLS is an alternative option to a Site-to-Site VPN for providing a secure remote connection between them. Inherent to MPLS is privacy because the connection avoids the use of public Internet; the pathway occurs over private circuits, thereby isolating traffic from external from external threats. In addition, as MPLS provides a dedicated pathway between endpoints, guaranteed bandwidth with low latency can be provided.

Even though an MPLS link is considered private and isolated, network administrators can still choose to encrypt the data over the link, similar to a Site-to-Site VPN over a public network. In addition, the same defense-in-depth measures identified previously for Site-to-Site VPN, such as IDS/IPS and logging via a SIEM, can be implemented in conjunction with MPLS to further protect the connection. Routing is also available, with native support for each local area network (LAN) at either side. All firewalls and routers that belong in the LAN can avoid interfering with the MPLS link.

4.2 Class 1: Remote Monitoring Only

Remote monitoring only is possible under current physical- and cybersecurity requirements. Based on the assessment conducted in Chapter 3, a remote operations center that receives information only for monitoring purposes would not need to meet physical-protection system requirements as defined by the NRC in §73.55. Because there is no connection or pathway to any CDAs at the reactor facility from the remote-operation center, the remote-operations center and pathway (i.e. communication infrastructure) would not be a cybersecurity program under §73.54. Both statements are based on two assumptions: (1) no remote control functionality or response requirements are in place for the remote-operation center, and (2) reactor-facility data are sent to the remote-operations center using one-way outbound communication accomplished through unidirectional boundary devices: e.g., data diodes.

In fact, remote monitoring is currently permissible and is implemented under the U.S. regulatory framework. Remote monitoring is in use and widely deployed across the U.S. reactor fleet. Examples include the NRC ERDS for monitoring under emergency conditions [22] or third-party remote monitoring of plant performance from a central location [32]. Because remote monitoring is already a mature technology within the U.S. nuclear industry and is widely implemented, implementation architecture will not be discussed for remote monitoring in this chapter.

4.3 Class 2: Remote Allowlisted Control

Class 2 remote allowlisted control, which introduces limited reactor-facility control capability from the remote-operations center in the form of allowlisted commands, may have a path forward to implementation from a U.S. physical- and cybersecurity requirements perspective as *conceptually* allowlisted operations have no impact on reactor safety. However, this is extremely dependent on the implementation of such a concept. From a physical-security perspective, because no functions taken at the remote-operations center can impact the reactor safety, no systems at the remote-operation center would qualify as target elements. Therefore, the remote-operations center would not be required to be physically protected under §73.55. From a cybersecurity perspective, if the "launch" signal from the allowlisted command is performed on a non-critical digital asset at the reactor facility, the information pathway (e.g., communication network) and the DAs used to send the launch signal at the remote-operations center would not be considered CDAs and not be subject to the cybersecurity program under §73.54. Both statements are made assuming: (1) no response requirements from the remote operation center, and (2) the reactor facility is restricted to executing predefined, safe, verified, and validated local control programs upon receipt of a command from the remote-operations center. Section 4.3.1 provides an in-depth example of a potential implementation of Class 2 remote operations.

Allowlists are a security control measure that only permits known and approved entities to access or run on a system. As defined formally by the NIST, "an allowlist is a list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline" [33]. Only applications, connections, actions, etc. that are verified, validated, and approved can be executed on the protected system. The most-familiar implementation of the practice to a reader may be in the information technology (IT) system context, where allowlisting can refer to limiting the programs that a user can install on a device without administrator approval, limiting devices allowed on the corporate network to only known devices, limiting the visibility of devices on the corporate network to specifically defined devices, or limiting email to known and approved senders.

In the OT context, allowlisting can appear in several different forms. One method is limiting the applications or specific files installed on controller hardware, such as programable logic controllers (PLCs), to only known and approved versions. Another approach involves limiting the actions that can be taken by an operator to a per user basis. A last example is limiting the visibility amongst components in the OT network to only specific, approved devices, and not all devices on a network.

The proposed application of allowlisting for the remote operation of A/SMRs restricts the remote-control actions that can be applied to the reactor to a predefined set as shown in Figure 4. This restriction is enforced through system design, software enforcement, hardware enforcement, or some combination of all. This report presents an example implementation of allowlists for nuclear remote operations that uses the system-design and hardware-enforcement approaches to limit the commands that the reactor facility can accept to a deterministic set. This approach ensures that there is no pathway for adversarial access to the reactor-facility systems through the remote-operation infrastructure. This example implementation is not meant to be prescriptive in terms of how allowlisted remote operations should be done; instead, it is intended to be informative to stakeholders on how allowlisting could potentially be applied in order to inform their system design.

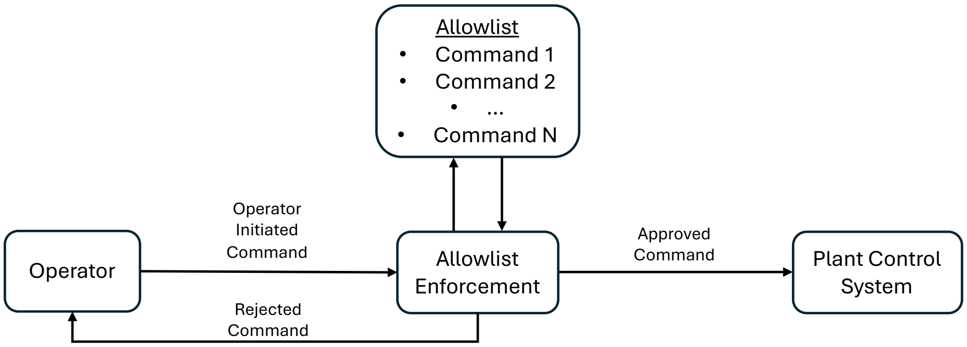

Figure 4. Allowlisted command structure basic information flow.

4.3.1 Remote Allowlist Control Implementation

The design intent of an allowlisted command implementation is to restrict the remote-operations center's control capabilities to a specific set of approved control actions or programs that can be executed at the reactor facility. Meeting this design intent requires two conditions for successful implementation. The first requires that the interaction between the remote-operations center and the reactor facility is limited to executing approved control actions or programs only. The remote-operations center shall have no ability to perform any unapproved functions at the reactor facility, and the remote-operations center shall have no access to reactor-facility systems that are not part of the allowlist-command execution system. The second condition for successful implementation of an allowlisted control structure is that the approved control actions or programs that can be commanded remotely have undergone verification and validation to ensure that no unsafe plant state can be reached by the execution of any allowlisted control action or program. Section 4.3.1.1 provides an example implementation of an allowlisted control architecture that meets both conditions.

4.3.1.1 Example Implementation

The first condition of an allowlist-command implementation that would allow the sending of a command from a remote-operations center to a reactor facility is that any compromise of the remote control infrastructure should not provide a pathway to access the reactor-facility SSCs. Guidance, such as IAEA NSS 17-T, often suggests that the flow of information should only take place from a higher security level to a lower security level [19]. However, in the context of remote operations, there may be use cases where it is desired to send information or commands from a lower security level to a higher one. A potential means of accomplishing this without introducing a digital-communication pathway is by taking an approach analogous to the Westinghouse AP1000's control system, sending commands from its non-safety plant-control system to safety-related components [34]. This example is provided because it details a regulatorily approved, built, and operational example of a lower-security-level system providing commands to a higher security level in a nuclear plant. This is analogous to the task required of a reactor remote-operations system from which commands need to be issued from a lower-security-level system, the remote-operations center, to a higher-security-level system, the reactor facility.

In the AP1000 system, the non-safety control system provides commands to safety-system components via discrete outputs that pass through fiber-optical electrical isolation to input/output (I/O) on the safety system. In this case, the command is a binary on/off signal (like the on/off of a light switch) that passes from a dedicated output on the non-safety system to a dedicated input on the safety system corresponding to one specific safety-system function. Once received, the non-safety command must pass through a field-programmable gate array (FPGA)-based prioritization system that will override any non-safety command in the presence of a safety-system command to the same actuator. For example, if a non-safety command is directing the closing of a valve, but a competing safety-system command directs the valve open, the FPGA-prioritization system will forward the "open" command to the valve. More details are provided in Section 5.2.2 of the provided reference [34].

The following remote allowlisted-control example architecture uses the AP-1000 non-safety-to-safety control implementation as a reference case. In this example architecture, there is no communication link between the remote-operations center and reactor-facility control systems. Instead, the remote-operations center connects to an allowlist-enforcement system at the reactor facility that provides electrical and communication isolation from plant control systems.

Figure 5 shows how the example allowlist remote control implementation would fit into a DCSA. This DCSA contains five security levels. Specific to remote operations are the five security zones highlighted with a thick border; $Z_{5B,}$ Z_{4D}, Z_{4C}, Z_{3B}, and Z_{3C}. Boundary Device A is a firewall that allows connections between the remote-operations workstation in Z_{5B} and the first jump host in Z_{4C}. Boundary Device B is a firewall or similar device that only allows connection between the remote-operations center jump host in Z_{4C} and the reactor-facility jump host in Z_{4D}. Boundary Device C is a firewall or similar device that only allows connection between the jump host in Z_{4D} and the engineering workstation in Z_{3C}. Boundary Device D is a data diode that allows one-way communication from the higher Security Zone Z_{3B} to the lower Security Zone Z_{3C}. Finally, Boundary Device E is a discrete I/O or analog I/O passing through one-way boundary devices and fiberoptic electrical isolation to I/O in Z_{3B}, thus breaking any means of digital communication between remotely accessed Zones Z_{5B}, Z_{4D}, Z_{4C}, and Z_{3C}.

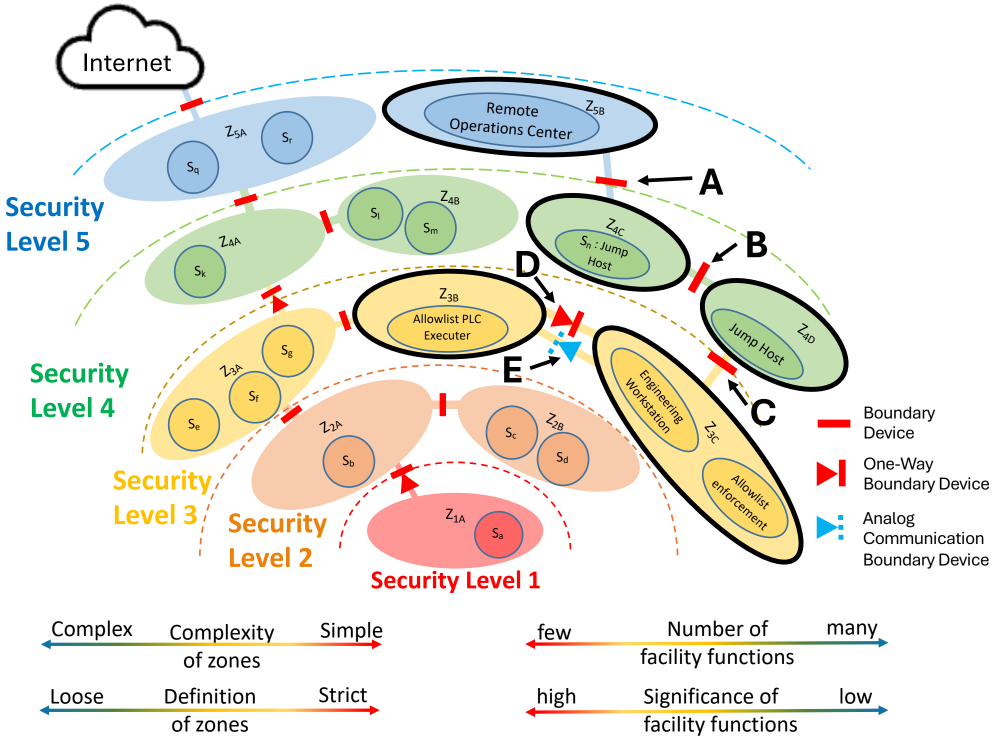

Figure 5. Defensive cybersecurity architecture for the proposed remote allowlisted-command implementation.

Figure 6 presents a network diagram for the connection between the remote-operations center and the reactor facility. The connection between the remote-operations center and the reactor facility is made using secure methods such as a VPN via IPsec, Jump hosts, and firewalls. The operator's station at the remote-operations center does not directly reach the engineering workstation at the reactor facility. Instead, the operator's station must have authorization to pass through a firewall and access a jump server located within the remote operations center. That jump server then connects via VPN through another firewalled, audited path, to a second jump server located at the reactor facility. From this second jump server, the operator again needs credentials and an MFA pass through a firewall to access the reactor-facility engineering workstation, which places the operator at the remote-operations center in an equivalent position to being at the reactor-facility engineering workstation physically, in person. At this point the operator can begin to send allowlisted commands to the reactor facility. If the received command is validated and authenticated, the command gets passed to an allowlist-enforcement device, such as a PLC. The allowlist-enforcement PLC is connected via discrete I/O or analog I/O through one-way boundary devices and fiberoptic electrical isolation to I/O nodes on plant-control systems. The allowlist-enforcement PLCs then pass commands via these discrete or analog I/O-to-I/O nodes on plant-control systems. One last allowlist controller on a plant-control system processes the signals received by the I/O, performs one more validation of the command, and starts the corresponding control program.

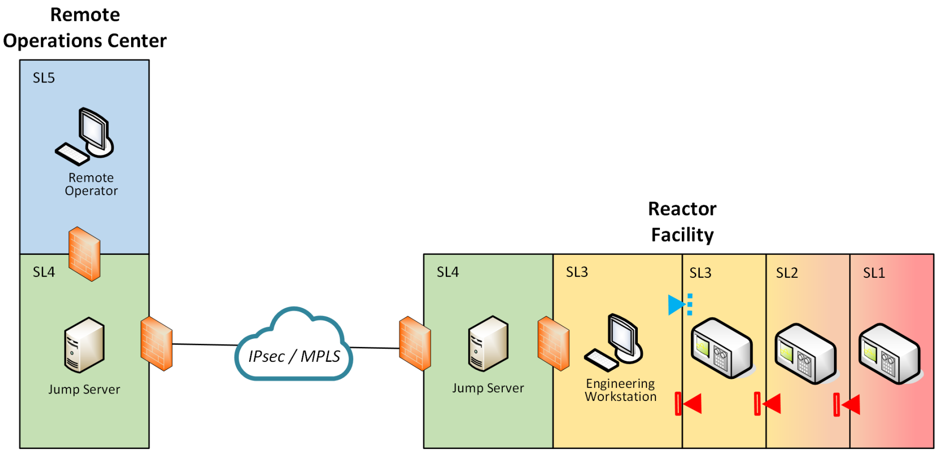

Figure 6. Network diagram for the remote-operations center to reactor-facility connection for allowlisted control.

The reason for the communication link's being limited to discrete I/O or analog I/O is the limited amount of information that can be conveyed over these connections via the presence, absence, or amount of electric current or voltage. With both discrete and analog I/O, one I/O pair, known as a channel, corresponds to one function. Discrete I/O is common in industrial control systems when the only information needed to be conveyed is a binary state, such as on or off, much like a light switch. One example is a signal sent by a PLC via discrete I/O to a relay to open or close the relay. Another example is a limit switch that indicates whether or not the limit switch has been activated. A common implementation in industrial controls of discrete I/O is 0–24 VDC, where the output device applies either 0 or 24 VDC to the connection while the input device monitors this voltage. Typically, 0 VDC corresponds to an OFF state while 24 VDC conveys an ON state, but could correspond to any binary state as set by the control-system designer. In the allowlist case, these binary states would correspond to whether or not a specific control program tied to that I/O pair is executed.

Analog I/O can communicate a continuous state as opposed to just a binary state like discrete I/O. With analog I/O, a voltage or current within a predefined range is applied to the connection with the amount of current or voltage corresponding to a system state or control action. Common implementations include 4–20 mA, 0–10 VDC or -10 to +10 VDC. An example would be a position sensor that provides a 4–20 mA current corresponding to a position to a PLC via analog I/O that the PLC then interprets to a position based on a predefined calibration. A control via analog I/O example would be a PLC that sends a voltage ranging from 0 to 10 VDC to a variable-position valve for which the amount of voltage corresponds to a commanded valve position. In an allowlist command case, an analog signal could be sent that corresponds to a continuous setpoint, such as a reactor power level.

The key benefit of using analog and discrete I/O is that communication is restricted to simple electrical signals. Although a cyber adversary could theoretically manipulate the signal if they had access to the sending device, they cannot move through the connection to downstream devices. Analog and discrete connections do not support such functionality, making them effective network-boundary devices.

This example architecture satisfies the first condition laid out that the remote control infrastructure cannot provide a pathway to access plant-control systems because there is no digital-communication pathway between the remote control infrastructure and plant-control systems. In the worst-case misuse or compromise scenarios of the remote-operations infrastructure, actions taken against a plant-control system would be limited to those actions designed into the I/O link.

This leads to the second condition of successful implementation of an allowlisted remote-operations system: remotely operated plant-control systems must only take actions that are verified, validated, and safe. Even in the case of compromise of the remote-operations infrastructure and manipulation of allowlist control signals sent from Z_{3C} to Z_{3B}, reactor safety must be maintained. Because all reactor safety-significant, important-to-safety, and safety-related systems are isolated from any remotely accessed systems, their functionality should not be impacted even under the case of unintended manipulation of any of the remotely accessed systems. However, the proposed mitigations in Table 6 are example functions that could be implemented within Z_{3B} in order to maintain a defense in depth against any malicious remote actions. Keep in mind these are proposed mitigations and are not intended to be an exhaustive list.

Table 6. Example mitigations for increased defense in depth for remote allowlisted operations.

Proposed Mitigation	Function Served	Example
Local Control Override	Any locally issued control action has overriding authority over remote issued action.	Remote action drives plant outside of defined process bounds to local control issues overriding and corrective action. Local control issues an action different from the remote issued action. Remote action is overridden.
Remote Command Redundancy	Redundant allowlist command issued from Z_{3C} to Z_{3B}. Agreement among commands required for action.	Three allowlist PLCs, each network segmented from the others, receive the remote command. Two out of three voting is required for the plant-control system to act.
Local Programming Access Only	Any component of the remote operations infrastructure can only have its programming altered locally, no remote programming updates.	Remotely accessed hardware, such as the allowlist PLC in Z_{3C}, has a key switch to put the controller in “Run” or “Program” mode that disallows programming changes unless the switch is physically actuated in person.

4.3.1.2 Allowlist Functionality

The intent of the allowlist system is to limit control function to only specific and approved commands that have known, deterministic outcomes. This severely limits the actions that can be taken by the entity upstream of the allowlist, in this case a remote operations center. The intent of this section is to provide example reactor-facility functions that could be controlled remotely from the remote-operations center using the allowlisted-command approach. Table 7 provides a set of functions that could be controlled from the remote-operations center, the allowlisted command that would be sent from the remote-operations center to the reactor facility, and the local-control program that would perform the function.

Table 7. Example remote allowlist control functions.

Function	Allowlisted Command	Local Control Program
Power Output Change	Power Setpoint Value	Reactor and BOP automated-control program that drives the plant to the commanded power output setpoint.
Operating Mode	Load Follow or Programmed Schedule	Reactor and BOP automated-control program that drives the plant to the commanded power output setpoint.

Reactor Startup	Start Reactor	Executes a program that performs automated reactor startup. If conditions are passed, a pre-programmed series of steps are enacted to start the reactor, with checks along the way for proper progression.
Planned Shutdown	Shutdown Reactor	Executes a program that brings the reactor to a shutdown state. Note that this is not the scram function, but for planned shutdowns.

A key feature, but also limitation, of the allowlist remote-operations architecture is that the remote-operations center can take no action that is not part of a pre-programmed control. For example, an operator at the remote-operations center is not able to directly command the actuation of a single valve unless the actuation of that valve is itself an allowlisted command. However, in order to put the actuation of a single component on the command allowlist, it would have to be demonstrated that actuation of the valve in any manner while the plant is in any possible state leads to a deterministic outcome and is safe, which is most likely an unreasonable task. For this reason, the ability to manipulate any individual actuator in the plant is likely to not be possible via allowlist. To prevent any remote action from adversely impacting plant health, every remote command must be executed by a local control program that has been validated not only to perform the requested command properly and safely and to abandon execution of the requested command if safe execution is not possible. Because of the effort required to create, validate, deploy, and maintain such control programs, the amount of remote control functionality from the remote operations center will likely be limited.

4.3.2 Allowlist Cybersecurity Regulatory Considerations

A design goal of the proposed Class 2 architecture with regards to cybersecurity was to avoid the subjugation of the remote-operations center and associated pathway to §73.54. The approach used to accomplish this was to design the architecture in such a way that limits assets in the remote-operations infrastructure from being classified as a CDA. This section covers how the proposed allowlist architecture may be evaluated for applicability of §73.54.

Referring to Figure 5, the DCSA for the proposed allowlist remote-operations architecture includes five zones, highlighted in black, that are part of the remote-operations infrastructure. Of these five zones, four zones—Z_{5B}, Z_{4D}, Z_{4C}, and Z_{3C}—contain only DAs, no CDAs. No asset in any of these zones performs any SSEP function, no asset in these zones serves as a support system to SSEP functions, and no asset in these zones has a pathway to any device that performs SSEP functions because of Boundary Devices D and E. Therefore, it can be stated that no CDAs are present in any of these zones, and §73.54 is not applicable to any of these four zones as no assets in any of these zones would meet the guidelines laid out for the classification of assets as CDAs in NEI 10-04, Rev. 3 [13].

The fifth zone of the remote-operations infrastructure, Z_{3B}, is where §73.54 may be applicable and requires closer examination. There are two cases for the classification of assets in Z_{3B}, dependent on the classification of plant functions ultimately controlled via allowlist. In Case 1, if no SSEP functions or SSEP function support systems are controlled via the allowlisted control program, and no pathway is present to any SSEP function performing assets, then all DAs in Z_{3B} would not be classified as CDAs, and Boundary Devices D and E would not be classified as CDAs. In Case 2, the allowlisted control program does control a SSEP function, SSEP support system, or has pathways to systems that do perform SSEP functions. In this case, the DAs within Z_{3B} as well as Boundary Devices D and E would be considered CDAs. Therefore, Z_{3B} and Boundary Devices D and E would be subject to the Cyber Rule and would require commensurate protection under §73.54.

In practical application in a reactor deployment, it is likely that Case 2 would be more probable than Case 1 in terms of classification of Z_{3B}. This is because most reactor-facility functions useful to remote controls would likely receive an SSEP designation. For example, see the allowlisted control functions presented in Table 7. All proposed example functions would involve an SSEP function, such as manipulating reactivity control or BOP control in the "Power Output Change" example, thereby qualifying as Case 2 and requiring Z_{3B} be protected under §73.54.

4.3.3 Allowlist Physical Security Considerations

The physical-security considerations of a remote-operations facility with allowlist functionality to the reactor site will depend on the personnel executing the allowlist commands at the remote location. The MCR might be located at the reactor site with non-licensed operators executing the allowlist commands. In that case, there are no perceived security requirements on the remote facility because any action there would not negatively impact security. If the remote facility contains the designated MCR, then physical-protection requirements will apply to control access to the MCR and associated defined vital areas at the remote facility. This class of remote operation is predicated on the allowlist architecture, only allowing approved actions and denying any action from the remote-operations center that could negatively impact security.

4.4 Class 3: Remote Control of Non-Safety Systems

Remote control access from the remote-operations center for systems and equipment that do not impact reactor safety may *conceptually* be possible under the current or proposed U.S. regulatory frameworks, assuming all safety actions are controlled by systems located at the reactor facility, and no action taken from the remote operations center can impact reactor safety. However, this is extremely dependent on the implementation of such a concept. From a physical security perspective, control of non-safety-significant systems that do not have an impact on reactor facility safety from the remote-operations center would not qualify systems at the remote-operation center as target elements. Thus, the remote-operations center requires no specific physical protections under §73.55. From a cybersecurity perspective, it is slightly more complex. Any remote control of non-CDAs at the reactor facility would not subject the remote-operations center DAs and the associated pathway (i.e., the communication network) to a cybersecurity program under §73.54. However, any remotely controlled non-safety, but CDAs, would subject the remote-operations center DAs and the associated pathway to a cybersecurity program under §73.54 and would require commensurate protection. Section 4.4.1will provide an in-depth example of a potential implementation of Class 3 remote operations.

Class 3 remote operations allows for the full remote control for non-safety-significant, not important to safety, or non-safety-related SSCs at the reactor facility from the remote-operations facility. In Class 3, no commands are required for safety, meaning that no commands are required from the remote-operations center for the reactor to maintain a safe state. In addition, all safety actions are controlled by systems located at the reactor facility, and no action taken from the remote-operation facility can impact reactor safety. The key difference between Class 2 and Class 3 operation is that Class 3 remote operation provides for the ability to remotely control individual functions of the reactor facility, such as modifying a pump speed or opening and closing a valve. The intent is to give operators at the remote-operations center similar amounts of control as they would have in a local control room, but only for non-safety systems. This capability to remotely control individual functions offers higher amounts of control than Class 2 operations, where the only remote-operator actions possible are the commanding of the execution of local control programs at the reactor facility, with no control over individual functions, systems, or components.

The proposed application of remote control for non-safety-significant, not important to safety, or non-safety-related systems and equipment in A/SMRs restricts remote control capability to SSCs and DAs that both are (1) non-safety and (2) designated for remote operation. This report presents an example architecture of non-safety-system remote control for nuclear remote operations that uses system design to limit remote access only to those non-safety systems that have been designated for remote operation. This approach ensures that there is no pathway for adversarial access to the reactor-facility systems through the remote-operation infrastructure. This example implementation is not meant to be prescriptive in terms of how the remote operation of non-safety systems should be conducted; instead, it is intended to be informative to stakeholders on how allowlisting could potentially be applied in order to inform their system designs.

4.4.1 Remote Non-Safety Control Implementation

The design intent of a non-safety control implementation is to limit remote control capabilities and remote-access pathways to specific non-safety systems at the reactor facility that have been designated for remote control. Two conditions are required for the remote control of non-safety SSCs. Remote access is limited only to non-safety SSCs that (1) are contained to a security zone isolated from all other plant systems and (2) cannot lead to a safety issue, as detailed in Section 2.3. The first condition states that the remotely accessed SSCs and DAs should be segmented from all other plant SSCs and DAs to prevent unintentional access to other plant systems that may not be intended for remote access. In short, there should be no pathways for a malicious or non-malicious actor, either internal or external, to access any SSCs deeper within or adjacent to the remotely accessed non-safety system. Proper segmentation is context dependent, with specific implementations differing between functions and applications. For example, in some contexts, separation between the remotely accessed zone and other control systems through a two-way boundary device, such as a firewall, may be sufficient. In other circumstances, complete separation of the remotely accessed zone from all other plant non-safety systems, or the limitation of communication to one-way from non-remote zones to the remote zone via data diode may be necessary.

The second requirement states that any remotely accessed non-safety SSCs cannot impact reactor safety. This means that any action the non-safety system can take in any state of the plant cannot directly or indirectly cause or lead to an unsafe state. If a system is not classified as part of the safety basis of a plant and, therefore, is a non-safety system, it can be assumed that it has no impact on plant safety, even in the case of failure or manipulation. However, this assumption must be validated if the system of interest is to be remotely controlled. Note that this is not just limited to digital connections between the remotely accessed SSC and other plant SSCs, but physical functionality of the remotely accessed SSC and its impact on other SSCs. Section 4.4.1.1 provides an example implementation of a non-safety control architecture that would meet both conditions.

4.4.1.1 Example Implementation

Once again, Figure 3 and the IAEA Nuclear Security Series No. 17-T representation of a DCSA showing the segmentation of plant systems into security levels and function-based zones will be used as a guide for remote non-safety-control implementation. As discussed previously, it is often discouraged or even prohibited within nuclear power plants to allow communications from Security Level 2 to the higher Security Level 1 (and often from Security Level 3 to Security Level 2 and Security Level 3 to Security Level 4, depending on the SSCs in each security level). In the case of the Class 2 allowlisted-command example implementation, this barrier was overcome by restricting the commands that can be sent from a lower security level to a higher level. This restriction was implemented through the use of dedicated analog channels for each allowlisted command between the lower and higher security level system, thus breaking the digital communication pathway. However, this approach significantly limits the actions taken by an operator at the remote operations center to those control programs that have been built into the system. Class 3 remote control of non-safety systems expands the amount of control capability over reactor-facility functions from the remote-operations center relative to the allowlist-command implementation. Class 3 remote operations provides an operator at the remote-operations center the ability to control individual functions, such as a valve position, pump speed, or flow-rate set point. This is opposed to the allowlist-command implementation, where any individual function actuation is handled by a local control program.

Figure 7 presents the way the example non-safety control implementation would fit into a DCSA. This DCSA contains five security levels. Specific to remote operations are the four security zones highlighted with a thick border: Z_{5B}, Z_{4D}, Z_{4C}, and Z_{3C}. Boundary Device A is a firewall that allows connections between the remote operations workstation in Z_{5B} and the first jump host in Z_{4C}. Boundary Device B is a firewall or similar device that only allows connection between the remote-operations center jump host in Z_{4c} and the reactor facility jump host in Z_{4D}. Boundary Device C is a firewall or similar device that only allows connection between the jump host in Z_{4C} and the engineering workstation in Z_{3C}. Boundary Device D is a data diode that allows one-way communication from the higher security zone, Z_{3B} to the lower security zone, Z_{3C}. In this particular example, no outbound data flow is possible from the remotely connected Z_{3C} to any other security zone not already part of the remote-operations pathway.

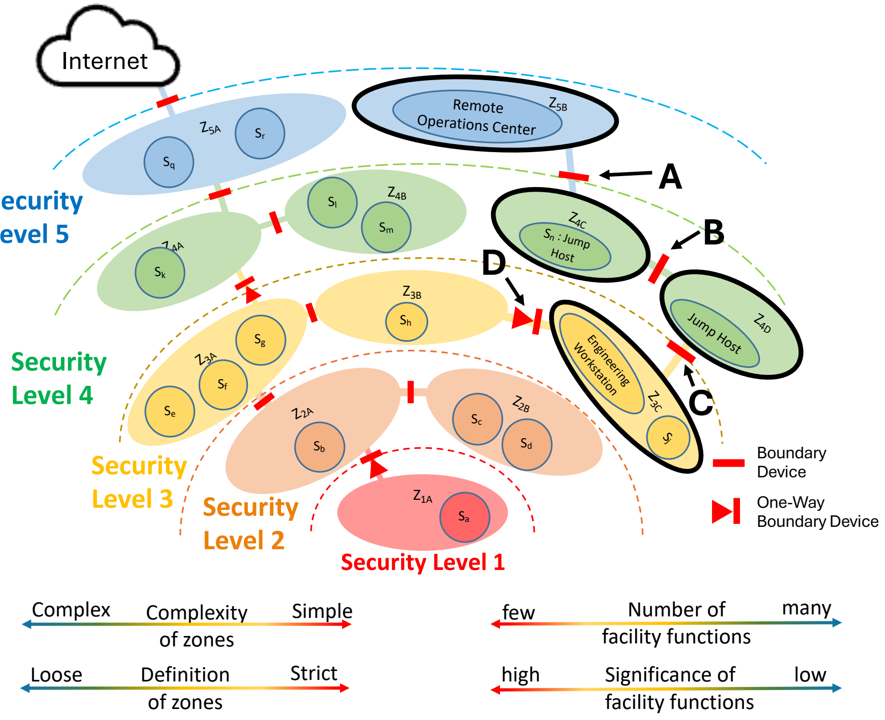

Figure 7. Defensive cybersecurity architecture for the proposed non-safety control implementation.

The following proposed architecture for the remote control of non-safety systems is designed to meet the first condition of the remote control of non-safety-systems design intent: the remote facility only has access to a limited set of non-safety systems at the reactor facility. Figure 8 presents the network diagram for Class 3 remote operation. The connection between the remote-operations center and the reactor facility is made using secure methods such as a VPN via IPsec, jump hosts, and firewalls. The operator's station at the remote operations center does not directly reach the engineering workstation at the reactor facility. Instead, the operator's station must have authorization to pass through a firewall and access a jump server located within the remote-operations center. That jump server then connects via VPN through another firewalled, audited path, to a second jump server located at the reactor facility. From this second jump server, the operator again needs credentials and an MFA pass through a firewall and access to the reactor-facility engineering workstation, which places the operator at the remote-operations center in an equivalent position to being at the reactor-facility engineering workstation physically, in person. Notably, remote access is limited only to non-safety SSCs that (1) cannot lead to a safety issue, as detailed in Section 2.3 and (2) are contained to a security zone isolated from all other plant systems.

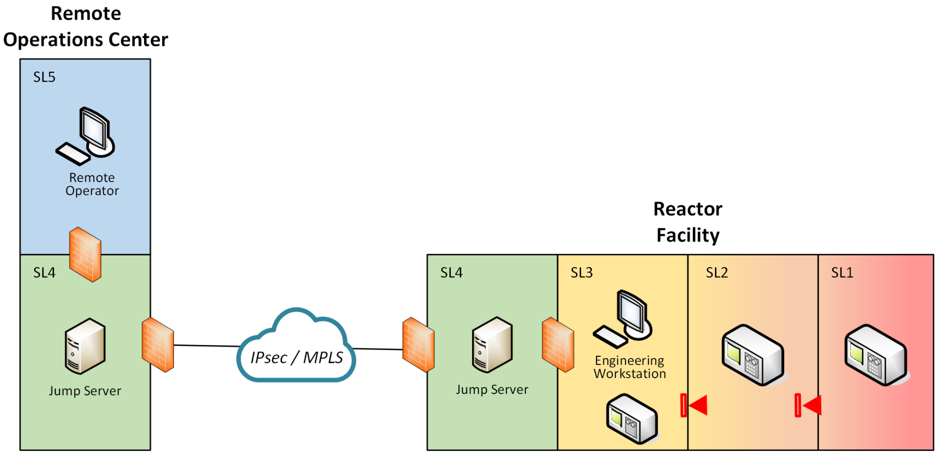

Figure 8. Network diagram for the remote operations center to reactor facility connection for non-safety control.

This example architecture satisfies the first condition for non-safety-system remote control that remote control access is limited to a specific set of non-safety systems at the reactor facility. In the worst-case misuse or compromise scenarios of the remote operations infrastructure, actions taken against a plant-control system would only be limited to those actions that can be taken from Z_{3C}.

The second condition for successful implementation of a non-safety remote control structure is that the remotely controlled non-safety SSCs cannot cause any safety issues in the plant. Even in the case of compromise of the remote-operations infrastructure and manipulation of control signals within Z_{3C}, reactor safety must be maintained. Because all reactor safety-significant, important-to-safety, and safety-related systems are isolated from any remotely accessed systems in the proposed architecture, their functionality should not be impacted even in the case of unintended manipulation of any of the remotely accessed systems. However, even with this isolation, defense-in-depth should still be practiced to ensure safety of the reactor. Table 8 presents example mitigations that could be implemented within Z_{3C} to improve defense in depth. Keep in mind, these are proposed mitigations and are not intended to be an exhaustive list.

Table 8. Example mitigations for increased defense in depth for remote non-safety control operations.

Proposed Mitigation	Function Served	Example
Local Control Override	Any locally issued control action has overriding authority over remote issued actions.	Remote action drives plant outside of defined process bounds, but local control issues overriding and corrective action. Local control issues an action different from the remote issued action. Remote action is overridden.
Local Programming Access Only	Any component of the remote-operations infrastructure can only have its programming altered locally: no remote programming updaters.	Remotely accessed hardware, such as a controller or engineering workstation in Z_{3C}, has a key switch to put the controller in “Run” or “Program” mode that disallows programming changes

		unless the switch is physically actuated, in person.

4.4.1.2 Examples of Remotely Controlled Non-Safety Functions

The intent of a Class 3 non-safety remote-operation system is to limit remote control functions only to specific systems within the reactor facility, but provide operators at the remote operations facility a greater degree of control over said systems than is provided through the allowlist remote control implementation. While this implementation does allow for a remote-operations center to have a higher degree of control of reactor facility systems, the systems that can be remotely controlled are much more limited relative to Class 2 allowlisted remote control. Table 9 provides example functions, systems, and parameters that could be controlled by the remote-operations center for systems that are typically classified as non-safety systems. Note that the list is for example purposes and not exhaustive of all functions.

Table 9. Example non-safety functions that could be controlled from the remote operations center.

Function	Non-Safety System	Example Control Parameters
Plant Power Output	Turbine Control System	Steam Inlet Valve Position
Grid Connection	Generator System	Close Generator Circuit Breaker
Nuclear Reactor Thermal Power	Reactivity Control System	Control Rod or Drum Position

Of the three example functions provided, two would control systems that would most likely be designated as non-safety systems—specifically, plant power output via the turbine control system and the connection of the plant via the generator system. Any manipulation of these systems via the remote-access pathway would not cause a direct or indirect safety issue for the reactor, and proper segmentation of the digital components of these systems from the remainder of the plant should block any pathway from the remotely accessed non-safety systems to any other systems at the plant. The primary risk of any unintended manipulation of these remotely accessed systems and functions is the loss of power output of the plant. In many LWRs, sudden loss of the turbine generator will result in a reactor trip. While this is of concern to the plant operator, a reactor trip and lost generation does not represent a safety issue for the plant, with the caveat that a reactor trip can challenge safety systems. And, in accordance with the current guidance in NEI 13-10, Revision 7, if the compromise of a DA can result in the generated megawatts being reduced to zero within 15 minutes, then it is designated as either a BOP CDA or BOP/Trip-SCRAM CDA [12].

The third example, changing reactor power via a change in control-rod or drum position, is less certain on whether the system would receive a non-safety designation, and therefore, the capability to control this system and achieve the desired change-of-reactor power function from the remote operations center is questionable. That being said, if a reactor designer wants to achieve this function remotely, careful consideration needs to be taken in the design of the plant to designate this system as non-safety. This includes designing the reactor in a manner that the remotely operated reactivity control mechanisms are not part of the safety basis of the reactor, and that the control of DAs associated with remotely operated control mechanisms are properly segmented from any important-to-safety or safety-related systems or pathways.

4.4.2 Non-Safety Cybersecurity Consideration

The design intent for the proposed Class 3 non-safety remote-operations architecture, from a cybersecurity perspective, is to limit remote access to systems at the reactor facility to only those non-safety systems that have been designated for remote access. The approach used was to isolate remotely accessed systems from all other reactor-facility systems such that no pathway exists between the remotely accessed systems and non-remotely accessed systems that would be subject to §73.54.-This section covers how the proposed non-safety remote control architecture may be evaluated for applicability of §73.54.

Figure 7 presents the DCSA for the proposed non-safety remote control architecture. In this architecture, there are four security zones, highlighted in black, that are part of the remote-operations infrastructure with the expressed purpose of remotely controlling non-safety systems located in Z_{3C} from the remote-operations center. The classification of assets and the applicability of §73.54 to remotely accessed zones Z_{5B}, Z_{4D}, Z_{4C}, and Z_{3C} are dependent on the functions performed by assets within Z_{3C}. In general, because only non-safety systems may be located in Z_{3C}, no digital asset in any of the remotely accessed zones should receive a safety-related or important-to-safety CDA designation. In addition, because no pathway leads to any other security zones that may perform or support an SSEP function due to either total isolation from other zones (no connection) or isolation via one-way boundary devices, such as Boundary Device D. Therefore, zones Z_{5B}, Z_{4D}, Z_{4C}, and Z_{3C} may not fall under the Cyber Rule if they do not contain CDAs. However, if any non-safety system in Z_{3C} performs a function that would result in the system receiving a BOP CDA, BOP-Trip/SCRAM CDA or EP CDA designation under NEI 13-10, Rev. 7, then the entire remote-operations infrastructure, including the pathway from reactor facility to remote-operations center, would require protections under §73.54 commensurate with guidance outlined in NEI 13-10, Rev. 7, for protection of BOP CDA, BOP-Trip/SCRAM CDA or EP CDA [12].

4.4.3 Non-Safety Physical Security Considerations

This class of remote operation introduces new security considerations due to the connectivity to specific reactor-site systems. At the reactor site, the I&C architecture will need to provide strict separation between the safety-related and safety-significant I&C, and the I&C that connects to the remote-operations facility. This separation would ensure that the remote facility does not impact the safety of the reactor. The possibility may be that the remotely operated non-safety-related or non-safety significant equipment may be defined as a target element, and as such, must be considered within the site protective strategy (to include the assumed loss of those target elements). Connectivity of the remote-operation facility to safety-significant and safety-related equipment would change the class of remote operation to Class 4 or 5 remote operation, and incur additional physical-security requirements, up to securing the transmission pathway.

In the case of the MCR's being located at the reactor site, and the remote-operations center being also staffed with licensed operators who cannot impact safety, no regulatory requirements would apply to the remote facility. If the MCR was defined at the remote-operations center but could only control non-safety and non-safety-significant equipment and transmit non-safety commands, the MCR would need access control and protection as a vital area. Any SSCs defined as target elements would also need to be protected as determined by the protective strategy.

4.5 Class 4: Remote Control of Safety-Significant and Important-to-Safety Systems

Class 4 remote operations permit full remote control of safety-significant and important-to-safety systems and equipment. The intent is to capture those safety systems and equipment that may fall within the scope of the security program to protect, but that are not defined as safety-related. However, doing so would have serious implications from a physical- and cybersecurity requirements perspective. From a physical-security standpoint, the remote-operations center and transmission pathway (i.e., communication infrastructure) would most likely contain target elements and would thus require physical protection under §73.55 and §73.56. From a cybersecurity standpoint, all remote-operations center DAs and pathway DAs (i.e., communication infrastructure) would be classified as, at minimum, indirect CDAs. Thus, all remote-operations center and pathway DAs would be subject to the protection requirements commensurate with §73.54. These protections, especially for the communication pathway, would be extremely expensive, if not logistically impossible. Therefore, the implementation practically of Class 4 remote operations is extremely low and likely has no path forward within the current regulatory environment. For this reason, this report does not present an example architecture for the implementation of Class 4 remote operations. They are not likely a viable current option for remote-operations implementation in the U.S.

4.6 Class 5: Remote Operation of Safety-Related Systems

Class 5 remote operations allow for remote control of all reactor-facility systems and equipment, including safety-related systems. Similar to Class 4 remote operations, allowing for remote control of safety-related systems would have serious physical- and cybersecurity requirements implications. The remote-operations center would contain target-set systems and equipment and would require a physical-protection program as defined in §73.55 and §73.56. In addition, the physical-protection program would also need to protect necessary support and transmission equipment (i.e., communication infrastructure) as vital equipment. In terms of cyberprotections, all remote-operations center DAs and pathway DAs (i.e., communication infrastructure) would be classified as CDAs. Thus, all remote-operations center and pathway DAs would be subject to the protection requirements commensurate with §73.54. Similar to Class 4, implementing these protections, especially for the communication pathway, would likely be logistically prohibitive, if not impossible to implement. This leads to the conclusion that there is likely no regulatory path forward to gain approval for Class 5 remote operations. In addition, there is little reason to pursue this class of remote control because safety-related systems may not be able to satisfy certain design requirements, such as response time to emergency events, if such actions had to be taken remotely. Finally, reactor-safety systems are largely fully automated in their current deployments, leaving little reason to shift their control to remote operation.

4.7 Non-Regulatory Cyber Security Implications of Remote Operations

Presented so far in this report is a framework for classes of remote operation and their relation to existing physical- and cybersecurity requirements regulations, as well as two example architectures of remote operation that may have a path forward to regulatory compliance. However, these proposed architectures are focused on regulatory requirements for protecting reactor safety and preventing the possibility of radionuclide release and nuclear sabotage. What has not been discussed is the non-regulatory impacts of remote operation, especially for the plant’s operational availability, which refers to the actual availability of a plant to output power to its intended consumer relative to the planned availability of production. For example, even if a remote-operations architecture is implemented in accordance with Class 2 or 3 remote operations proposed in this report, and therefore, remote operation proposes no safety risk to the reactor (e.g., of radionuclide release), if the operation of the reactor is dependent on the connection to the remote-operations center, disruption of that connection could render the reactor unable to accomplish its mission even if the safety of the reactor is maintained. This section will provide insight into the current threat landscape facing remotely operated critical infrastructure and the impact these potential threats would have on the proposed Class 2 and 3 remote-operations architectures.

4.7.1 Current and Recent Threat Landscape

This section presents five different cyberattacks on critical infrastructure wherein each attack leveraged a remote connection to the target’s network, ultimately causing an interruption or change to the OT process. Each example describes what happened, the mechanism used for the attack, the impact of the attack, and means by which the attack could have been prevented. This review is not meant to provide a comprehensive threat assessment of cyberattacks on remotely operated critical infrastructure. Instead, it is meant to provide some context as to the types of threats that any remotely operated nuclear power plant will need to mitigate against in order to maintain plant power-generation availability.

4.7.1.1 Ukraine 2015

In December 2015, Russian threat actors interrupted power at multiple locations through a remote connection, affecting approximately 225,000 people in western Ukraine for about six hours. The attackers used a combination of spear-phishing emails, malware, and remote-access tools to infiltrate the networks of three energy-distribution companies [35]. The malware used, called BlackEnergy, allowed the attackers to take control of the systems and remotely switch off substations [36]. Mitigations and recommendations released after the attack include ensuring proper network segmentation, employing active logging for both IT and OT networks, and backing up critical project files [35].

4.7.1.2 Ukraine 2016

In December 2016, another attack hit Ukraine's power grid, this time targeting the Pivnichna substation in Kiev. The incident caused a power outage that lasted about an hour. The malware used in this attack, known as Industroyer or CrashOverride [37], was a more advanced version of BlackEnergy and was specifically designed to disrupt industrial control systems [38]. Mitigations and recommendations published after the attack included further-improved network segmentation, including a network demilitarized zone (DMZ) with jump hosts and a rehearsed incident recovery and response plan including both IT and OT personnel.

4.7.1.3 Ukraine 2022

In October 2022, Russian threat actors exploited a hypervisor[c] and interrupted power by loading a malicious batch file in the system. This native implementation of a batch file not only interrupted power at the target substation, but it also allowed the threat actors to cause an impact without the development of a specific malware tool [39]. Mitigations and recommendations produced after the attack included the development of network baselining[d] and the added security and patching of hypervisors interacting with controls networks.

4.7.1.4 Aliquippa Municipal Water Authority 2023

In December 2023, Iranian threat actors accessed and defaced an Internet-facing booster pump controller, subsequently knocking it offline. The attack caused a minor loss in water pressure, but the utility was able to move to manual operations and ensured the quality of the drinking water was unaffected. Further analysis of the attack discovered the controller was likely discoverable on the Internet and configured with default credentials. Best practice includes segmenting controllers from the external Internet, and default credentials should be changed upon installation [40].

4.7.1.5 Texas Water Facilities 2024

In 2024, four Texas water facilities reported cyberattacks on their infrastructure [41]. In the city of Muleshoe, the attackers successfully gained remote access to the controls network and altered setpoints within the system. These changes caused an elevated water tank to overflow for 30–45 minutes before the plant was switched to manual operations. In Hale Center, the utility noted 37,000 failed log-in attempts against their firewall over four days, prompting them to unplug the system and switch to manual operations [42]. Analysis of the attacks found that the four water utilities shared common vendor software for remote access. In these cases, the utilities were able to switch to manual operations, foregoing remote operations and monitoring until the attacks subsided [43]. Mitigations and recommendations for brute-

[c] A hypervisor is a software program used to create and manage multiple virtual machines on a single set of hardware.

[d] Network baselining includes extensive observation of network traffic to identify normal network activity. This baseline is then employed to identify changes and irregularities in network traffic.

force attacks[e] against remote-access login include employing MFA and implementing logging and alerting for failed login attempts [44].

4.7.2 Cyberattack Impact on Proposed Class 2 and Class 3 Architectures

The proposed architectures for both Class 2 and 3 remote operations are designed to mitigate threats to reactor safety that originate from the addition of remote access to designated systems, assuming full compromise of the remotely accessed systems. Class 2 or 3 remote operations using the proposed architectures should not result in any threats to safety of the reactor. However, the addition of remote-operations infrastructure to the reactor facility does lead to the risk of cyberattack on this infrastructure, which could affect the plant's ability to perform its intended function, even if reactor safety is preserved. Therefore, a primary driver for the amount of protection applied to the remote operations infrastructure is the level of risk tolerance and desired capacity factor (e.g., amount of electrical power produced) a reactor owner/operator has for reactor deployments. The intention of this statement is not to downplay the risk of cyberattack or diminish the need for cybersecurity protections. Instead, it is to highlight that, with a properly architected system, the goal of cyberprotection of remote-operations infrastructure shifts from reactor safety to plant availability and generation output.

Each attack outlined in Section 4.7.1, if successfully executed against a Class 2 or 3 remote-operations implementation, would have disrupted plant operations, potentially even resulting in the loss of electricity production of the reactor facility. But notably, the attack would have been limited to only the remotely accessed security zones, and no attack would have resulted in a threat to reactor safety. However, each of the attacks could have been prevented with the proper mitigations put in place, such as improved authentication control using methods like MFA and proper network segmentation using DMZs and jump hosts. These are all protections that should be in place when following and maintaining a well-structured defensive cybersecurity plan, especially one that aligns with modern standards for protection of critical infrastructure, such as those found within NIST's SP 800-series publications for computer-security guidance, like NIST SP 800-82, Rev. 3, "Guide to Operational Technology (OT) Security" [45]. While implementing a Class 2 or 3 remote-operations framework may not result in regulatorily prescribed protections for the remote-operations infrastructure, it is within the best interest of any reactor owner/operator to put in place a robust defensive cybersecurity plan to maintain plant operational availability.

5 AUTONOMOUS OPERATIONS AND THE RELATION TO REMOTE OPERATIONS

Autonomous operations promise substantial operational cost reductions achieved by reducing staffing that would otherwise be required to safely operate a reactor. However, like remote operations, autonomous operations are novel to the nuclear industry and there is a knowledge gap when it comes to understanding the security implications of integrating autonomous operations into reactor designs. As discussed, adding remote operation capability to a reactor heavily influences security requirements. Further, incorporating a new, geographically distinct facility into reactor operations introduces direct implications for an existing physical- and cybersecurity requirements regulatory-framework which were originally designed around a single facility. For autonomous operations, the security implications are more nuanced and can be separated into two cases. Autonomous operations supported by SSCs located only at the reactor site, and autonomous operations supported by SSCs outside of the reactor site.

5.1 Autonomous Systems Contained Within Plant Boundary

Autonomous digital control systems may introduce new operational considerations to ensure reactor safety and, therefore, would require validation. From a cybersecurity and physical-security regulatory

[e] A brute-force attack is a tactic in which malicious software systematically attempts passwords and/or usernames until the correct combination is obtained, and access is granted.

perspective, if all components of the autonomous-operations system are located within the plant boundary, the introduction of autonomous systems will likely not change the facility's requirement to comply with existing cyber and physical security regulations. The systems would still have to be evaluated for the applicability of §73.54 and §73.55, and if applicable, commensurate protections applied. However, this will likely not be the case for complying with other portions of the U.S. regulatory framework, such as 10 CFR 50.54, which explicitly requires that only a licensed operator or senior operator manipulate controls that impact reactivity or reactor power. One potential impact of adding autonomous systems strictly within the reactor facility from a security perspective is the increased complexity of evaluating these systems for compliance with regulation. It is necessary to gather appropriate evidence to ensure that the cyber protections are adequate and that the functionality of the control system cannot be compromised by their introduction. This situation is analogous to introducing digital systems into a nuclear facility that was predominantly designed around analog systems. Notably, the software used in autonomous systems has the potential to be much more complex than the current software used by OT control systems, leading to a more-complex analysis of the software for compliance with cybersecurity requirements, such as those laid out in RG 5.71 Rev. 1 [11] and NEI 08-09, Rev. 7, Appendix E [14].

5.2 Autonomous Systems with External Support

Autonomous operations do present unique needs for data collection and storage and have significant computational needs that may not be feasible to co-locate within the reactor facility, especially in the case of A/SMR deployments with a small footprint, such as a microreactor. Therefore, it may be necessary to site elements of the autonomous system, such as those running high-fidelity physics simulation or large-scale training for AI based models, either at a separate site, such as a company headquarters that has high-performance computing capabilities, or within a cloud-based service. Even if the operations were truly autonomous, with no human involvement, the operations essentially become remote. In this case, the autonomous operations system would need to be evaluated under the remote-operations framework proposed in this report. For example, if the autonomous control system were to act on a safety-significant system at the reactor facility using actions generated on a high-performance computing system at a separate facility, and then protections required would be commensurate with Class 4 or 5. What might be more prudent is to design the autonomous system such that it can exist within Class 2 or 3 to ensure the system and exposed access cannot impact safety. For example, the autonomous functionality could be external to the reactor facility and make use of the allowlist-communication structure to issue commands that can act on the reactor.

6 CONCLUSIONS

Remote operations represent a new paradigm requiring significant changes from existing practices, but they are also of significant interest to A/SMR developers due to potential cost reductions if they can be effectively integrated into reactor designs and concepts of operation. However, as with any technology novel to an industry, there are unknown impacts, including the physical- and cybersecurity implications of integrating remote or autonomous operations. The aim of this report was to investigate and identify the physical- and cybersecurity implications of incorporating remote autonomous operations into an A/SMR concept of operation.

This report contains four major accomplishments. The first is identifying and defining a classification framework of remote operations based upon two factors. The first factor is the functionality at the remote-operations facility enabled by the access to reactor-control systems. The second factor includes the types of control systems that are accessible as well and the safety significance of those control systems. This classification framework offers a structured approach to understanding and implementing remote operations, based on these two factors, to ensure adequate protections are considered and appropriately implemented.

The second accomplishment defined the physical- and cybersecurity requirements that are applicable to the remote-operations facility in each of the defined remote-operations class. For example, in Class 1, where the remote-operations facility has no ability to impact the reactor, essentially none of the physical- and cybersecurity programs required at the reactor facility are required at the remote facility. This is because a compromise in either the physical- or cybersecurity of the remote-operations facility poses no threat to the safety of the reactor. However, at the higher classes, such as Class 4 and 5, where the remote-operations facility has access to safety systems at the reactor, physical- and cybersecurity programs traditionally implemented only at the reactor facility would be required for the remote-operations facility and infrastructure as well. This is due to the risk of physical- or cybersecurity compromise of the remote-operations facility's threatening reactor safety and potentially leading to a radiological release.

The third accomplishment is an assessment of practicality of implementing each of the five proposed remote-operation classes. Of the five proposed classes, only three were deemed practical or potentially practical from a physical- and cybersecurity requirements perspective. Class 1, remote monitoring, is already implemented within the U.S. nuclear industry. Classes 2 and 3—remote allowlisted control and remote control of non-safety systems—were found to have a potential path to implementation within the U.S. regulatory frameworks. Potential architectures for implementing Class 2 and 3 remote operations were proposed. Class 4 and 5 remote operations, which allow for remote control of safety systems, were found to be impractical to implement based on the amount of cyber- and physical-protections necessary on the remote-operations center and pathway between facilities.

The final accomplishment is an assessment of the physical- and cybersecurity requirement implications of autonomous control and the relation between autonomous and remote control. Autonomous control is another new concept for the nuclear industry that may bring potential cost savings. Autonomous functionality may require remote-access capabilities, but the technology itself is compatible with the framework and requires no special treatment beyond the framework considerations for control-system elements.

Multiple pathways of research should be pursued to continue to advance remote and autonomous operations towards commercial deployment:

- Detailed design and demonstration of remote or autonomous control architectures to serve as a learning platform for stakeholders such as reactor developers, reactor end users, and regulators
- Proposed regulations for deployed remote or autonomous control systems to provide clarity to reactor developers on how to proceed with A/SMR design
- Proposed regulatory-guidance documents to provide developers with pathways to meet any current or future regulation that encompasses remote or autonomous operations
- Identification, adoption, or creation of standards by the nuclear community in support of remote- or autonomous-operations deployment.

Overall, this report provides insight for reactor vendors, regulatory bodies, and other stakeholders in the nuclear industry as to how to approach the problem of implementing remote or autonomous operations within the existing U.S. physical- and cybersecurity regulatory framework. By providing a classification framework and practical implementation pathways, it aims to facilitate the safe and effective integration of remote operations into A/SMR designs.

7 REFERENCES

[1] A. Sanghvi *et al.*, "Roadmap for Wind Cybersecurity," United States, 2020–07–01 2020. [Online]. Available: https://www.osti.gov/biblio/1647705

[2] V. Hepsø and E. Monteiro, "From Integrated Operations to Remote Operations: Socio-technical Challenge for the Oil and Gas Business," presented at the Proceedings of the 21st Congress of the International Ergonomics Association, Vancouver, CA, 2021, 2021.

[3] *Domestic Licensing of Production And Utilization Facilities,* United States Nuclear Regulatory Commission 10 CFR Part 50, 1956.

[4] *Licenses, Certifications, and Approvals for Nuclear Power Plants,* United States Nuclear Regulatory Commission 10 CFR Part 52, 1989.

[5] *Risk Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors,* U.S. NRC, Proposed 10 CFR Part 53, 2024.

[6] *Physical Protection of Plants and Materials,* United States Nuclear Regulatory Commission 10 CFR Part 73, 1973.

[7] *Protection of Digital Computer and Communication Systems and Networks,* U.S. NRC, 10 CFR Part 73.54, 2009.

[8] *Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage.,* U.S. NRC, 10 CFR Part 73.55, 2023.

[9] *Target Set Identification and Development for Nuclear Power Reactors,* United States Nuclear Regulatory Commission Regulatory Guide 5.81 Rev. 1, 2019.

[10] *Target Set Identification and Development for Nuclear Power Reactors,* United States Nuclear Regulatory Commission Draft Regulatory Guide 5.81 Rev. 2 2024.

[11] *Cyber security programs for nuclear facilities; U.S. Nuclear Regulatory Commission,* United States Nuclear Regulatory Commission Regulatory Guide 5.71 Rev. 1, 2023.

[12] *Cyber Security Control Assessments*, NEI 13-10 Rev. 7, Nuclear Energy Institue, 2021.

[13] *Identifying Systems and Assets Subject to the Cyber Security Rule* NEI 10-04 Rev. 3, Nuclear Energy Institute, 2021.

[14] *Cyber Security Plan for Nuclear Power Reactors*, NEI 08-09 Rev. 7, Nuclear Energy Institute, 2024.

[15] *Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation, Revision 1*, 30020012752, Electric Power Research Institute, 2018. [Online]. Available: https://www.epri.com/research/products/000000003002012752

[16] *Computer Security Techniques for Nuclear Facilities* (IAEA Nuclear Security Series No. 17-T (Rev. 1)). Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2021.

[17] *Computer Security of Instrumentation and Control Systems at Nuclear Facilities* (IAEA Nuclear Security Series No. 33-T). Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2018.

[18] *Computer Security for Nuclear Security* (IAEA Nuclear Security Series No. 42-G). Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2021.

[19] *Computer Security at Nuclear Facilities* (IAEA Nuclear Security Series No. 17). Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2011.

[20] *Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53,* United States Nuclear Regulatory Commission Draft Regulatory Guide DG-5075: Proposed new Regulatory Guide 5.96 Rev. 0, 2024.

[21] "Pre-Application Activities for Advanced Reactors." U.S. NRC. https://www.nrc.gov/reactors/new-reactors/advanced/who-were-working-with/pre-application-activities.html (accessed January 1, 2025).

[22] *Emergency Response Data System*, NUREG-1394, Revision 2, U.S. NRC, 2022.

[23] H. Smartt, "Remote Monitoring Systems/Remote Data Transmission for International Nuclear Safeguards," Sandia National Laboratories, SAND2022-4273, 2022. [Online]. Available: https://www.osti.gov/biblio/1862624

[24] "Safety-Related." U.S. NRC. https://www.nrc.gov/reading-rm/basic-ref/glossary/safety-related.html (accessed Nov. 21, 2024).

[25] "Safety-Significant." U.S. NRC. https://www.nrc.gov/reading-rm/basic-ref/glossary/safety-significant.html (accessed Nov. 21, 2024).

[26] *Personnel Access Authorization Requirements for Nuclear Power Plants,* United States Nuclear Regulatory Commission 10 CFR Part 73.56, 2023.

[27] *Facility Security Clearance and Safeguarding of National Security Information and Restricted Data,* United States Nuclear Regulatory Commission 10 CFR Part 95, 1980.

[28] "Selecting and Hardening Remote Access VPN Solutions," NSA/CISA, U/OO/186992-21 | PP-21-1362 2021. [Online]. Available: https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/csi_selecting-hardening-remote-access-vpns-20210928.pdf

[29] Elaine Barker, Quynh Dang, Sheila Frankel, Karen Scarfone, and P. Wouters, "Guide to IPsec VPNs," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-77 Rev. 1, 2020.

[30] L. De Ghein, *MPLS Fundamentals*. Cisco Press, 2007.

[31] "Multiprotocol Label Switching for the Utility Wide Area Network." Cisco. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/mpls_wp_v2.pdf (accessed August 13, 2025.

[32] "M&D Center." Curtiss-Wright. https://www.cwnuclear.com/brands/scientech/information-technologies/md-and-center (accessed July 9, 2025).

[33] A. Sedgewick, M. Souppaya, and K. Scarfone, "Guide to Application Whitelisting," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-167, 2015.

[34] A. W. Crew, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," Westinghouse Electric Company, APP-GW-GLR-087, Rev 2, WCAP-16674-NP, Rev 4, 2011. [Online]. Available: https://www.nrc.gov/docs/ML1105/ML110590487.pdf

[35] "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case " E-ISAC and SANS Institute, 2016. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

[36] "When the Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructure " Booze, Allan, Hamilton 2019. [Online]. Available: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

[37] "Industroyer." MITRE ATT&CK https://attack.mitre.org/software/S0604/ (accessed July 28, 2025).

[38] Daniel Kapellmann Zafra *et al.* "INDUSTROYER.V2: Old Malware Learns New Tricks " Mandiant https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/ (accessed July 28, 2025).

[39] Ken Proska *et al.* "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology." Mandiant. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/ (accessed July 28, 2025).

[40] "Exploitation of Unitronics PLCs used in Water and Wastewater Systems." CISA. https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems (accessed July 29, 2025).

[41] "11 Recent Cyber Attacks on the Water and Wastewater Sector " Wisdiam. https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/ (accessed July 29, 2025).

[42] K. Miller, "Rural Texas towns report cyberattacks that caused one water system to overflow," *Texas Tribune*, 2024. [Online]. Available: https://www.texastribune.org/2024/04/19/texas-cyberattacks-russia/

[43] E. Harris, "Leaders from Area Towns Discuss Cyber Attack on Water Infrastructure Systems," *Plainview Herald*, 2024. [Online]. Available: https://www.myplainview.com/news/local/article/leaders-area-towns-discuss-cyber-attack-water-18640534.php

[44] "Brute Force " MITRE ATT&K https://attack.mitre.org/techniques/T1110/ (accessed July 29, 2025).

[45] Keith Stouffer *et al.*, "Guide to Operational Technology (OT) Security," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-82 Rev. 3, 2023.