U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RIL 2024-09

Cybersecurity Audits Alongside a Digital Instrumentation and Controls Licensing Review

May 2024

Prepared by:
E. Lee
A. Kim
K. Lawson-Jenkins
S. Darbali
L. Dumont
I. Garcia

Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001

Eric Lee, NRC Project Manager

Research Information Letter
Office of Nuclear Regulatory Research

Disclaimer

Legally binding regulatory requirements are stated only in laws, U.S. Nuclear Regulatory Commission (NRC) regulations, licenses, including technical specifications, or orders; not in Research Information Letters (RILs). An RIL is not regulatory guidance, although the NRC's regulatory offices may consider the information in an RIL to determine whether any regulatory actions are warranted.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

One effective and efficient way to protect a digital instrumentation and controls (DI&C) safety system upgrade from cybersecurity threats and to comply with U.S. Nuclear Regulatory Commission (NRC) cybersecurity requirements is by integrating a security by design (SBD) framework into every phase of its development lifecycle. By applying an SBD framework from the beginning of the development process, a DI&C safety system can be designed to minimize systems vulnerabilities, reduce the attack surface, and incorporate security features to protect itself from cyber threats and comply with applicable cybersecurity requirements. The NRC staff and licensees recognize the importance of integrating cybersecurity at the early development lifecycle phases for critical digital assets (CDAs) and critical systems (CSs). Regulatory Guide (RG) 5.71, Revision 1, “Cyber Security Programs for Nuclear Power Reactors,” issued February 2023, and the licensee cybersecurity plan[1] (CSP) template provided in Nuclear Energy Institute (NEI) 08-09, Revision 6, “Cyber Security Plan for Nuclear Power Reactors,” issued April 2010, include cybersecurity controls from the initial design to the retirement phases of a CDA’s or CS’s lifecycle. However, integrating cybersecurity controls and features into the safety system design and licensing review is challenging for both licensees and the NRC staff for the following reasons:

- The cybersecurity controls provided in RG 5.71 and the CSPs are not arranged in a lifecycle sequential order similar to RG 1.152, Revision 2,[2] “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” issued January 2006. As a result, the cybersecurity controls associated with a DI&C system upgrade are not chronologically identified or explained in RG 5.71, NEI 08-09, and the CSPs.

- The regulatory framework separates the licensing review of a DI&C upgrade from the cybersecurity audits. The regulatory framework requires the NRC staff to review and approve the design of a DI&C system upgrade (a CDA or a CS) against safety requirements, while the cybersecurity regulation requires the NRC to inspect the licensees’ implementations of their cybersecurity programs under the agency’s Reactor Oversight Process (ROP). Fundamentally, this is a difference between licensing (safety) and oversight (security), which may cause challenges in the application of cybersecurity controls during a DI&C system upgrade for an operating reactor.

Therefore, this report will discuss how an SBD methodology could be applied to a DI&C system upgrade by explaining “what” and “when” cybersecurity measures provided in the CSPs should be addressed by licensees and audited by the NRC to protect a DI&C system upgrade efficiently and effectively from cyber threats while reducing regulatory uncertainties and maximizing efficiencies. This report will explain the following:

- what CSP cybersecurity controls provided in a licensee’s CSP should be addressed by the licensee during a DI&C system upgrade and when they should be addressed

- when the NRC staff should audit a licensee’s resolution of CSP commitments for DI&C system upgrades

[1] NEI 08-09, Revision 6, provides the CSP template used by licensees to develop their CSPs. Therefore, in general, NEI 08-09 is synonymous with the term “cybersecurity plan” (CSP).

[2] Although the latest revision of RG 1.152 is Revision 4, this report makes references to RG 1.152, Revision 2, because that version is actively referred to in RG 5.71, Revision 0.

This report is an informative document that explains a regulatory framework and lists a set of the CSP cybersecurity controls that are associated with a DI&C system upgrade. This report does not establish any NRC policies or positions.

ABBREVIATIONS AND ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
ARP	Alternate Review Process
CDA	critical digital asset
CFR	*Code of Federal Regulations*
CS	critical system
CSP	cybersecurity plan
DA	digital asset
DI&C	digital instrumentation and controls
DIDPS	defense-in-depth protection strategy
EIA	U.S. Energy Information Administration
I&C	instrumentation and controls
ICS	industrial control systems
IEC	International Electrotechnical Commission
ISCM	information security continuous monitoring
ISG	interim staff guidance
ISO	International Organization for Standardization
IEEE	Institute of Electrical and Electronics Engineers
IP	inspection procedure
FAT	factory acceptance testing
HW	hardware
LAR	license amendment request
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
NPP	nuclear power plant
NRR	Office of Nuclear Reactor Regulation
NSIR	Office of Nuclear Security and Incident Response
RG	regulatory guide
RIL	research information letter
ROP	Reactor Oversight Process
SAT	site acceptance test
SIA	security impact analysis
SBD	security by design
SDOE	secure development and operational environment
SRP	Standard Review Plan
SSEP	safety, security, emergency preparedness
Std	standard
SW	software
TR	topical report
VOP	vendor oversight plan

1 BACKGROUND

Licensees are currently upgrading their digital instrumentation and control (DI&C) systems, which are aging and becoming challenging to maintain. DI&C system upgrades are subject to both safety and cybersecurity requirements. The staff of the U.S. Nuclear Regulatory Commission (NRC) and licensees recognize that by integrating cybersecurity into the development and design of DI&C safety systems, licensees can efficiently and effectively comply with both safety and cybersecurity requirements. However, because the Cybersecurity Rule (i.e., Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, “Protection of digital computer and communication systems and networks”) was issued under 10 CFR Part 73, “Physical Protection of Plants and Materials,” and power reactors are licensed under 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities,” or 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants,” the safety evaluation associated with a DI&C upgrade is performed under a license amendment request (LAR), while the cybersecurity evaluation is performed under the Reactor Oversight Process (ROP). Additionally, cybersecurity evaluations are currently performed following installation of a digital system into a plant. Therefore, the NRC is currently engaged with licensees and their vendors to explore the need and opportunities for performing cybersecurity audits parallel to the staff’s licensing review of future DI&C upgrades.

2 DISCUSSION—DIGITAL INSTRUMENTATION AND CONTROL SYSTEM UPGRADES

Integrating cybersecurity requirements from the beginning of the development of a DI&C system upgrade is not new to the NRC staff and licensees. For example, in January 2006, the NRC staff issued Regulatory Guide (RG) 1.152, Revision 2, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,”[3] which includes guidance recommending the integration of cybersecurity requirements from the beginning of the DI&C system development lifecycle. For the same reasons, licensees’ cybersecurity plans (CSPs) include the security controls associated with DI&C system upgrades. This integration of cybersecurity requirements from the beginning of the development of a digital system upgrade is supported by several documents and the collective body of knowledge and experience documented by standards organizations and agencies, such as the International Society of Automation, the Institute of Electrical and Electronics Engineers (IEEE), and the National Institute of Standards and Technology (NIST). These sources state that by integrating cybersecurity from the beginning of the DI&C system development lifecycle, a digital system can be more efficiently and effectively protected from cyber threats while meeting safety goals. The reason is that licensees can develop a strategy to protect their proposed DI&C system upgrades. These strategies include taking advantage of the plant’s security controls and procuring (or designing) a DI&C system that has the minimum attack surface for its environment and implements the security features necessary to address potential risks caused by the upgrade. However, if cybersecurity is addressed only after a system is designed and potentially installed, licensees may face the following challenges:

- needing to implement additional security measures to address the cyber threats that are not eliminated by the design

- adding external security features to the system to address cybersecurity requirements in the licensee’s CSP because the system does not include certain security controls

- potentially redesigning the DI&C system because the cybersecurity requirements (or the cyber threats) are difficult to address using the facility’s programmatic measures or conflict with the functional requirements of digital assets (DAs) or external security features, and possibly needing to resubmit a revised LAR for NRC review of the redesigned system

Although the NRC staff and licensees recognize these challenges, the specific cybersecurity concerns that need to be addressed (i.e., the “what”), and when in the development lifecycle the concerns should be addressed (i.e., the “when”), the following are noted:

- The integration of cybersecurity from the beginning of a DI&C system upgrade design is not required by the NRC until the new system is a DA that must be protected under the Cybersecurity Rule or until the licensee has completed the implementation of its cybersecurity program at its facility.

- The NRC staff has limited experience with cybersecurity evaluations of DI&C system upgrades.

[3] The current revision of RG 1.152 is Revision 4.

- The Office of Nuclear Reactor Regulation (NRR) reviews the safety aspects of the LAR while the Office of Nuclear Security and Incident Response (NSIR) staff evaluates the adequacy of cybersecurity features for compliance with 10 CFR 73.54. The NRR staff communicates with NSIR to report any cybersecurity concerns or design features identified during the LAR review of the DI&C upgrade.

- Licensees often have questions for the NRC regarding application of security controls in their CSPs and how they should be addressed in their LAR. Similarly, the NRC staff often have questions regarding how licensees and their vendors addressed cybersecurity controls, and when during the safety licensing review these questions can and should be addressed (e.g., use of a hardware data diode to control one-way data flow).

This report discusses the following subjects to answer the “what” and “when” questions noted above:

- the regulatory history of cybersecurity
- the safety and cybersecurity regulatory framework
- the NRC’s safety-security interface efforts
- critical digital asset (CDA) changes within the scope of licensees’ CSPs
- security impact analysis
- licensees’ commitments associated with a CDA change
- DI&C-ISG-06, Revision 2, “Licensing Process,” issued December 2018
- engagement with licensees and vendors for a DI&C system upgrade
- DI&C system upgrade cybersecurity inspection of licensees and vendors
- CSP cybersecurity controls associated with a DI&C system upgrade

2.1 Regulatory History of Cybersecurity

Recognizing the potential security issues in commercial nuclear power plants (NPPs) after the terrorist attacks on September 11, 2001, the NRC issued the following, germane to cybersecurity:

- NRC Order EA-02-026, “Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants,” dated February 25, 2002, addresses the threat environment at the time. This order included a specific requirement that directed nuclear power plant licensees to address certain cybersecurity vulnerabilities.

- NRC Order EA-03-086, “Design Basis Threat for Radiological Sabotage,” dated April 29, 2003, supplemented the design-basis threat for NPPs as specified in 10 CFR 73.1, “Purpose and scope,” and, in part, required licensees to address additional cyberattack characteristics. In 2002, the NRC initiated a cybersecurity pilot study at NPPs to develop a method that licensees can use to manage cyber risks at their facilities. The NRC published the results of its cybersecurity pilot study at NPPs in 2004. On November 18, 2005, the Nuclear Energy Institute (NEI) issued NEI 04-04, Revision 1, “Cyber Security Program for Power Reactors,” the power reactor industry’s first cybersecurity guidance. Licensees subsequently agreed to voluntarily implement cybersecurity programs by 2008 that comply with NEI 04-04.

- In 2006, the NRC issued RG 1.152, Revision 2. This RG provided the NRC's first guidance on protecting safety systems from cyber threats. The regulatory bases for the cybersecurity measures included in RG 1.152 are tied to provisions in 10 CFR Part 50 and the security orders discussed above. RG 1.152 added nine regulatory positions to incorporate cybersecurity guidance at each phase of the digital safety system lifecycle. The NRC staff developed the cybersecurity guidance in RG 1.152 based on NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," issued October 2004, and NEI 04-04.

- In 2009, the NRC issued 10 CFR 73.54, commonly referred to as the Cybersecurity Rule. The objective of the Cybersecurity Rule was to codify the NRC-issued security orders and insights gained from protecting NPPs from cyber threats.

- In January 2010, the NRC issued RG 5.71, Revision 0, "Cyber Security Programs for Nuclear Facilities," to provide guidance for complying with 10 CFR 73.54 and the protection of CDAs[4] defined under 10 CFR 73.54(a)(b) from cyberattack, up to and including the design-basis threats as defined in 10 CFR 73.1. RG 5.71, Revision 0, included the cybersecurity guidance originally provided in RG 1.152, Revision 2.

The focus of the Cybersecurity Rule and RG 5.71 is to protect CDAs from harm or deliberate actions that cause damage, disclosure of confidential information, and use by adversaries whose objective is to cause harm or risk to plant facilities' abilities to perform safety, important-to-safety, security, or emergency preparedness functions to protect public health and safety. Cybersecurity is achieved through the application of technical controls and administrative controls as well as physical security measures, all of which function to protect assets from malicious, or even unintentionally harmful, actions. Security improves the reliable operation of a system because of its blocking of malicious, harmful acts. However, security does not impact the wear and tear placed on a system by its normal operations, or its physical reliability, which is associated with its design, component selection, and fault tolerance.

The focus of the safety requirements in 10 CFR 50.55a(h) and of RG 1.152 is the safe and reliable operation of instrumentation and controls (I&C) systems. The term "reliability" is generally defined as a system's ability to consistently perform its intended or required function without degradation or failure. Reliability is often measured by the mean time between failures. This measurement usually excludes any failure caused by malicious actions; it is based on failures resulting from normal operations within the specified range of environmental conditions and parameters (e.g., response time, system load, operating temperature). Unlike security, reliability is concerned with performing CDAs' (systems') required functions, not protecting against malicious acts.

The issuance of RG 5.71 resulted in confusion regarding how it would be used alongside RG 1.152, Revision 2, as both RGs provide a method that licensees can use to address the cyber threats of a CDA. Furthermore, the references to cybersecurity measures included in RG 1.152, Revision 2, became duplicative when the NRC issued the Cybersecurity Rule and RG 5.71 for the following reasons:

[4] The digital assets that need to be protected under the Cybersecurity Rule are referred to in the CSP as critical digital assets (CDAs) or critical systems (CSs). CDA and CS are defined in Appendix B, "Glossary," to NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," issued April 2010.

- The NRC's safety and cybersecurity regulatory frameworks do not require performing a cybersecurity review as an element of the safety evaluation. Under the NRC's regulatory framework, a safety evaluation of a DI&C system is part of the licensing review. However, a cybersecurity review of a DI&C system is an inspection that is part of the ROP.

- The scopes of the systems and cybersecurity measures covered by 10 CFR 73.54 and RG 5.71 were broader than those covered by RG 1.152, Revision 2. Specifically, the Cybersecurity Rule and RG 5.71 cover security, emergency preparedness, and important-to-safety systems in addition to safety-related systems covered by RG 1.152, Revision 2.

- The breadth and depth of cybersecurity regulatory guidance provided in RG 5.71 comprehensively covers concerns and protections beyond those in RG 1.152, Revision 2.

To reduce confusion between safety and cybersecurity, the NRC issued RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," in July 2011, which accomplished the following:

- removed implications that, as part of a 10 CFR Part 50 licensing review, the NRC staff will evaluate a digital safety system during licensing for its ability to withstand cybersecurity events

- removed cybersecurity provisions covering the digital system's lifecycle beyond the factory acceptance testing (FAT) stage, since these evaluations are handled after the licensing review

- clarified language in the RG to provide guidance for a secure development and operational environment (SDOE) of digital safety systems to comply with portions of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 and IEEE Standard (Std) 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

RG 1.152, Revision 3, focuses on eliminating or minimizing errors that can reduce the reliable operation of safety-related DI&C systems or equipment by establishing the following two concepts for digital safety systems: a secure development environment and a secure operational environment. The concept of a secure development environment is focused on protecting the software development environment such that digital safety systems do not include unwanted, unneeded, and undocumented code. The concept of a secure operational environment provides design features and protective measures to ensure that the reliability of the digital safety system is not compromised by either undesirable behavior by connected systems or inadvertent access to the safety system. Neither of these concepts necessarily involves consideration of a malicious entity.

In July 2023, the NRC staff issued RG 1.152, Revision 4, "Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants," which endorses, with some exceptions and clarifications, IEEE Std 7-4.3.2-2016, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations." Clause 5.9, "Control of Access," of IEEE Std 7-4.3.2-2016 incorporates the SDOE criteria originally found in

RG 1.152, Revision 3. As such, RG 1.152, Revision 4, does not explicitly discuss SDOE criteria, as they are now endorsed through IEEE Std 7-4.3.2-2016.

2.2 Safety and Cybersecurity Regulatory Framework

For NPPs with construction permits issued between January 1, 1971, and May 13, 1999, 10 CFR 50.55a(h) requires protection systems to comply with IEEE Std 279-1968, “Proposed IEEE Criteria for Nuclear Power Plant Protection Systems”; IEEE Std 279-1971, “IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems”; or IEEE Std 603-1991 and the correction sheet dated January 30, 1995. The criteria in IEEE Std 603 provide functional and design criteria for a safety I&C system. Additionally, any change to an approved safety I&C system design outside the bounds of 10 CFR 50.59, “Changes, tests and experiments,” requires the licensee to request approval before implementing the design change. Over the past 30 years, the NRC staff has developed a process for reviewing these changes. Specifically, NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (SRP), Chapter 7, “Instrumentation and Controls,” and other associated guidance provide review guidance for these I&C design changes.

The 2009 Cybersecurity Rule (10 CFR 73.54) is high level and performance based. For licensing, the Cybersecurity Rule requires current operating nuclear power plant licensees to submit their CSPs to the NRC staff for review and approval. Once the NRC has reviewed and approved a licensee-submitted CSP, the CSP becomes a condition of the license. A licensee’s implementation of its cybersecurity program in accordance with its CSP is inspected under the ROP.

A licensee is required to submit an LAR[5] for NRC approval before altering its existing CSP if the change reduces the effectiveness of the licensee’s CSP. A design change to a CDA (or a DI&C system upgrade) may not necessitate a CSP-related LAR because licensees’ CSPs generally allow changes to CDAs. Therefore, a design change of a CDA alone would not lead necessarily to a CSP change. Regardless, a CDA design change (including a DI&C system upgrade) may be selected for inspection to ensure that the design change complies with the licensee’s CSP.

Recognizing the difference between and independence of the cybersecurity review and safety evaluation (as part of a licensing review), the NRC staff could perform independent cybersecurity audits alongside safety evaluations when a licensee submits an LAR to change or upgrade its existing DI&C safety system designs, even if the CSP is unchanged.

2.3 Safety-Security Interface Effort

The Advisory Committee on Reactor Safeguards (ACRS) has long recognized that digital safety system designs should incorporate hardware and software architectures capable of providing a cybersecurity defensive architecture to combat malicious cyber security threats. In a letter dated April 20, 2011 (Agencywide Documents Access and Management System Accession No. ML11101A013), the ACRS, which was reviewing RG 1.152, Revision 3, sent a memorandum to the NRC Executive Director for Operations with several recommendations associated with performing cybersecurity reviews as part of the staff’s licensing reviews. One of

[5] Criteria for determining whether a plant needs to request a license amendment before implementing a change are provided in 10 CFR 50.59.

the recommendations instructed the staff to update chapter 7 and Chapter 13, “Conduct of Operations,” of the SRP to formally require NRR and NSIR staff coordination of system design reviews based on RG 1.152, Revision 3, and RG 5.71, Revision 0.

In response to the ACRS recommendations, the Executive Director for Operations directed the staff to develop an interoffice instruction for performing safety and cybersecurity evaluations of a DI&C system upgrade. The staff developed a framework for the interoffice instructions that included NRR, Office of New Reactors, regional offices, and NSIR staff. This framework coordinated evaluations of new reactor applicants’ and operating reactor licensees’ proposed DI&C systems that performed safety-related and important-to-safety functions to comply with requirements under 10 CFR Parts 50, 52, and 73. Based on interactions with licensees regarding the timing of future DI&C upgrades, the staff prioritized development of this detailed interoffice instruction so that it could benefit from lessons learned from licensees’ initial implementation of their cybersecurity programs in accordance with their approved CSPs. By the end of 2017, all operating plant licensees had implemented their cybersecurity programs. In 2018, the staff issued DI&C-ISG-06, Revision 2, which included the interoffice coordination instructions between safety and cybersecurity evaluations.

DI&C-ISG-06, Revision 2, instructs the NRR I&C staff to communicate with the NSIR cybersecurity staff on any cybersecurity concerns or design features identified during evaluation of a DI&C system upgrade. The NRC staff also issued Inspection Procedure (IP) 52003, “Digital Instrumentation and Control Modification Inspection,” in 2021. IP 52003 is used for regional inspections of major DI&C modifications and includes inspection items for cybersecurity. Specifically, it includes inspection items to verify a licensee’s compliance with its cybersecurity commitments associated with a DI&C system update, as provided in its CSP.

Although the interim staff guidance (ISG) and IP provide guidance for interoffice interaction, they do not provide guidance for the staff on how to perform cybersecurity audits in parallel with the licensing review of a DI&C system upgrade. This guidance may be helpful to the staff for two main reasons. First, the staff has limited experience auditing DI&C system upgrades at operating facilities. Second, the cybersecurity controls in RG 5.71 and licensees’ CSPs are not arranged in an order that facilitates auditing throughout various stages of the lifecycle design. Instead, the cybersecurity controls are arranged in a manner that facilitates installed CDAs. As a result, the CSP cybersecurity controls that licensees have committed to address at each stage of the design are not identified for a DI&C upgrade lifecycle.

To facilitate cybersecurity audits alongside a licensing review of a DI&C system upgrade, the reviewers and inspectors would need to understand the cybersecurity regulatory and technical issues and controls associated with the DI&C system. Specifically, the reviewers and inspectors will need to understand (1) digital asset changes within the scope of the licensee’s CSP and (2) CSP cybersecurity controls that are associated with the DI&C system upgrade. These are both discussed in the following sections.

2.4 Digital Asset Changes within the Scope of the Licensees’ Cybersecurity Plans

Licensees’ CSPs and 10 CFR 50.54(p) provide requirements associated with any change to a CDA. A DI&C system upgrade is a change to a CDA or CS. Specifically, by incorporating Section 4.2.2, “Cyber Security Impact Analysis of Changes and Environment,” of NEI 08-09, Revision 6, into their CSPs, licensees commit to perform a security impact analysis (SIA) before making a change to a CDA (or CS) or its environment. The SIA is used to manage risk introduced to the licensees' established defense-in-depth protective strategies (DIDPS). Section 2.5, "Defense-in-Depth Protective Strategies," of this document contains additional information on the subject. Additionally, 10 CFR 50.54(p) prevents a licensee from making a change that would decrease the effectiveness of a cybersecurity program (i.e., the effectiveness of the licensees' established cybersecurity DIDPS) without prior NRC approval. If a change to a CDA or a CS, such as a control change or a design change (including a DI&C system upgrade), does not adversely affect the established DIDPS, then a licensee can make that change within the scope of its CSP. The impact of a change to a CDA or a CS is determined by the licensee's SIA.

Based on the impact to a licensee implemented DIDPS, a change to a CDA or CS can be grouped by the following three categories:

Category 1: Security Control Changes

A security control change (e.g., use of an alternate control) is a change to how a CSP cybersecurity control is addressed. An alternative security control of a CSP cybersecurity control is an example of a security control change. This change does not modify the CDA design or the CDA's existing interdependencies with other digital assets (including other CDAs), nor does it reduce the effectiveness of established DIDPS. Therefore, the revised control must provide at least the same level of protection as the controls being replaced or must mitigate all threat vectors the original control was intended to address.

NEI 08-09, Revision 6, Section 3.1.6, "Mitigation of Vulnerabilities and Application of Cyber Security Controls," provides licensees' commitments associated with such changes. Specifically, it states the licensee would do the following:

- Document the basis for revising the control.

- Perform and document an analysis of the CDA and revised control to confirm that the latter mitigates the threat/attack vector the original control is intended to protect against, or provides at least equal protection as the original control.

Category 2: Design Change

A design change (e.g., a DI&C upgrade) is any design modification to a CDA that could adversely impact the CDA being modified and any devices that have functional or connection relationships with the CDA being modified. However, a design change does not reduce the effectiveness of the established DIDPS by not reducing the effectiveness of DIDPS characteristics that are used or relied on to protect multiple CDAs. Such protective measures include the deterministic isolation provided by use of hardware, based on a one-way data diode and prohibition of wireless technology and other protective measures. This established isolation eliminates any direct (wired) attack pathways from external networks or devices and is relied on to develop the CSP cybersecurity controls by tailoring the security controls provided in NIST SP 800-53, dated August 2009, "Security and Privacy Controls for Information Systems and Organizations," issued September 2020, and NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security," dated September 29, 2008. In general, the categorization of a CDA change must carefully assess how the change affects the DIDPS characteristics. Most DI&C system upgrades involve a design change.

Category 3: Cybersecurity Plan Change

A CSP change is a change that modifies the DIDPS described in a licensee's CSP and reduces that CSP's effectiveness. NEI 08-09, Revision 6, states that the DIDPS is established by implementing defense-in-depth architecture and addresses the cybersecurity controls provided in Appendix D, "Technical Cyber Security Controls," and Appendix E, "Operational and Management Cyber Security Controls," to NEI 08-09. Therefore, any change to a CDA design, a network change, a protective configuration and condition, or an operation or a baseline control change, including elimination of a CSP cybersecurity control that modifies the DIDPS, is a CSP change if the change reduces the effectiveness of the licensee's CSP. Changes that modify the DIDPS include a change to the following:

- defense-in-depth network architecture
- fundamental bases used to tailor the CSP cybersecurity controls

For these changes, the licensee's SIA must include an assessment of risks caused by the change and impact to the effectiveness of its CSP. If the change reduces the effectiveness of the CSP, then the licensee would need to submit an LAR under 10 CFR 50.54(p).

2.5 Defense-in-Depth Protective Strategies

Under 10 CFR 73.54(c)(2), licensees' cybersecurity programs must be designed to apply and maintain DIDPS to ensure the capability to detect, respond to, and recover from cyberattacks. This requirement ensures that a failure of a single protective strategy or security control would not result in the compromise of a Safety, Security, and Emergency Preparedness (SSEP) function. To comply with this requirement, licensees have committed to section 3.1.6 of NEI 08-09, which states that DIDPS is established by documenting and implementing the following:

- defensive strategy described in Section 4.3, "Defense-in-Depth Protective Strategies," of NEI 08-09

- technical CSP cybersecurity controls in Appendix D to NEI 08-09, Revision 6, consistent with the process described below

- operational and management cybersecurity controls in Appendix E to NEI 08-09, Revision 6, consistent with the process described below

Additionally, section 4.3 of NEI 08-09 explains that licensees implement, document, and maintain the DIDPS of their cybersecurity programs to ensure they have the capability to detect, delay, respond to, and recover from cyberattacks on CDAs. This section of NEI 08-09 also explains that the DIDPS of a plant describes the plant's defensive security architecture; the protective controls associated within each security level; implementation of CSP cybersecurity controls, in accordance with section 3.1 of its CSP; the implemented defense-in-depth measures described in NEI 08-09; the Appendix E, section 6, CSP cybersecurity controls; and maintenance of the cybersecurity program, in accordance with section 4 of the CSP.

A change that modifies the elements of a DIDPS would impact a number of CDAs because protections or protective conditions provided by elements of DIDPS are inherited or used by the CDAs to ensure that the CDAs are protected from cyber threats. Therefore, the SIA of a change should include an evaluation of whether the proposed change modifies the established DIDPS. If the proposed change modifies (or adversely impacts) an established DIDPS, the change may require an amendment to the licensee's CSP. In accordance with 10 CFR 50.54(p), a licensee may need to submit an LAR if the proposed change decreases the effectiveness of its established cybersecurity DIDPS.

2.5.1 Security Impact Analysis

The configurations of DAs within a facility and their environment are continually changing to increase efficiencies or reliability of the functions performed by the DA. Because a change to a CDA (e.g., a DI&C system upgrade) or its environment exposes the facility to cyberattacks and could adversely impact the CDA and prevent it from properly performing its functions, the potential cybersecurity risks resulting from the change must be managed to maintain the facility's established cybersecurity posture. An assessment that identifies potential cybersecurity risks of a change to CDA or its environment so that the risks can be managed is called an SIA.

Specifically, an SIA is a systematic process used to assess the potential effects of various security threats on an organization's operations. An SIA is performed before any changes are made to a DA. This analysis enables people involved with DI&C upgrades to prioritize risks based on their potential impact and develop tailored, effective mitigation strategies. Data (information) obtained from this analysis provides critical input that a security by design process would use to integrate security measures at the initial stages of design and development of systems, processes, or products. It emphasizes the incorporation of security features as inherent elements, not as afterthoughts or add-ons.

The following NIST documents state that an SIA is the analysis conducted by qualified staff within an organization to determine the extent to which changes to the system affect the security posture of the system:

- NIST SP 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” issued May 2004

- NIST SP 800-30, Revision 1, “Guide for Conducting Risk Assessments,” issued September 2011

- NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View,” issued March 2011

- NIST SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems,” issued August 2011

- NIST SP 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations,” issued September 2020

- NIST SP 800-18, Revision 1, “Guide for Developing Security Plans for Federal Information Systems,” dated February 24, 2006

NIST SP 800-128 states that an SIA is one of the most critical steps in the configuration change control process with respect to configuration management. The purpose of an SIA is to analyze the potential security impact of a proposed change, if implemented. Specifically, an SIA is used to answer the question of whether a proposed change could expose the facility to cyber threats and adversely impact the important digital assets (or CDAs) to prevent them from properly performing their function(s). The objective of performing an SIA is to manage risks introduced or increased by the proposed change. Thus, an SIA is performed before the change is approved and implemented. Once a change is implemented and tested, operation and maintenance of the implemented licensees' cybersecurity programs ensure that (1) the change has been implemented as approved, and (2) the baseline security controls provided in their CSPs are addressed and the implemented security controls are continuously effective in protecting the CDA.

To achieve the objective of the SIA, the changes are examined for impact on the established security postures of protected DAs (or CDAs), and for mitigating controls that can be implemented to reduce any resulting vulnerability to manage the risks associated with the change. Through SIA, assessors need to identify and understand direct and indirect functional and communication interdependencies (relationships) between the CDA being revised and other assets associated with the CDA. Additionally, assessors need to identify and understand the spatial relationship between the CDA and its environment. These interdependencies are established by data or information linkages or flows (e.g., direct wired or wireless connection and sneaker network connections) between the CDA and other assets associated with it. For this reason, NIST's definition of an SIA states that it is performed by qualified individuals. For an NPP, qualified individuals are those who have working knowledge in the following areas necessary in performing SIAs: a plant's information and digital system technology, operations, engineering, nuclear safety, physical security, cybersecurity, and emergency preparedness. For NPPs, qualified individuals are the plant's cybersecurity assessment team.

To minimize the cybersecurity risks introduced by a change, SIAs are conducted by qualified individuals throughout the following phases of a software development lifecycle:

- For the Initiation Phase (before a change is deployed), the SIA is performed to determine whether the change will impact the secure state of the system before a change is deployed. The SIA is performed as part of a protected DA (CDA) functional requirements assessment. As engineers define a protected DA's (CDA's) functions, data flow, and storage, the result of the SIA of the protected DA (CDA) identifies the most cost-effective way to manage the potential risks caused by the change. The management of the potential risks includes designing in engineering cybersecurity mitigation solution(s) to the protected DA (CDA) or mitigating measures external to the DA (CDA). This minimizes efforts to rebuild, retest, and re-rollout a design change after the design is completed or a change is deployed. The protected DA (CDA) requirements developed from this process are used to engage with vendors to acquire the protected DAs (CDAs).

- For the Requirements[6]/Development/Acquisition and Implementation/Assessment Phases, an SIA needs to be performed as the protected DA (CDA) is

[6] Any requirements needed for the system developer to implement technical security controls (such as access controls, audit logs, hardening) should be identified and included as part of the DI&C system upgrade requirements that are provided to the vendor. These security controls should be verified (e.g., tested) by the licensee before installation.

developed/acquired and implemented. The reason is that the way the change will be built and implemented may not be the same as the change proposed and reviewed at the initial phase. These differences can greatly influence the cybersecurity risks of the change. For example, for a custom-built component during the design phase, an SIA is performed on technical design documents to ensure that the design considers security best practices, implements the appropriate controls, and would not need to be redeveloped later due to introduced vulnerabilities. Therefore, an SIA is performed as new information is obtained. The result of the SIA is used to ensure that security is considered as a developer builds the component or the component is acquired, and the design is tested during implementation to confirm that expected controls were implemented and that no new or unexpected vulnerabilities were introduced.

- For the Operations and Maintenance Phase (after a change is deployed), an SIA in this phase confirms that the original SIA was correct, and that unexpected vulnerabilities or impacts to security controls not identified in the testing environment have not been introduced in the operational environment. Additionally, the security impact of unscheduled and unauthorized changes is analyzed during the operation and maintenance phase.

The SIA process provided in NIST SP 800-128 consists of the following steps:

(1) The first step is to understand the change and prepare for the analysis by understanding the overview of the architecture of the change and how it will be implemented. This includes identifying (1) the objectives of the change, (2) the method (including process and technology) used to achieve the objectives, (3) the affected assets, including the network architecture associated with the CDA being changed (interdependent assets), (4) the operating and maintenance procedures, and (5) the current security measures that protect the CDA.

(2) The second step is to identify potential vulnerabilities associated with the changed CDA with the objective of identifying those that can be used to attack the CDA being changed. If the change is related to the implementation of a new commercial off-the-shelf product, the identification may be limited to the search for known vulnerabilities by searching the National Vulnerability Database and performing a vulnerability scan. Even if the change involves the implementation of a CDA update that is custom developed by a vendor, the change is analyzed to identify any potential vulnerabilities of the custom-designed CDA. For such a CDA, the assessor may have more information about the CDA and will be able to perform a more detailed assessment than for commercial off-the-shelf CDAs.

(3) The third step is to perform assessments of the risk of the vulnerabilities identified in the second step. The objective of this step is to determine whether the vulnerabilities identified in the second step should be mitigated before the proposed change is implemented. Addendum 5 of NEI 08-09 contains additional guidance on performing this assessment.

(4) The fourth step is to assess and determine whether and how the proposed change will impact the existing DIDPS, which includes CSP cybersecurity controls and network isolation. For example, the proposed change may involve the installation of software or new technology that alters the existing baseline configuration used to develop the CSP cybersecurity controls or implemented CSP cybersecurity controls. The change may also affect other assets associated with the CDA being revised.

(5) The fifth step is to identify countermeasures to mitigate the identified vulnerabilities to manage the risks. If vulnerabilities have been identified and it has been determined that these vulnerabilities can be exploited to compromise the CDA being revised or associated assets, the countermeasures (existing and newly added to the CDAs) are identified to mitigate the potential risks caused by the identified vulnerabilities. In general, the security controls that are implemented and executed by the CDA through mechanisms contained in the hardware, software, or firmware components of the CDA are most effective against the identified vulnerabilities of a CDA. When engaging with vendors for DI&C systems upgrade, licensees need to incorporate these security controls into the overall system's design requirements.

NIST SP 800-128 states that an SIA supports the implementation of NIST SP 800-53, control CM-4, "Security Impact Analysis." The NRC tailored the NIST SP 800-53 CM-4 control for NPPs, as provided in Section 4.2.2, "Security Impact Analysis," of RG 5.71. Specifically, RG 5.71 states the following:

> The security impact analysis assists in managing potential vulnerabilities, weaknesses, and risks introduced by changes in the system, network, environment, or emerging threats. Section 4.2.2 of Appendix A to this guide includes a template for licensees to perform a security impact analysis before making a design or configuration change to a CDA or when changes to the environment occur.

2.5.2 Timing of Performing Security Impact Analysis

In accordance with Section 4.2.2 of NEI 08-09, Revision 6, licensees committed to perform SIAs before implementation of a change to a CDA and its environment. However, NEI 08-09 (CSP) does not specifically state when before implementation of a change that the SIA is to be performed. RG 5.71 provides guidance that an SIA of a CDA change starts from the concept phase of the development lifecycle provided in RG 1.152, Revision 2. Although the current revision of RG 1.152 is Revision 4, Revision 2 is referenced in RG 5.71, Revision 0, for managing the configuration changes of a CDA. RG 1.152, Revision 2, provides guidance that an SIA for a DI&C system (which is a CDA) change is performed from the conceptual phase of the CDA development lifecycle. To understand how RG 1.152 provides guidance for when an SIA of a CDA change is performed, knowledge of the historical relationship between RG 1.152, RG 5.71, and NEI 08-09 is helpful, as discussed below.

With the increased concern about the potential for cyberattacks and the terrorist attack on September 11, 2001, the NRC recognized that the DI&C systems that perform safety functions need to be protected from cyber threats to maintain the reliable operation of plants' safety functions. However, the NRC did not have any regulations for protecting these DI&C systems from cyber threats. Therefore, in February 2002, the NRC issued NRC Order EA-02-026 to address the threat environment at the time. Additionally, at the same time, the NRC initiated a cybersecurity study at four NPPs to develop a method that licensees can use to manage cybersecurity risks at their facilities. The NRC published the study results in NUREG/CR-6847. Based on this report and insights gained during the study, NEI developed NEI 04-04 to provide nuclear power reactor licensees with a means to develop and maintain a cybersecurity program at their sites. The NRC staff evaluated the NEI submittal and, in a letter dated December 23, 2005, informed NEI that NEI 04-04, Revision 1, is acceptable for use to manage cybersecurity risks at the time.

In 2006, when the NRC issued RG 1.152, Revision 2, to endorse IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems Nuclear Power Generating Stations,” the NRC added regulatory positions regarding the need to protect DI&C systems from cyber threats because IEEE Standard 7-4.3.2-2003 did not offer guidance associated with protecting digital systems from cyber threats. The regulatory positions provided in RG 1.152, Revision 1, Part C, sections 2.1–2.9 cover the following phases of the waterfall lifecycle framework:

(2.1) Concepts
(2.2) Requirements
(2.3) Design
(2.4) Implementation
(2.5) Test
(2.6) Installation, checkout, and acceptance testing
(2.7) Operation
(2.8) Maintenance
(2.9) Retirement

For each lifecycle phase of a DI&C system, RG 1.152, Revision 2, includes a regulatory position that provides guidance for protection against threats of cyberattack.

RG 1.152, Revision 2, provided the industry regulatory guidance on protecting DI&C systems from cyber threats until the NRC issued its Cybersecurity Rule (10 CFR 73.54) in 2009. Shortly after publishing the Cybersecurity Rule, the NRC issued RG 5.71, Revision 0, which provided guidance for complying with 10 CFR 73.54. This RG was developed based on the following:

- insights and knowledge gained from the study, reviewing NEI 04-04

- regulatory positions associated with cybersecurity provided in RG 1.152, Revision 2

- tailoring the “high-impact” CSP cybersecurity controls described in NIST SP 800-53 and NIST SP 800-82

For this reason, RG 5.71 references RG 1.152, Revision 2; for example, Section C.2, “Elements of a Cyber Security Plan,” states that one way to comply with 10 CFR 73.54(d)(3) is by ensuring the following:

- Modifications to plant assets and the addition of new equipment do not adversely impact cybersecurity.

- Cybersecurity issues are addressed throughout the system design lifecycle phases.

RG 1.152, Revision 2, provides additional guidance for the design and development process of safety systems.

In accordance with 10 CFR 73.54(d)(3), licensees must ensure that modifications to CDAs are evaluated before implementation to ensure that the cybersecurity performance objectives identified in 10 CFR 73.54(a)(1) are maintained. Additionally, Section 3.3.3.1, “Systems and Service Acquisition,” of RG 5.71 states that for safety systems (or DI&C system upgrades), Part C, “Regulatory Position,” sections 2.1–2.6, of RG 1.152, Revision 2, provide additional guidance on addressing cybersecurity when replacing DI&C systems. The regulatory positions provided in RG 1.152, Revision 2, Part C, sections 2.1–2.6, cover the concepts, requirements, design, implementation, test, installation, checkout, and acceptance testing phases of a CDA's lifecycle.

Based on the above, an SIA of a DI&C upgrade is initiated at the conceptual phase of the software development lifecycle described in the regulatory positions of RG 1.152. In addition, this conclusion is supported by the following:

- RG 5.71 provides a method that licensees can use to comply with the Cybersecurity Rule (10 CFR 73.54). Since the Cybersecurity Rule requires licensees to submit their CSPs for the NRC's review and approval, RG 5.71 provides a method that licensees can use to comply with the commitments provided in their CSPs.

- RG 5.71 references the regulatory positions provided in RG 1.152, Revision 2, to provide regulatory guidance on when an SIA of a CDA upgrade is performed.

2.6 Licensee's Commitments Associated with a Change

As mentioned above, licensees committed in Section 4.2.2 of NEI 08-09 to perform an SIA to manage risks introduced by a change to a CDA or its environment. As part of an SIA, licensees have committed to ensuring that their cybersecurity assessment team will perform actions described in table 1.

Table 1 CSP Commitments Associated with a Change

Confirm the location of the DI&C system: • Perform, where practical, a physical inspection of the connections and configuration of a DI&C system, including tracing communication connections into and out of the DI&C system to termination points along communication pathways. • Examine the physical security established to protect DI&C system and the system's communication pathways.
Confirm direct and indirect connectivity pathways between the DI&C system and other assets: • Examine and validate that the description of the DI&C system's data flow (direct and indirect) is complete and correct. • Verify that electronic validation is performed when physical walkdown inspections are impractical to trace a communication pathway to its conclusion. When there is a risk of operational disruption, electronic validation tests are conducted during periods of scheduled outage. Where used, a justification of the adequacy of the electronic validation technique is documented.

Confirm infrastructure interdependencies between the DI&C system and other assets:

- Examine and validate that the identified interdependencies with other DAs (including CDAs) and trust relationships between other assets and the DI&C system are complete and correct.

- Examine and verify that the interdependencies with infrastructure support systems, including electrical power, environmental controls, and fire suppression equipment that, if compromised, could adversely impact the proper functioning of the DI&C system, are complete, documented, and correct.

Review any DI&C system assessment documentation:

- Examine and verify that the configuration information of the DI&C system is complete and correct.

- Assess and validate the CSP cybersecurity controls (e.g., firewalls, intrusion detection systems, data diodes) along the communication pathways are complete and effective.

- Verify that the DI&C system cybersecurity exposures, including specific attack/threat vectors to be assessed for mitigation using the method in section 3.1.6 of NEI 08-09 are complete and documented. Additionally, verify that attack/threat vectors associated with interdependencies and other information collected from this process are examined and correctly addressed.

- Examine and verify that the physical security established to protect the DI&C system and its communication pathways is complete and applicable to the DI&C system.

Review the defensive strategies:

- Examine and confirm the implementation of plantwide physical and cybersecurity policies and procedures that secure the DI&C system from a cyberattack, including attack mitigation and incident response and recovery.

- Examine and verify that the CSP cybersecurity controls of the DI&C system are complete and addressed properly.

- Examine and verify that the CSP cybersecurity controls of the CDA are addressed.

- Examine and verify that the implementation of plantwide physical and cybersecurity policies and procedures that secure the DI&C system from a cyberattack, including attack mitigation and incident response and recovery, are in place and effectively performing their functions.

Review the defensive models:

- Confirm that the defensive model of the plant is still in place and effective.

Confirm the qualification of the staff members:

- Assess and verify that any staff members working with the DI&C system are trained to a level of cybersecurity knowledge commensurate with their assigned responsibilities.

Resolve information and configuration discrepancies identified during tabletop reviews:

- Resolve the presence of undocumented and missing connections, and other cybersecurity-related irregularities associated with the CDA. Document information and configuration discrepancies identified during the tabletop reviews and walkdowns, including the presence of undocumented and missing connections, and other cybersecurity-related irregularities associated with the CDA, for remediation in the corrective action program.

Note:

An evaluation of interdependency includes analysis to identify any direct and indirect functional, informational, or data dependency between the asset being revised and other assets. The objective of this interdependency evaluation is to identify and determine potential attack pathways and the potential exploit mechanism that allows an attacker to adversely impact plants' SSEP functions through compromising the CDA being revised and other assets that are interdependent with the CDA being revised. Most of the information collected for an interdependency evaluation performed for an SIA is the information needed for developing system's requirements for a DI&C system upgrade. The potential risks identified from an SIA of DI&C upgrade are addressed through the vendor using a design change or through shared controls (such as the protection provided by the facility). If the identified potential risks are addressed through design, the cybersecurity solutions for the potential risks are incorporated into the design requirements of the DI&C system upgrade. Therefore, the cybersecurity related issues identified during the change management process for a DI&C system upgrade are addressed within the change management process and therefore are not handled by a corrective action program. As explained above, addressing the cybersecurity issues during the design process is the most cost-efficient path.

Finally, the licensees have committed in their CSPs that any adverse conditions identified after the modification is implemented are entered into the site's corrective action program. Risks to SSEP functions, CDAs, and CSs are managed through ongoing evaluation of threats and vulnerabilities and by addressing threat and attack vectors associated with the CSP cybersecurity controls provided in appendices D and E to NEI 08-09, Revision 6, during the various phases of the lifecycle. Therefore, as the licensees collect and assess the information described in table 1, licensees should identify the potential risks introduced by a DI&C system upgrade and mitigate them.

2.7 DI&C-ISG-06 DI&C Licensing Process

The NRC staff's licensing criteria for reviews associated with I&C are documented in SRP chapter 7. On January 19, 2011, the NRC staff issued DI&C-ISG-06, Revision 1, "Task Working Group #6: Licensing Process," to provide specific guidance for the licensing review of safety-related DI&C equipment modifications. DI&C-ISG-06 references the SRP chapter 7 criteria as well as the guidance in several NRC RGs that endorse IEEE standards for the development of a high-quality system design. DI&C-ISG-06, Revision 1, was used from 2011 to 2018 to perform DI&C licensing reviews, as well as reviews of DI&C platform topical reports (TRs). DI&C-ISG-06, Revision 2, was issued in December 2018, and it incorporates the NRC staff's lessons learned and industry feedback from the use of Revision 1. Revision 2 improved the usability of the ISG and describes two licensing review processes: the traditional Tiered Review Process and the new Alternate Review Process.

2.7.1 Traditional Review Process: The Tiered Review Process

DI&C-ISG-06, Revision 1, introduced a graded approach for defining the scope of a review based on how an application references a previously approved TR for a DI&C platform. This graded approach is separated into tiers: Tier 1 is the review of an LAR that references a previously approved TR; Tier 2 is the review of an LAR that references a previously approved TR with deviations; and Tier 3 is the review of an LAR that does not reference a previously approved TR. Under this graded approach, a Tier 1 review is focused on the plant-specific aspects of the application and requires the least review effort, whereas a Tier 3 review requires the most effort because both the DI&C platform and plant-specific aspects are reviewed concurrently. Because of the tiered aspect of this traditional review process, they are collectively referred to as the Tiers 1, 2, and 3 Process, or the Tiered Review Process.

The Tiered Review Process was streamlined in Revision 2 of DI&C-ISG-06 to focus the evaluation on the licensee's implemented high-quality lifecycle design for the DI&C safety system. This includes the system design, implementation, and testing stages of the design. The NRC had traditionally issued DI&C license amendments for operating reactors only after completion of the system implementation and testing lifecycle phases (see figure 1).

The Tiered Review Process is based on the review of the LAR—which is submitted early in the design—and a later LAR supplement or Phase 2 submittal containing the completed design, implementation, and test information.

NRC inspections associated with the Tiered Review Process cover activities after the FAT, which include the site acceptance test (SAT) and site installation.

2.7.2 New Licensing Process: The Alternate Review Process

DI&C-ISG-06, Revision 2, introduced the Alternate Review Process (ARP), which allows for earlier issuance of a license amendment, typically before completion of the system implementation and testing lifecycle phases. Under this process, the NRC staff focuses its review on the system design and development process to support a determination that the design meets regulatory requirements, and that the development process is of sufficiently high quality to produce systems, software, and hardware suitable for use in a safety-critical application. Under the ARP, the final system implementation and testing (e.g., FAT) will be subject to verification through NRC inspection processes, in addition to the site inspections that will take place after FAT. The staff also performs inspections of the licensee's vendor oversight activities, as described in their vendor oversight plan (VOP).

Figure 1 shows a timeline representation of both the Tiered Review Process and the ARP, as well as some of the key characteristics for each process. The figure depicts when licensing review and inspection activities for each process take place in relation to the licensee and vendor lifecycle activities. Note that the timeline is not to scale and does not represent the actual duration of these activities.

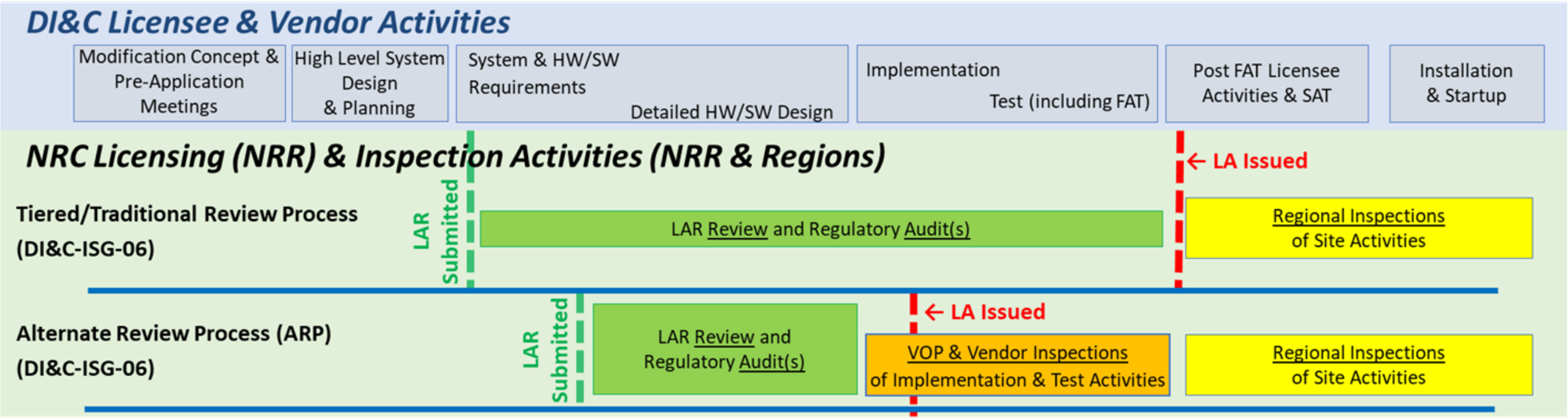

DI&C Licensee & Vendor Activities
Modification Concept & Pre-Application Meetings
High Level System Design & Planning
System & HW/SW Requirements
Detailed HW/SW Design
Implementation
Test (including FAT)
Post FAT Licensee Activities & SAT
Installation & Startup
NRC Licensing (NRR) & Inspection Activities (NRR & Regions)
Tiered/Traditional Review Process (DI&C-ISG-06)
LAR Submitted
LAR Review and Regulatory Audit(s)
← LA Issued
Regional Inspections of Site Activities
Alternate Review Process (ARP) (DI&C-ISG-06)
LAR Submitted
LAR Review and Regulatory Audit(s)
← LA Issued
VOP & Vendor Inspections of Implementation & Test Activities
Regional Inspections of Site Activities

Figure 1 DI&C-ISG-06 Tiered Review Process and ARP

2.8 Engagement with Licensees and Vendors for a DI&C System Upgrade

Licensees' DI&C system upgrade process can be divided into the following activities:

- modification concept and preapplication meetings
- high-level system design and planning
- system and hardware (HW)/software (SW) requirements
- detailed HW/SW design
- implementation test (including FAT)
- post-FAT licensee activities and SAT

> **Note:**
> The above DI&C system upgrade activities descriptions are based on the licensing process described in DI&C-ISG-06, Revision 2.
>
> The above activities map to the following lifecycle phases provided in RG 1.152, Revision 2, that are referenced in RG 5.71, Revision 0:
>
> (1) concepts:
> - modification concept and preapplication meetings
> - high-level system design and planning
>
> (2) requirements:
> - system and HW/SW requirements
>
> (3) design:
> - detailed HW/SW design
>
> (4) implementation + (5) test
> - implementation test (including FAT)
>
> All other lifecycle phases provided in RG 1.152 fall under the post-FAT licensee's activities and SAT.

As explained in earlier sections of this report, licensees have committed in their CSPs to address certain CSP cybersecurity controls during these activities. These security controls include an SIA and configuration management. For these DI&C system upgrades, licensees submit an LAR, and the NRC staff performs a licensing review of the submitted LAR using the guidance provided in DI&C-ISG-06, Revision 2, and in SRP chapter 7.

Based on DI&C-ISG-06 and the SRP, the NRC staff's engagements with licensees on their DI&C upgrade can generally be divided into the following three categories:

- pre-LAR submittal
- LAR review
- post-LAR site inspections

The pre-LAR submittal activities that involve NRC staff engagement depend on the LAR review process. Although licensees may inform the NRC of their preferred review process, the NRC selects the licensing process to be used for reviewing licensee submitted LARs based in part on the information provided to support the application. For example, if the traditional review process is used, the NRC staff's pre-LAR submittal engagements with licensees may cover "Modification Concept" and "High-Level System Design & Planning." However, if the ARP is used, the NRC staff's pre-LAR submittal engagements with licensees may cover "Modification Concept," "High-Level System Design & Planning," and some discussion on the "System & HW/SW Requirements." For these presubmittal engagements, the NRC's cybersecurity staff can be engaged alongside the technical staff to perform cybersecurity reviews (audits) to ensure that cybersecurity commitments provided in licensees' CSPs that are associated with the DI&C upgrade activities discussed above are performed and documented. For pre-LAR submittal engagements, licensees have committed in their CSPs to perform an SIA and identify the cybersecurity requirements for the proposed DI&C system upgrade. The cybersecurity requirements are incorporated into overall DI&C system upgrade requirements for engagements with potential vendors or the vendor for the DI&C system upgrade.

For LAR review engagements, the NRC DI&C reviewers performing the licensing review engage with the licensee and the DI&C system upgrade vendors to ensure that DI&C system upgrades meet regulatory requirements. The purpose of the cybersecurity review performed in parallel with the licensing review engagements would be to ensure that the upgrade obtained from the vendors is secure. Specifically, the objective of the cybersecurity staff engaging with vendors is to ensure that licensees obtain a DI&C system that met the following criteria based on their SIA:

- implemented security capabilities to mitigate applicable attack vectors

- implemented only the functional capabilities to meet the requirements of the DI&C without unnecessary functions

- were developed securely

For "Post-LAR Review" engagements, the NRC regional inspectors and cybersecurity staff perform independent site inspections in accordance with the ROP.

Figure 2 maps independent cybersecurity activities to the LAR review process and the activities of licensees and their vendors associated with digital I&C system upgrades. Three cybersecurity engagements can be performed alongside the current LAR review process, and they are shown in the long pink rectangular box. The three individual pink boxes at the bottom of figure 2 provide the focus of each engagement in the long rectangular pink box.

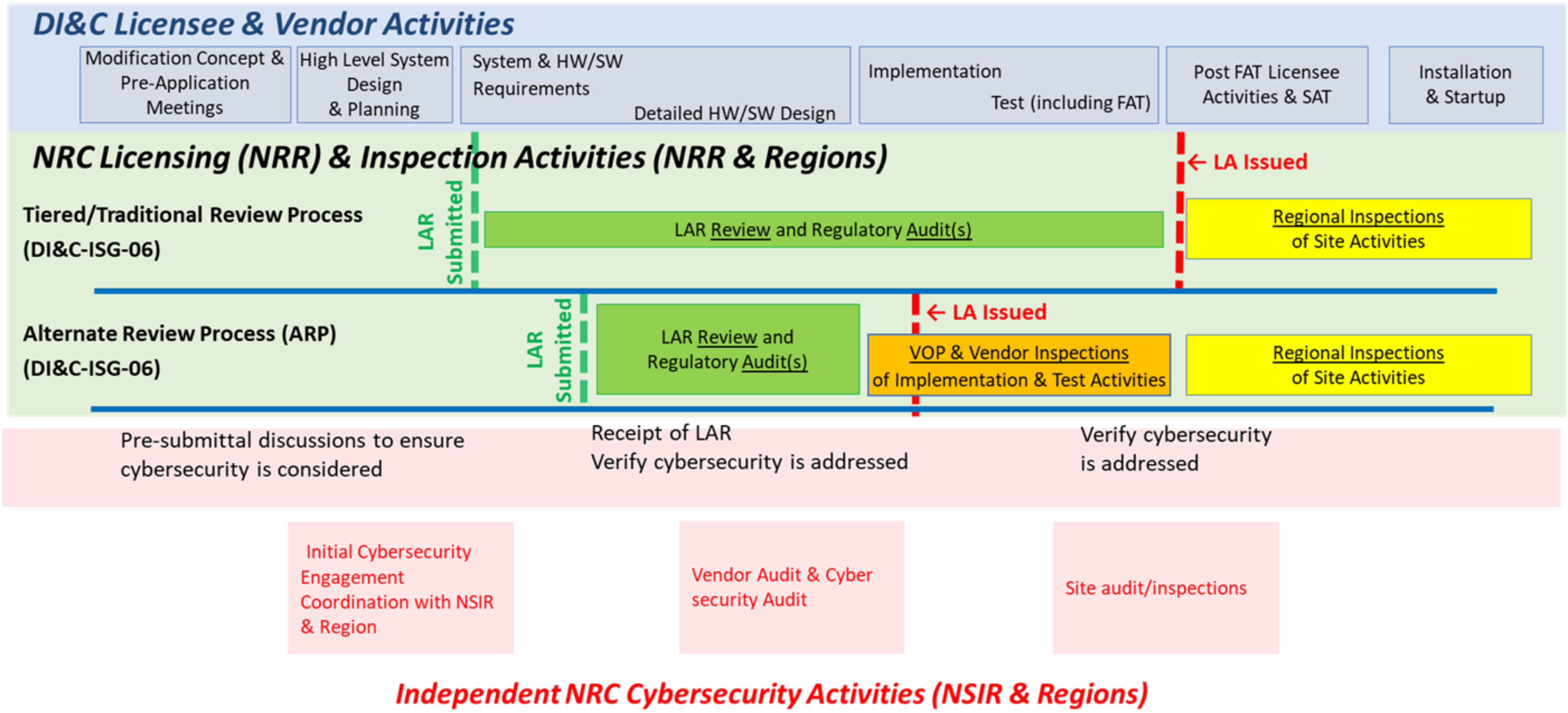

DI&C Licensee & Vendor Activities
Modification Concept & Pre-Application Meetings
High Level System Design & Planning
System & HW/SW Requirements
Detailed HW/SW Design
Implementation
Test (including FAT)
Post FAT Licensee Activities & SAT
Installation & Startup
NRC Licensing (NRR) & Inspection Activities (NRR & Regions)
← LA Issued
Tiered/Traditional Review Process
(DI&C-ISG-06)
LAR Submitted
LAR Review and Regulatory Audit(s)
Regional Inspections of Site Activities
← LA Issued
Alternate Review Process (ARP)
(DI&C-ISG-06)
LAR Submitted
LAR Review and Regulatory Audit(s)
VOP & Vendor Inspections of Implementation & Test Activities
Regional Inspections of Site Activities
Pre-submittal discussions to ensure cybersecurity is considered
Receipt of LAR
Verify cybersecurity is addressed
Verify cybersecurity is addressed
Initial Cybersecurity Engagement Coordination with NSIR & Region
Vendor Audit & Cyber security Audit
Site audit/inspections
Independent NRC Cybersecurity Activities (NSIR & Regions)

Figure 2 DI&C system upgrade—focus of cybersecurity activities associated with licensee and vendor activities

2.9 Cybersecurity Audits of Licensees and Vendors

The licensee's CSP describes the complete DI&C system's security lifecycle and provides comprehensive requirements for each security lifecycle phase. As discussed above, the security controls provided in the licensees' CSPs are arranged neither in the sequential order of the lifecycle phases of a CDA nor into the licensees' and vendors' activities associated with a DI&C upgrades. Thus, the security controls provided in the licensees' CSPs (NEI 08-09, Revision 6) were examined as part of this research effort to identify the CSP cybersecurity controls associated with the licensees' and vendors' activities for a DI&C system upgrade. The licensees' CSPs and RG 5.71 divide the security controls into two categories: technical controls[7] and the management and operational security controls.[8] For this section, if guidance (or interpretation) was needed to identify the security controls associated with the DI&C system upgrade, the regulatory guidance provided in RG 5.71, Revisions 0 and 1, was used. Table 2 summarizes the identified security controls that map to the licensee and vendor activities.

[7] Technical controls are safeguards or protective measures that are executed through nonhuman mechanisms contained within the hardware, firmware, operating systems, or application software. See Section 3.3.1 "Technical Controls," of RG 5.71 and Section 2, "Cyber Security Plan Preparation," of NEI 08-09, Revision 6.

[8] Management and operational CSP cybersecurity controls are safeguards or protective measures that are executed through policies, procedures, and programs, including cybersecurity enhancing activities in policies, implementing procedures, and processes such as engineering lifecycle activities, engineering procurement procedures, software quality assurance programs, and ensuring procurement contracts specify cybersecurity requirements. See section 2 of NEI 08-09, Revision 6.

Table 2 Mapping of CSP Cybersecurity Controls to Licensee and Vendor Activities

	Security Controls (NEI 08-09)
Modification Concept & Preapplication Meetings **High-Level System Design & Planning**	**Appendix E, Section 10.5,** “Security Impact Analysis.” (Additional guidance on these sections is provided in RG 5.71, Section C.2, “Elements of a Cyber Security Plan”; RG 5.71, Section C.1.3, “Identification of Critical Digital Assets”; Section C.3.3.3.1, “System and Service Acquisition”; and Section 2.6 of RG 1.152, Revision 2.)
System & HW/SW Requirements	**Licensee’s engagement with its vendor (requirements)** Appendix D. 1.6 Least Privilege Appendix D. 2.2 Auditable Events Appendix D. 2.3 Content of Audit Records Appendix D. 2.4 Audit Storage Capacity Appendix D. 2.6 Audit Review, Analysis, and Reporting Appendix D. 2.9 Protection of Audit Information Appendix D. 5 System Hardening Appendix E. 3.2 Flaw Remediation Appendix E. 10.9 Component Inventory Appendix E. 11 System and Services Acquisition • 11.1 System and Services Acquisition Policy and Procedures • 11.2 Supply Chain Protection • 11.3 Trustworthiness • 11.4 Integration of Security Capabilities
Detailed HW/SW Design Implementation Test (including FAT)	Appendix D 11.5 Developer Security Testing
Post-FAT Licensee Activities and SAT	Appendix E. 11.5 Developer Security Testing Appendix E. 11.6 Licensee Testing All other CSP cybersecurity controls. The DI&C system update needs to comply with the licensee’s CSP and is subject to the NRC’s ROP, including inspections.

Notes:

1. This table shows only those security controls that are applicable to a DI&C system upgrade.

2. The technical security controls are most effective if they are designed into a device or system. If possible, the technical security controls (cybersecurity features) that can address any cybersecurity concern of a DI&C system upgrade should be incorporated into the system requirements. Licensees identify these technical controls through their SIA for a DI&C system upgrade.

3. Certain security controls, such as audit features and cryptography, cannot be implemented adequately unless the controls are supported on the device. Throughout the SIA and the requirements phase, the licensee should clearly be able to map out which security controls will be implemented by the vendors, including the appropriate requirements to be transmitted to the vendors. The licensee should also be able to

map out which controls will be implemented in the operational environment or plant procedures. The licensee should verify adequate vendor implementation of the security requirements before transitioning the DI&C system to an operational state.

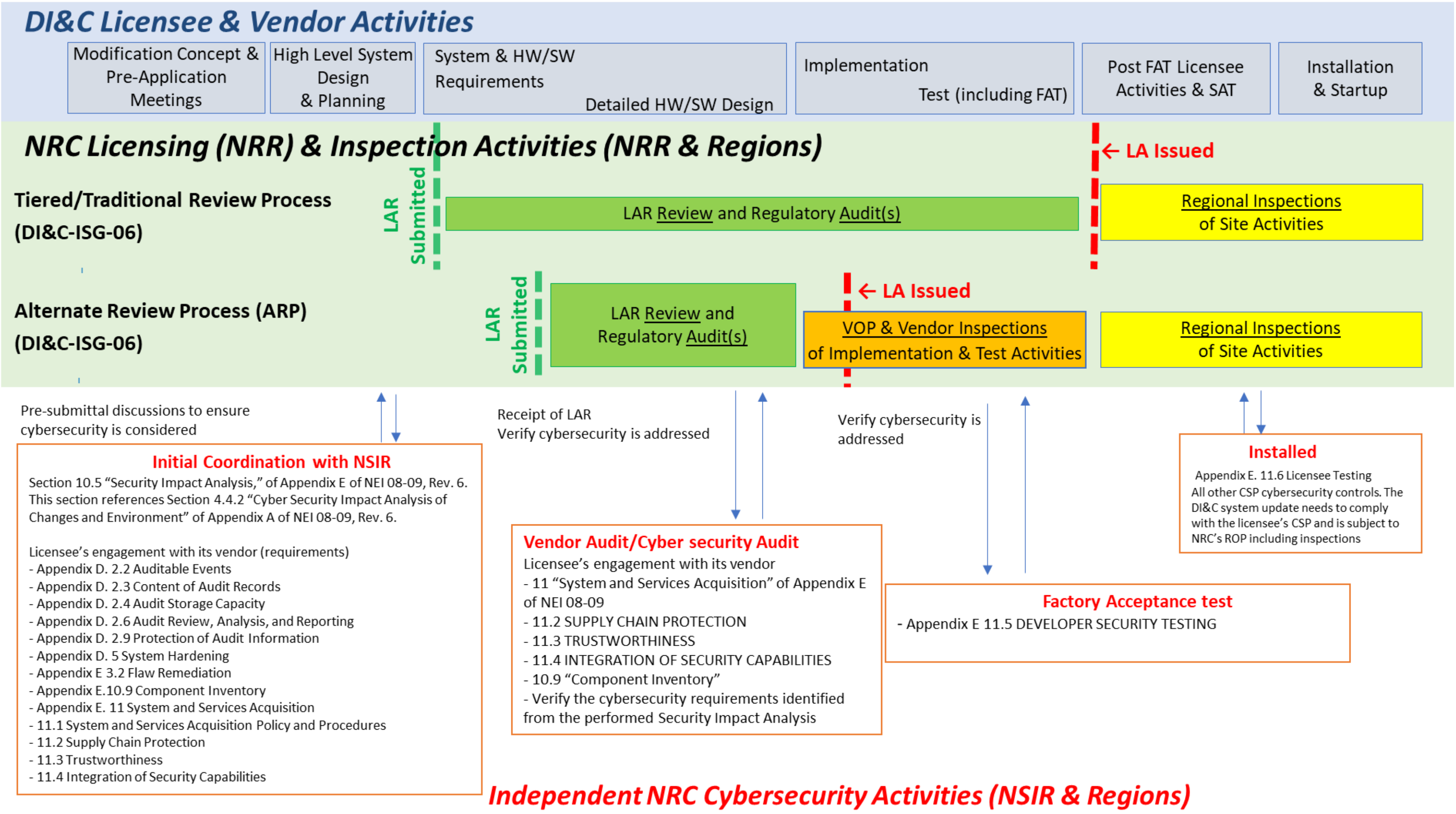
4. The security controls that reduce the attack surface of the DI&C upgrade system should be considered. These controls include, but are not limited to, the following:

   - Section 5, “System Hardening,” of appendix D to NEI 08-09, Revision 6
   - Section 10.8, “Least Functionality,” of appendix E to NEI 08-09, Revision 6

To reduce regulatory uncertainty associated with the cybersecurity of a DI&C system upgrade, licensees should address the security controls as they perform the activities listed in table 3 and document how they have addressed the security controls. Additionally, the NRC staff (regional inspectors and headquarters (NSIR) staff) should take the opportunity to engage with the licensees in parallel with (or during) the equivalent licensing review engagements related to the DI&C system upgrade.

By identifying potential cybersecurity issues associated with a DI&C system upgrade during the early phase of licensee and vendor activities, licensees can address issues in a more efficient and effective manner. At early phases of a DI&C system upgrade, licensees can work with a vendor to minimize the attack surface of the DI&C system or to add security features to address any issues. If this is not possible, licensees should work with their plant staff to identify any licensee programs and physical and logical access control measure(s) that can be applied to provide reasonable assurance that only an authorized individual could access and modify the updated system. If the cybersecurity issues are not addressed early, then licensees may be faced with redesigning the system if the cybersecurity requirements (or the cyber threats) are difficult to address using the facility’s programmatic measures or external security features.

Figure 3 adds the CSP cybersecurity controls that licensees should address when they perform DI&C system upgrades to the three pink boxes introduced in figure 2. Figure 3 also includes a white box to illustrate the requirements after the DI&C system is installed.



DI&C Licensee & Vendor Activities

Modification Concept & Pre-Application Meetings

High Level System Design & Planning

System & HW/SW Requirements

Detailed HW/SW Design

Implementation

Test (including FAT)

Post FAT Licensee Activities & SAT

Installation & Startup

NRC Licensing (NRR) & Inspection Activities (NRR & Regions)

Tiered/Traditional Review Process (DI&C-ISG-06)

LAR Submitted

LAR Review and Regulatory Audit(s)

← LA Issued

Regional Inspections of Site Activities

Alternate Review Process (ARP) (DI&C-ISG-06)

LAR Submitted

LAR Review and Regulatory Audit(s)

← LA Issued

VOP & Vendor Inspections of Implementation & Test Activities

Regional Inspections of Site Activities

Pre-submittal discussions to ensure cybersecurity is considered

Initial Coordination with NSIR

Section 10.5 "Security Impact Analysis," of Appendix E of NEI 08-09, Rev. 6. This section references Section 4.4.2 "Cyber Security Impact Analysis of Changes and Environment" of Appendix A of NEI 08-09, Rev. 6.

Licensee's engagement with its vendor (requirements)
- Appendix D. 2.2 Auditable Events
- Appendix D. 2.3 Content of Audit Records
- Appendix D. 2.4 Audit Storage Capacity
- Appendix D. 2.6 Audit Review, Analysis, and Reporting
- Appendix D. 2.9 Protection of Audit Information
- Appendix D. 5 System Hardening
- Appendix E 3.2 Flaw Remediation
- Appendix E.10.9 Component Inventory
- Appendix E. 11 System and Services Acquisition
- 11.1 System and Services Acquisition Policy and Procedures
- 11.2 Supply Chain Protection
- 11.3 Trustworthiness
- 11.4 Integration of Security Capabilities

Receipt of LAR
Verify cybersecurity is addressed

Vendor Audit/Cyber security Audit

Licensee's engagement with its vendor
- 11 "System and Services Acquisition" of Appendix E of NEI 08-09
- 11.2 SUPPLY CHAIN PROTECTION
- 11.3 TRUSTWORTHINESS
- 11.4 INTEGRATION OF SECURITY CAPABILITIES
- 10.9 "Component Inventory"
- Verify the cybersecurity requirements identified from the performed Security Impact Analysis

Verify cybersecurity is addressed

Factory Acceptance test

- Appendix E 11.5 DEVELOPER SECURITY TESTING

Installed

Appendix E. 11.6 Licensee Testing
All other CSP cybersecurity controls. The DI&C system update needs to comply with the licensee's CSP and is subject to NRC's ROP including inspections

Independent NRC Cybersecurity Activities (NSIR & Regions)

Figure 3 DI&C system upgrade—security controls associated with licensee and vendor activities with applicable security controls

2.10 Security Controls Associated with a DI&C System Upgrade

Appendices B and C to RG 5.71, Revision 1, address the intent of the security controls listed in table 2. For licensees to effectively protect and comply with the Cybersecurity Rule and for the NRC to effectively inspect a DI&C system upgrade, both parties should understand the intent (i.e., purpose(s) and objective(s)) of the applicable security controls. Understanding the purpose(s) and objective(s) of the security controls is important for properly implementing and inspecting them. If the security controls are not well understood, the implemented controls may not effectively protect the DI&C systems from potential cyber threats. Therefore, the NRC included the intent of the cybersecurity controls when the agency issued RG 5.71, Revision 1, in 2023 to incorporate lessons learned from operating experience since the original publication of the guide.

3. CONCLUSION

To implement a safe and cybersecure DI&C system upgrade, cybersecurity should be incorporated into the initial design stages. The licensees' CSPs currently include commitments to address cybersecurity from the initial design stages. The NRC's regulatory framework also supports performing cybersecurity audits in parallel with the licensing review.

A cybersecurity audit of a DI&C system upgrade could be conducted on a schedule independent of the NRC's safety evaluation. This allows the NRC cybersecurity staff to work in parallel with the NRC licensing staff and to not impact safety-related review milestones. Cybersecurity audits could be divided into the three DI&C-ISG-06 stages: pre-LAR submittal, LAR review, and post-LAR inspections.

The scope of the cybersecurity audits would be limited to the security controls that licensees are committed to address for each of the following DI&C upgrade activities:

- modification concept and preapplication meetings
- high-level system design and planning
- system and HW/SW requirements
- detailed HW/SW design
- implementation test (including FAT)
- post-FAT licensee activities and SAT

Figure 3 summarizes licensees' CSP commitments that could be audited in parallel with the licensing review. By performing cybersecurity audits in parallel with the licensing review, the NRC staff could potentially provide additional cybersecurity-related regulatory certainty and increase the inspection efficiency of cybersecurity controls associated with the DI&C system upgrade. These activities are also consistent with the good engineering practice concept of "secure by design."

4. REFERENCES

U.S. Code of Federal Regulations (CFR)

1. 10 CFR Part 73, "Physical Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.

2. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

U.S. Nuclear Regulatory Commission

1. Regulatory Guide (RG) 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Washington, DC, January 2006 (ML053070150).

2. RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Washington, DC, July 2011 (ML102870022).

3. RG 1.152, Revision 4, "Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants," Washington, DC, July 2023 (ML23054A463)

4. RG 5.71, Revision 0, "Cyber Security Programs for Nuclear Facilities," Washington, DC, January 2010 (ML090340159).

5. RG 5.71, Revision 1, "Cyber Security Programs for Nuclear Power Reactors," Washington, DC, February 2023 (ML22258A204).

6. Digital Instrumentation & Control (DI&C) Interim Staff Guidance (ISG)-06, Revision 2, "Licensing Process," Washington, DC, December 2018 (ML18269A259)

7. Digital Instrumentation & Control (DI&C) Interim Staff Guidance (ISG)-06, Revision 1, "Licensing Process," Washington, DC, January 2011, (ML110140103)

8. NRC Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," Washington, DC, February 25, 2002.

9. NRC Order EA-03-086, "Design Basis Threat for Radiological Sabotage," Washington, DC, April 29, 2003.

10. NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," October 2004 (ML15111A054).

11. NEI, "Addendum 4 to NEI 08-09, Revision 6 Dated April 2010 Physical and Operational Environment Protection," Washington, DC, July 2017. (ML17212A635)

Other

1. Nuclear Energy Institute (NEI), NEI 04-04, Revision 1, "Cyber Security Program for Power Reactors, Washington, DC, November 18, 2005.

2. Zimmerman, R.P., Letter to M.T. Coyle, NEI, “NRC Acceptance of NEI 04-04, ‘Cyber Security Program for Power Reactors,’ Revision 1,” December 23, 2005.

3. NEI 08-09, Revision 6, “Cyber Security Plan for Nuclear Power Reactors,” Washington, DC, April 2010. (ML101180437).

4. Institute of Electrical and Electronic Engineers (IEEE) Standard 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Piscataway, New Jersey.

5. IEEE Std 603-2009, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Piscataway, NJ.

6. National Institute of Standards and Technology (NIST) SP 800-82, Revision 2, “Guide to Industrial Control Systems (ICS) Security,” Gaithersburg, Maryland, September 29, 2008.

8. NIST SP 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” Gaithersburg, Maryland, May 2004.

9. NIST SP 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations,” Gaithersburg, Maryland, September 2020.

10. NIST SP 800-30, Revision 1, “Guide for Conducting Risk Assessments,” Gaithersburg, Maryland, September 2011.

11. NIST SP 800-39, Revision 1, “Managing Information Security Risk: Organization, Mission, and Information System View,” Gaithersburg, Maryland, March 2011.

12. NIST SP 800 1 8, Revision 1, “Guide for Developing Security Plans for Federal Information Systems,” dated February 24, 2006

13. NIST SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems,” Gaithersburg, Maryland, August 2011.