Analysis of Inspection Findings on Defense-in-Depth Implementation

Eric Lee

9/18/2020

Introduction

Nuclear power plants completed the full implementation of their cyber security programs by the end of the 2017 year in order to comply with regulations set by the U.S. Nuclear Regulatory Commission (NRC) to protect against cyber attacks. In 2017, the NRC began full implementation inspections at nuclear power plants to assess licensees' full implementation of their cyber security program, as outlined in their NRC approved cyber security plans. During these cyber security full implementation inspections at power reactors, NRC inspectors observed that some licensees have taken the position that their critical digital assets (CDAs) located inside the Protected Area (PA) (or in some cases the Vital Area (VA)) and secured by the data diode are adequately protected by the following licensee-implemented security measures:

- Data diodes;
- Physical security programs; specifically, gates, guns, and guards (i.e., the "3Gs");
- Portable media and mobile devices (PMMD) programs;
- Wireless usage restrictions; and
- Supply chain programs (collectively, the licensees' implemented security measures).

Those licensees asserted that the above security measures provided adequate defense-in-depth protective strategies to comply with their cyber security plans (CSPs) because the implemented security controls are adequate alternative controls/countermeasures for cyber security controls enumerated in Appendices D and E of NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," dated April 2010.

During inspections, the inspectors assessed whether the implemented security measures were adequate alternative security controls for the security controls provided in Appendices D and E to determine whether the above implemented security measures adequately provide defense-in-depth protective strategies to comply with their CSPs. The inspectors performed their evaluation based on the existing NRC-approved licensee CSPs, which follow the CSP template in NEI 08-09.[1] Additionally, inspectors' found that, for licensees to comply with their CSPs, the licensees

[1] The CSP sections discussed in this document are the same as the corresponding sections in NEI 08-09, Revision 6 (including Addendum 1) because the licensees used NEI-08-09 as the template for the implementation of their CSPs.

should have performed assessments on each CDA per the process described in Sections 3.1.1 through 3.1.6 of their CSPs to identify and implement applicable security controls to protect the CDA. Therefore, the inspectors identified several findings for the improper implementation of defense-in-depth protective strategies, which included the failure to address the Appendices D and E security controls. In these instances, inspectors identified violations of very low safety significant.

Discussion

This section gives additional information about the instances where inspectors identified violations of NRC's cyber security requirements with respect to defense-in-depth. For the CDAs located inside the PA and the VA and secured by the data diode, the licensees identified the following attack pathways that adversaries can exploit to deliver cyber attacks from sources external to the plant:

1. Logical pathway through the data diode,
2. Physical pathways through the gates (including PMMD and other physical pathways),
3. Supply chain pathway, and
4. Wireless pathway.

In their implementation, the licensees' assessment was based on the fact that any external cyber attacks through their hardware-based deterministic data diodes are not possible. Based on their assessment, some licensees asserted that the following respective mitigating measures (implemented along the pathways described in the second, third, and fourth bullets above) provided defense-in-depth for the protection of the CDAs that are air-gapped and/or behind the data diode:

- Physical security measures are implemented to protect the plant from adversaries, including the following:
    - The access authorization program, which is implemented to ensure that those individuals who have access to the PA and the VA are trustworthy and reliable, authorized, and fit for duty,
    - Physical access controls, which are implemented to prevent unauthorized individuals from entering the PA and the VA. The PMMD program mitigates malicious files from external sources,
- CDAs are procured and stored in accordance with licensee procurement programs, and
- All wireless communications are prohibited for safety-related and important-to-safety CDAs.

Additionally, these licensees claimed that the above security measures provide adequate defense- in-depth protective strategies, because the implemented security measures protect against and mitigate the threat vectors that are applicable to the CDAs located behind the data diode and inside the PA and the VA. Based on this conclusion, the licensees determined that the above security measures were adequate alternative controls/countermeasures that mitigated the consequences of the threat/attack vector(s) associated with one or more of the cyber security controls enumerated in Appendices D and E that are referenced in licensees' CSPs.

During full implementation inspections, the inspectors evaluated the licensees' above determination that the implemented security measures were adequate alternative

controls/countermeasures for the Appendices D and E security controls, by examining whether each of the alternative countermeasures met the following criteria provided in Section 3.1.6 of their CSPs:

a. Documentation of the basis for employing alternative countermeasures, and
b. Performance and documentation of the analyses of the CDA and alternative countermeasures to confirm that the countermeasures mitigate the threat/attack vector the corresponding Appendix D or E control is intended to protect.

Specifically, the inspector's evaluation:

- Identified all the requirements associated with the defense-in-depth strategies and alternative security controls that are contained in the licensees' CSPs and the cyber security rule;
- Evaluated the potential cyber attack pathways for those CDAs located behind the data diode and located inside the PA and the VA;
- Based on the attack pathway assessment, determined whether the licensees' implemented security measures mitigate the threat/attack vectors that the Appendix D and E controls are intended to protect.

Based on the above steps, the inspectors determined whether the licensees violated requirements associated with the defense-in-depth strategies and alternative security controls that are contained in the licensee's CSPs and the cyber security rule.

Program Requirements Associated with Defense in Depth Strategies

The basis for the licensees' cyber security program requirements associated with the defense-in-depth protective strategies is from 10 CFR 73.54(c)(2).

> *(c) The cyber security program must be designed to:*
> *……..*
> *(2) Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. . .*

Table 1 below provides a list of the cyber security program performance requirements that are associated with defense-in-depth protective strategies. These program performance requirements are provided in Section 2.2 "Performance Requirements" of the licensees' CSP.

The table also provides the regulations that correspond with the cyber security program performance requirements.

Table 1. Cyber Security Program Performance Requirements and Associated Cyber Security (Rule) Requirements for Defense-in-Depth Protective Strategies

Cyber Security Program Performance Requirements	Cyber Security Regulations Addressed by the Performance Requirements
2.2.7 Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure effectiveness of the Program.	10 CFR 73.54(c)(2) *The cyber security program must be designed to: Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks*
2.2.8 Maintain the capability to mitigate the adverse consequences of cyber attacks.	10 CFR 73.54(c)(3) *The cyber security program must be designed to: Mitigate the adverse affects [sic] of cyber attacks* 10 CFR 73.54(e)(2)(ii) *The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will: . . . Mitigate the consequences of cyber attacks*
2.2.13 Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in 10 CFR 73.1 at all times. (10 CFR 73.54(e)(2)(i), 10 CFR 73.54(e)(2)(iv) and 10 CFR 73.55(b)(2)).	10 CFR 73.54(e)(2)(i) *The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will: . . . Maintain the capability for timely detection and response to cyber attacks* 10 CFR 73.54(e)(2)(iv) *The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will: . . . Restore affected systems, networks, and/or equipment affected by cyber attacks*

Additionally, the term “defense-in-depth protective strategies” is explained in Section 4.3 “Defense-In-Depth Protective Strategies,” of the licensees’ CSPs. Specifically, the first paragraph of Section 4.3 of NEI 08-09 (also in the licensees’ CSPs) states the following:

> *Defense-in-depth protective strategies have been implemented, documented, and are maintained to ensure the capability to detect, delay, respond to, and recover from cyber attacks on CDAs. The defensive strategy describes the defensive security architecture, identifies the protective controls associated within each security level, implements cyber security controls in accordance with Section 3.1 of this Plan, employs the Defense-in- Depth measures described in NEI 08-09, Appendix E, Section 6, and maintains the cyber security program in accordance with in Section 4 of this Plan.*

Consistently, NEI 08-09, Revision 6, Section 3.1.6 “Mitigation of Vulnerabilities and Application of Cyber Security Controls,” states that defense-in-depth strategies are established by documenting and implementing the defensive strategy described in Section 4.3 and the security controls provided in Appendix D and Appendix E of NEI 08-09. Section 3.1.6 of NEI 08-09 Addendum 1 states, in part, that any one of the Appendices D and E security controls can be addressed by analyzing and documenting one or more of the following actions:

1. Implementing the security control as written in NEI 08-09, Appendices D and E.
2. Implementing an alternative control or countermeasures that mitigate the consequences of the threat/attack vectors associated with one or more of the cyber security controls enumerated in (1) above by:
    a. Documenting the basis for employing alternative countermeasures, and
    b. Performing and documenting the analyses of the CDA and alternative countermeasures to confirm that the countermeasures mitigate the threat/attack vector the original control is intended to protect
3. Not implementing the cyber security control by doing the following:
    a. Performing an analysis of the specific cyber security controls for the CDA that will not be implemented.
    b. Documenting justification demonstrating that the attack vector does not exist (i.e., not applicable), thereby demonstrating that those specific cyber security controls are not necessary.

.

Attack Pathway Evaluation

Attacks on any CDAs can only occur when (1) a vulnerability/weakness exists, (2) an exploit is developed to take advantage of the vulnerability, and (3) an attack vector (i.e., method, means, or mechanism that makes use of attack pathway(s)) exists for delivering the exploit to the asset. Without all three of these elements, a successful cyber attack is not possible. If any element of the chain is eliminated, then the attack cannot succeed. Thus, the following hold true:

- If the licensees' implemented security measures *eliminate* all attack pathways to

the CDAs, adversaries cannot successfully compromise the CDAs. In that case, no additional security controls are needed to protect the CDAs from cyber attacks.

- However, if the licensees' implemented security measures only *mitigate* the attack pathways to the CDAs, it is possible that an adversary can use the attack pathway(s) to compromise the CDA. In this case, to ensure that there is reasonable assurance of adequate protection against cyber attacks, the licensees will need to protect the CDAs by implementing the defense-in-depth protective strategies provided in their CSPs.

Therefore, if there is an attack pathway, the CDAs located behind the data diode and inside the PA and VA need to be protected to provide adequate defense-in- depth protective strategies as required by the licensees' CSPs.

Accordingly, the inspectors assessed the licensee-implemented cyber security measures by identifying and evaluating the attack pathways of those CDAs located behind the data diode and inside the PA and the VA. The primary objective of the attack pathway evaluation was to determine whether there are any attack pathways that can be exploited by an adversary to attack CDAs located behind the data diode and inside the PA and VA. The following attack pathways were identified and evaluated:

- **Logical Pathways**

  A data diode is a one-way, hardware-based deterministic diode that licensees have installed under their CSPs that eliminates certain logical attack pathways. This is because a data diode is an optical fiber with a sender on one side and a receiver on the other side. As a result, it is physically impossible for data to be transferred in the other direction, since the fiber-optic connection only allows one-way communication. Therefore, the installed data diode eliminates all logical attack pathways from external networks and eliminates all threat vectors from external networks.

  However, the logical attack pathways for CDAs behind the data diode exist from other connected CDAs located on internal networks, which are also behind the data diode. Because these attack pathways, such as wireless, supply chain, and physical attack pathways, are not eliminated by the implemented data diode, it is possible that an adversary can use these attack pathways to compromise the CDAs. For example, if one or more of the CDAs is compromised through portable media introduced to the CDAs through physical attack pathways of the licensee's PMMD program, then other CDAs located on the same internal network may become compromised.

- **Wireless Pathways**

  All wireless communications are prohibited for safety-related and important-to-safety CDAs. Security controls and the elimination of wireless communication ensure there is not any wireless communication, so the attack vectors through wireless attack pathways are eliminated.

- **Supply Chain Pathways**

Malware or unwanted software may be introduced to the CDAs or network behind the data diode through the procurement of CDA products or services. Procurement of CDA products or services includes software updates for CDAs located behind the data diode. Because it is not possible to test all the potential states of software to detect and eliminate unwanted software or software errors, the licensees implemented system and services acquisition controls as described in their CSPs to minimize the introduction of malware and security vulnerabilities associated with the procurement of the products and services for the CDAs. Additionally, the licensees implemented PMMD programs to minimize the potential introduction of unwanted data or software to the CDAs by vendors or authorized individuals by performing anti-virus scanning on any software or data before introducing to the CDAs to detect and remove any malware or unwanted software. Anti-virus programs employed by the licensees' PMMD program to detect and remove viruses use signature scanning, heuristic scanning, and/or integrity checking. Each of these methods has its own strengths and weaknesses. As a result, the employed anti-virus programs do not completely detect malware or unwanted software that may be inside the software brought in by a vendor or authorized individual. Therefore, the implemented supply chain protection measures and PMMD programs do not fully eliminate the supply chain attack pathway for CDAs located behind the data diode and inside the PA and the VA.

To ensure that there is reasonable assurance of adequate protection of the CDAs against cyber attacks through the supply chain pathways, licensees need to implement security measures to provide adequate defense-in-depth protective strategies as required by the licensees' CSPs.

Physical Pathways

Unlike the data diode that eliminated any data flowing from external sources to networks behind it, physical security measures and the PMMD program only mitigate against an attack through physical pathways for CDAs behind the data diode.

The focus of the physical security measures described early in the "Discussion" section of this paper is on a physical attack causing radiological sabotage. Specifically, these measures ensure the following: (1) individuals who are entering the nuclear power plants (i.e., PA and VA) are trustworthy and reliable, and (2) contraband (e.g., firearms, explosives, and incendiary devices that can be used by adversaries to cause radiological sabotage) are not brought into nuclear power plants. Thus, the physical security program provides limited protection against vendors or authorized individuals unknowingly introducing unwanted data or software to the CDAs located behind the data diode. To address these potential cyber security issues, the licensees implemented PMMD programs to minimize the potential introduction of unwanted data or software to the CDAs by vendors or authorized individuals. However, as discussed above, the employed anti-virus program does not completely eliminate attacks through physical attack pathways.

Therefore, the CDAs located behind the data diode and inside the PA and the VA are subject to cyber attacks through physical pathways. To ensure that there is reasonable assurance of adequate protection of the CDAs against cyber attacks through physical attack pathways, licensees need to implement security measures to provide adequate defense-in-depth protective strategies as required by the licensees' CSPs.

Furthermore, as discussed in the “Logical Pathways” subsection of this paper, the CDAs located behind the data diode are vulnerable to other CDAs behind the data diode, which may be compromised by the introduction of PMMD by a vendor or an authorized individual. Any CDAs compromised through a physical pathway or supply chain pathway can compromise other CDAs through the networks behind the data diode. Therefore, to ensure that there is reasonable assurance of adequate protection of the CDAs against cyber attacks, licensees need to implement security measures to provide adequate defense-in-depth protective strategies as required by the licensees’ CSPs.

Technical and Regulatory Questions

The inspectors evaluated whether the licensees’ implemented security controls provided adequate defense-in-depth protective strategies by answering the following two questions based on the above discussions and information collected during full implementation inspections:

Question One:
Are there any attack pathways that an adversary can exploit to perform cyber attacks on those CDAs located behind the data diode and located inside the PA and the VA?

Yes.
Based on the attack pathway assessment provided in the previous section, the supply chain pathways and the physical pathways provide attack pathways that an adversary can use to deliver unwanted and/or unauthorized software or data to CDAs located behind the data diode and located inside the PA and the VA. Additionally, although the implemented data diode protects the CDAs behind the data diode against external networks, the data diode does not provide any protection against other CDAs behind the data diode, which may be compromised through the supply chain attack pathways and the physical attack pathways.

Therefore, the CDAs located behind the data diode and located inside the PA and the VA need to be protected to provide adequate defense-in-depth protective strategies required by the licensee’s CSPs (1) to delay and detect unwanted software and data before they are delivered to the CDAs located behind the data diode and inside the PA and the VA via supply chain or physical pathways and (2) respond to and recover from cyber attacks on CDAs to minimize the consequences of cyber attacks. Specifically, to provide adequate defense-in-depth protective strategies required by the licensees’ CSPs, the licensees need to (1) implement Appendices D and E security controls, (2) other valid alternative controls that mitigate the threat/attack vector that the Appendices D and E security controls are intended to protect or (3) not implement the security controls and document that the attack vectors associated with Appendices D and E security controls do not exist.

Question Two:
Do those licensees’ implemented security controls described in Discussion Section provide multiple layers of protections that are sufficient to establish the level of defense-in-depth protective strategies required by the licensee’s CSPs to (1) delay and detect unwanted software and data before they are delivered to the CDAs

located behind the data diode and inside the PA and the VA via supply chain or physical pathways, and (2) respond to and recover from cyber attacks on CDAs to minimize the consequences of cyber attacks?

No.
Section 4.3 and Section 3.1.6 of the licensees' CSPs state that defense-in-depth protective strategies required by 73.54(c)(2) are established by implementing cyber security controls, the defensive security architecture, and maintaining the cyber security program. Since the licensees implemented the NRC-accepted defensive security architecture and implemented a program to maintain the cyber security program at their facilities, per Section 3.1.6 of NEI 08-09, the licensees need to provide adequate defense-in-depth protective strategies by:

- Implementing the security controls provided in Appendices D and E, or
- Implementing an alternative security control in place of the corresponding security control provided in Appendices D and E by documenting and confirming that the alternative security control mitigate the consequences of the threat/attack vector associated with the corresponding security control in Appendices D or E is intended to protect, or
- Not implement the security controls if the attack vectors associated with the security controls do not exist.

However, during inspections, the inspectors found that some licensees only documented and implemented the following security measures:

- Data diodes;
- Physical security programs; specifically, gates, guns, and guards (i.e., the "3Gs");
- Portable media and mobile devices (PMMD) programs;
- Wireless usage restrictions; and
- Supply chain programs (collectively, the licensees' implemented security measures).

When the inspectors questioned the implementation of other security controls provided in Appendices D and E during full implementation inspections, these licensees claimed that these implemented security controls are alternative security controls to other security controls provided in Appendices D and E. The inspectors evaluated whether these licensee-implemented security controls would meet the alternative security control criteria provided in NEI 08-09 Section 3.1.6. The inspectors determined that the licensees' implemented security measures do not mitigate the threat/attack vectors that each of the Appendices D and E security controls are intended to protect. For example, the D.5 "System Hardening" security control, which requires licensees to remove any unnecessary services and programs from the CDA to reduce the attack surface, cannot be addressed by physical security measures or by the licensee-implemented PMMD programs or other implemented security controls.

Based on the above, the inspectors found that the licensees' implemented security measures are not alternative security controls for all the security controls provided in Appendices D and E because the implemented security measures do not meet the alternative security criteria provided in their CSPs. Therefore, the licensees'

implemented security controls do not provide sufficient protection to meet the defense-in-depth protective strategies required by the licensee's CSPs to ensure that there is reasonable assurance of adequate protection against cyber attacks.

Using the answers to the above questions, the implemented security controls were evaluated to determine whether they comply with the cyber security program performance requirements and the cyber security regulations provided in Table 1. The results of the evaluation are provided in Table 2.

Table 2. Evaluation Results

Cyber Security Program Performance Requirements	Cyber Security Requirements Addressed by the Performance Requirements	Results of Evaluation
2.2.7 Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure effectiveness of the Program.	10 CFR 73.54(c)(2) *The cyber security program must be designed to: . . .* *Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks*	The answers to Questions One and Two show that the licensees' implemented security measures *do not meet* the program performance requirements and the cyber security requirements provided in this row.
2.2.8 Maintain the capability to mitigate the adverse consequences of cyber attacks.	10 CFR 73.54(c)(3) *The cyber security program must be designed to . . . Mitigate the adverse effects of cyber attacks* 10 CFR 73.54(e)(2)(ii)) *The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will: . . . Mitigate the consequences of cyber attacks*	The answers to questions Questions One and Two show that the licensees' implemented security measures *do not meet* the program performance requirements and the cyber security requirements provided in this row.

2.2.13 Ensure that the Program maintains the capability to detect, respond to, and recover from cyber attacks up to and including the design basis threat of radiological sabotage as stated in 10 CFR 73.1 at all times. (10 CFR 73.54(e)(2)(i), 10 CFR 73.54(e)(2)(iv) and 10 CFR 73.55(b)(2)).	10 CFR 73.54(e)(2)(i) *The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will: . . . Maintain the capability for timely detection and response to cyber attacks* 10 CFR 73.54(e)(2)(iv) *The cyber security plan must include measures for incident response and recovery for cyber attacks. The cyber security plan must describe how the licensee will: . . . Restore affected systems, networks, and/or equipment affected by cyber attacks*	The answers to questions Questions One and Two show that the licensees' implemented security measures *do not meet* the program performance requirements and the cyber security requirements provided in this row.

Conclusion

The results of this evaluation showed that the CDAs located behind the data diode and inside the PA and VA could potentially be subject to cyber attacks through physical and supply chain pathways, without adequate defense-in-depth in place. To adequately protect the CDAs located behind the data diode and inside the PA and the VA from cyber attacks, the licensees' CSP requires licensees to implement security measures to provide adequate defense-in-depth protective strategies. Inspectors have found instances where some licensees' implemented security measures did not provide adequate defense-in-depth protective strategies, because those licensees had not fulfilled all of the requirements specified within Section 3.1.6 of their CSPs. Therefore, contrary to the cyber security program performance requirements provided in the above table and the defense-in- depth criteria provided in Sections 3.1.6 and 4.3 of the licensees' CSP, those licensees failed to properly perform vulnerability assessments on the CDAs located behind the data diodes and inside the PA and the VA to identify and implement applicable Appendix D and E security controls or valid alternative security controls/countermeasures. Those evaluations showed that to protect CDAs behind the data diode and located inside the PA and the VA, licensees would need to perform assessments to identify vulnerabilities of CDAs and associated threat vectors to determine applicable security controls. The alternative security control is determination would be dependent on the outcome of the CDA assessment process described in Sections 3.1.1 through 3.1.6 of the CSP, including an evaluation of cyber security threats; potential vulnerabilities to, and consequences from, an attack; the effectiveness of existing cyber security controls; defensive strategies; and attack mitigation methods. Over the course of the full implementation inspections, the NRC issued multiple violations of low safety significance for not sufficiently addressing the defense-in-depth protective strategies required by the licensee's CSPs. However, in general, the staff has found that with reasonable assurance, licensees understood the cyber security requirements provided in their CSPs and implemented their cyber security programs.