Cyber Security Assessment Methodology of Critical Digital Asset in Nuclear Power Plant

Ieck Chae EUOM[1], Sung Cheol KIM[2], Joo Hyoung LEE[3]

1. Security Consulting Team, KEPCO KDN, Naju, Korea (icelaken@gmail.com)
2. Security Consulting Team, KEPCO KDN, Naju, Korea (kim.sungcheol17@kdn.com)
3. Security Consulting Team, KEPCO KDN, Naju, Korea (jhlee.217@kdn.com)

Abstract: Nuclear Power Plant Operators have approached the problem of cyber security by simply attempting to apply nation's committed catalog of cyber security requirements to every Critical Digital Asset under evaluation, which can number into the hundreds. This current approach does not provide guidance on how to assess a given requirement with a security method that effectively takes Critical Digital Asset. This paper analyzes Cyber Security Assessment Methodology about Industrial Control Systems. And then give an efficient methodology. It approaches the Regulations of KINAC/RS-015 from a technical vulnerability point of view, where any given Critical Digital Asset can be assessed for vulnerabilities
Keyword: Vulnerability identification, Security assessment, Attack vector, Logic tree

1 Introduction

Faced with regulatory commitments, Nuclear Power Plant(NPP) Operators have approached the problem of cyber security by simply attempting to apply nation's committed catalog of cyber security requirements to every Critical Digital Asset(CDA) under evaluation, which can number into the hundreds.

This current approach does not provide guidance on how to assess a given requirement with a security method that effectively takes a CDA. In addition, the control catalogs are incomplete or inappropriate for many CDAs that don't have vulnerabilities that would otherwise be associated with a given security control catalog requirement. When faced with hundreds of requirements imposed on thousands of CDAs, often inappropriately so, the burden of demonstrating adequate Cyber security becomes unsustainable and can result in adequate protection.

A more efficient and effective approach to cyber security assessment methodology is required. It can be used to demonstrate effective vulnerability assessment for any CDA or functional group of CDAs selected for evaluation by facility operator. It approaches the problem of cyber security from a technical vulnerability point of view, where any given asset can be assessed for vulnerabilities, then protected using selected, available security control methods. Some CDAs have more or less vulnerabilities than others, and some security control methods are more or less effective than others. The key is to match the most effective security control methods to each vulnerability that a CDA has, and if that can be demonstrated, then the CDA is adequately protected.

Develop a vulnerability discovery and mitigation process that demonstrates a high efficacy and that would enable a sustainable cyber security program at critical facilities while simultaneously improving the security of NPP's facilities.

2 Cyber Security Regulation Standard of Korea Nuclear Facilities

The Korea Institute of Nuclear Nonproliferation and Control (KINAC) regulatory agency published Regulatory Standard 015(KINAC/RS-015) to enact cyber security regulations in Republic Of Korea (ROK). KINAC/RS-015 based on Regulatory Guide 5.71. The origin of KINAC/RS-015 is shown in fig.1 and It provides specific criteria for establishing a Cyber Security Plan (CSP) to identify and protect CDA.

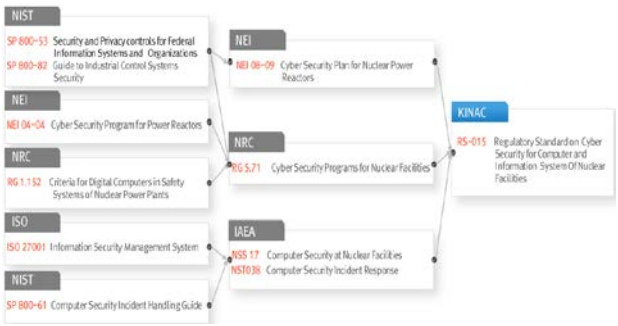


Fig.1 The origin of KINAC/RS-015

The ROK has revised its national laws, the Act on Physical Protection and Radiological Emergency (APPRE), and related regulations to reflect the cybersecurity requirements for computer and information system at nuclear facilities. Nuclear

facilities in ROK must comply with the APPRE. Pursuant to APPRE, the Nuclear Safety and Security Commission(NSSC) entrust to KINAC. KINAC is responsible for its development to facilitate regulatory activities on domestic nuclear facilities. Under evaluation, which can number into the hundreds[1]

In 2015, CSPs and implementation schedules submitted by 19 domestic nuclear facilities were approved by the NSSC. Seven steps of special inspections are to be performed to check phase-by phase CSP implementation. All the steps are expected to be completed in 2018[2]

The cyber security Regulatory basis of Korea is similar with United States. Comparison result is listed in Table 1.

Table 1 Comparison Result between U.S and R.O.K

Items	United States	Republic of Korea
The Law	10CFR73.54 "Protection of Digital Computer and"	Act On Measures For The Protection of Nuclear Facilities.
Regulatory Guidance	NRC Reg Guide 5.71	KINAC/RS-015
Industry Implement Guidance	· NEI 08-09 · NEI 10-09 · NEI 13-10	-

Reg Guide 5.71 has more cyber security control items than KINAC/RS-015. This is because the unnecessary security control items have been removed to reflect the operating environment of the Korea NPP and may be included in the body of KINAC/RS-015. The more detailed difference is shown in Fig.2

Class	Family		Quantity of Controls			
	Sec. No.	Description	RG 5.71		RS-015	
1. Technical Controls	1.1	Access controls	23	71	19	62
	1.2	Audit and Accountability	12		11	
	1.3	Critical Digital Assets and Communications Protection	22		19	
	1.4	Identification and Authentication	9		8	
	1.5	System Hardening	5		5	
2. Operational Controls	2.1	Media Protection	6	67	-	31
	2.2	Personnel Security	2		2	
	2.3	System and Information Integrity	11		8	
	2.4	Maintenance	3		2	
	2.5	Physical and Environmental Protection	9		8	
	2.6	Defensive Strategy	1		-	
	2.7	Defense-in-Depth	1		-	
	2.8	Incident Response	8		-	
	2.9	Contingency Planning/Continuity of Safety, Security, and Emergency Preparedness Functions	7		-	
	2.10	Awareness and Training	10		6	
	2.11	Configuration Management	9		5	
3. Management Controls	3.1	System and Service Acquisition	6	9	5	8
	3.2	Security Assessment and Risk Management	3		3	
Total	18		147		101	

Fig.2 Comparison of RG 5.71 and KINAC/RS-015

3 Cyber Security Assessment Methodology of Power Plant

There are limited Cyber Security Assessment Methodology in Industrial Control Systems. This paper lists three well known methodologies about Power Plants.

3.1 NEI 13-10

NPP have thousands of CDAs, but not all are operational safety-related assets. Nuclear Energy Institute's NEI 13-10 is an effort to reduce the workload associated with Cyber Security Assessment. NEI 13-10 is a guidance document that allows Licensees to group CDAs as Direct, EP or Indirect based on the importance of a CDA to a plant's safety operation and emergency planning.

NEI 13-10 provides important guidance when streamlining the control application process. Not only will it assist in reducing the initial assessment burden for certain CDA's, but it may also reduce the remediation efforts for devices that are no longer classified as Direct CDA's.

The Ratio of CDA Type is shown in Fig.3 Safety Related CDA is only 8.5% of total CDA in NPP, So it reduce the assessment efforts to CDA. [3]

However, the plants are still required to identify, document and assess all CDAs and with many of the CDA's still categorized as direct, some cases will result in millions of assessment decision points.

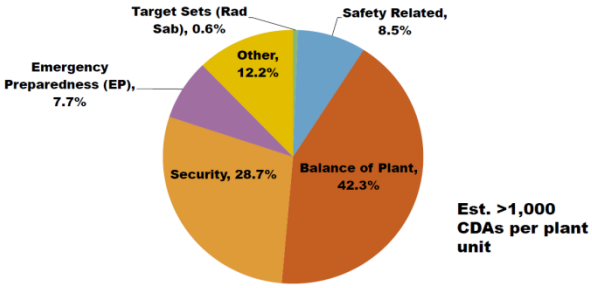


Fig.3 The Ratio of CDA Type

3.2 Logic Tree

The Logic Tree methodology is a bottom-up, compliance based approach. It should be possible to develop a process flow that starts with each parent Attack Surface Attribute and evolves through its dependent Attack Surface Attributes in such a way that the requirements associated with a particular Attack Surface Attribute are determined to be applicable to the CDA in its installed configuration, or that the attack vector is not present.

According to these concepts, it is possible to develop the Attack Surface Attributes and Logic Tree for an indexed set

of requirements. The development process is iterative and involves:

- Defining an initial set of parent and dependent Attack Surface Attributes.
- Assigning one or more of these Attack Surface Attributes to each indexed requirement.
- Constructing Logic Tree that reflect the hierarchical parent Attack Surface Attribute relationships.

The Example of Logic tree is shown in Fig.4

Consider the Attribute "Contains Communication Ports" with the Attribute value of "Yes" or "No" with multiple child Attributes[4]

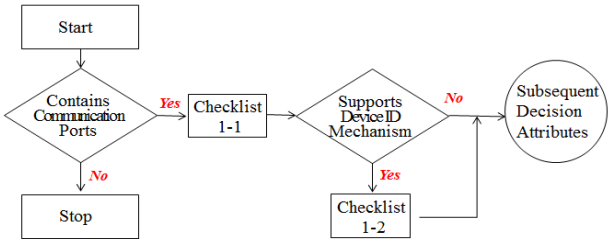
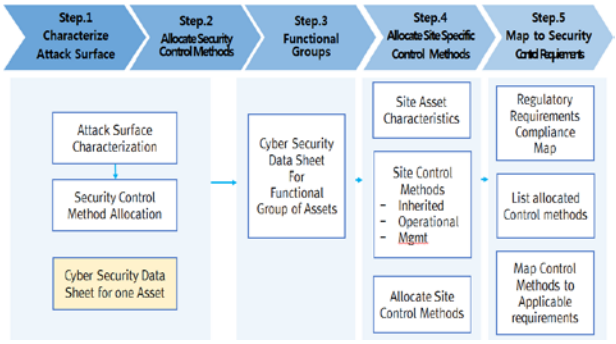


Fig.4 Logic Tree Example – Communication Ports

3.3 EPRI Cyber Security Technical Assessment Methodology



The EPRI Cyber Security Technical Assessment Methodology provides an efficient "bottom up" method to assess and mitigate cyber security vulnerabilities in equipment used in modern power plants. This method can be used at any point in the asset lifecycle, including the traditional supply chain. [5]

The five step of methodology is shown in Fig.5

Fig.5 EPRI TAM Process

Step 1 through 4 is technical in nature. They systematically address asset vulnerabilities and the most effective methods that will mitigate them, resulting in an adequately protected asset.

Step 5 is optional because it adds no technical arguments for protecting an asset; however, it does serve to demonstrate regulatory or certification compliance against a given set of cyber security or certification requirements.

4 The proposed methodology

This paper proposes security assessment methodology to cope with KINAC RS-015.This methodology is consisting of 5-steps. The 5 Steps are shown in Fig.5

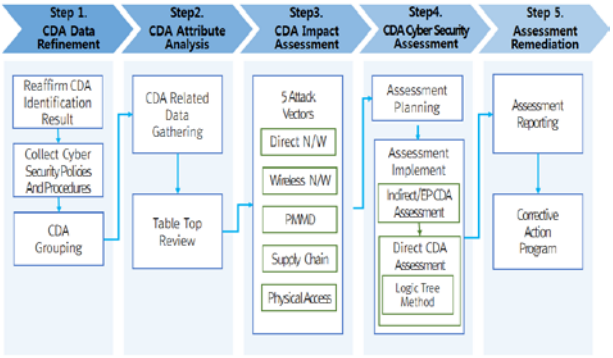


Fig.5 Five Steps in proposed methodology.

4.1 CDA Data Refinement

4.1.1 Reaffirm the CDA Identification Result

For the CDAs under assessment, obtain approved critical system, digital asset, and CDA list. and then complete the information is required for more accurate assessment, Required information is listed in Table 2.

Table 2 Vital CDA Information to assessment

Required information of CDA
· Critical System Description, Function, and Usage
· Consequence to the CS and SSEP function if a compromise of the CDA occurs
· Network security level of CDA
· Physical location of CDA

4.1.2 Collect Cyber Security Policies and Procedures

The Evaluator collects, examines and documents the existing cyber security policies, procedures, and practices; existing cyber security controls, detailed descriptions of network and communication architecture or network communication drawings information on security devices. Additional documentation could be necessary depending on the CDA or system. The Evaluator documents the collected information

and results of the information as part of the Tabletop Analysis.

4.1.3 CDA Grouping

Grouping CDAs into like groups for consideration during assessments can decrease the number of assessments needed and save time and effort of assessment. There are two methods for grouping CDAs: Aggregating and Type grouping.

Aggregation is an evaluation process to determine if several CDAs within a critical system may be combined to define a single CDA group. During the initial CDA identification process, individual CDAs are identified on a component level. The aggregated CDA group performs the SSEP function that the individual CDA cannot perform independently. The Aggregated CDA inherits the highest level of functionality of the component CDAs in the group

The Aggregation method listed below

- Identify CDAs within the systems which are to be considered for aggregation.
- Identify the SSEP function that the CDAs perform.
- Decompose the SSEP function into sub-functions and map each sub-function to a CDA.

Type grouping is the process of grouping CDAs that share a substantially similar security posture. This generally includes the same make and similar model. Type grouping method listed below

- Identify CDAs to be assessed based on the same make, similar model that have substantially similar security postures. CDAs with substantially similar security postures may be grouped using Type Grouping. CDAs are said to have similar security postures if they have similar physical protection levels and similar network security levels.
- Variation within a CDA Type is always exist. This does not preclude the use of Type Grouping. CDAs which are located in different units may be grouped together using Type Grouping as long as they have substantially similar security postures and similar functionality.

4.2 CDA Attribute Analysis

4.2.1 CDA Related Data Gathering

For The CDA characteristics used to identify available cyber security control methods. In documenting the characteristics, utilize diagrams and pictures. The CDA characteristics include the following:

- Firmware Description and Version.
- Installed Application Software and Version.
- Physical Communication Ports and Terminals.
- Available Data Communication Protocol.
- Configuration and Maintenance Methods.
- CDA Backup and Restore Capability.
- CDA Manufacturer Security Patch Program.
- Removable Media and Portable Devices.
- List of Manuals and Documentation.

4.2.2 Table Top Review

A cyber attack attempts to exploit one or more of the technical vulnerabilities by using one or more attack pathways that are specific to the CDA. The attack surface reveals which technical vulnerabilities, and is characterized by understanding the CDA characteristics. We can find more detailed and important information by Table top review.

The table top review activity includes the following:

- Identify the cyber security functional requirements and specification for the CDA.
- Identify the direct and indirect connectivity pathways to the CDA.
- Identify digital assets within infrastructure support system upon which the CDA rely to perform to the SSEP function.
- Gather all previous assessments on the CDA and identify any known vulnerabilities.
- Identify the portable media that are used with the CDA. Include media backups and recovery procedures. Indicate locations of primary and secondary recovery media.
- Identify maintenance and test equipment , including development equipment, used to calibrate, configure, support, maintain, or manage the CDA.

4.3 CDA Impact Assessment

The manner in which a cyber attack is delivered is by way of its attack vector or threat vector. If the “means exist” to exploit a technical vulnerability class, then the “means” follows an attack vector. Like the full scope of vulnerabilities for CDA, the full scope of potential attack vectors arises from both organizational and technical issues with in the NPP[6]. This paper focus on only on the technical aspects of attack vectors that are attributable to the CDA.

An attack vector is the combination of an actor with malicious intent and a pathway, either physical or logical access, to the CDA. There are 5 attack vectors per the US NRC’s risk informed Significance Determination Process[7]

- Direct Physical Access: An adversary has physical access to a CDA.
- Supply Chain: An adversary has physical or logical access to a CDA prior to or during the licensee's procurement process.
- Portable Media and Mobile Devices(PMMD) : An adversary has physical access to the PMMD that will be used with a CDA.
- Direct Network Connectivity: An adversary has logical access to a CDA via a wired network.
- Wireless Network Connectivity: An adversary has logical access to a CDA via a wireless network.

There are example technologies or indicators that enable the attack vector, and example mitigation methods. The example technologies and indicators represent "means" to exploit a vulnerability, and the example mitigation methods represent potential security control methods to implement.

If the means exist to exploit a vulnerability, then one or more of the attack vectors are present. However, in order to determine the specific security control method to implement, the exact attack pathway mechanism must be known.

But, It is very difficult to prove attack pathway within a limited time. So It is efficient to use check lists for finding attack vector. The Check Items to find out attack vector about "Supply Chain" is listed in Table 3. If all of the listed items 1 through 6 are "YES", then the supply chain access attack vector is mitigated. If any of the listed items 1 through 6 are "NO", then the supply chain access vector is not mitigated.

Table 3 Check Items about Supply Chain

No	Check Items
1	Is the CDA vendor prohibited from having remote access to the CDA?
2	Are recovery instructions utilized that detail Configuration control of replacement parts?
3	Are software patches and updates tested or validated on a separate support system or in a test environment prior to installation?
4	Are CDAs shipped to the site using procurement specification supply chain protections while maintaining a chain of custody?
5	Has the system been installed and operating with a known maintenance history?
6	Has the vendor approved all installed third party software applications on the CDA/CDA group?

There are several cyber security controls in KINAC RS-015 Appendix 2 that require alternate controls when the principal control cannot be implemented. These controls must be implemented with an alternate control or passed directly. they are ineligible to be mitigated using the Attack Vector. An example of such a control is listed in Table 4.

This control must be provided with an alternate control, a primary control, or a remediation action if neither alternate or principal controls are feasible.

Table 4 Example of exceptions to Attack Vector

No	Control Items
1.2.6(3) (NEI 08-09)	Audit Reduction And Report Generation
	1.Provide CDA audit reduction and report generation capability
	2. Provide the capability to process audit records for events of interest based upon selectable, event criteria in an automated fashion.
	3. This Technical cyber security control also documents the justification and details for alternate compensating security controls where a CDA cannot support auditing reduction and report generation by providing this capability through a separate system.

4.4 CDA Cyber Security Assessment

NEI 13-10 revision 5 was endorsed by Nuclear Regulatory Commission (NRC). So, America's NPP Licensees use NEI 13-10 to reduce workload associated with cyber security assessment.

4.4.1 Assessment Planning

The Cyber Security Specialist (CSS) is responsible for assembling all of the necessary documentation on plant and corporate cyber security policies, procedures, programs, and strategies. Also assembled is information about the critical system, digital assets, and CDAs to include vendor information, installation configuration, consequence, interdependencies, infrastructure and architecture. All of this information will be used during the Tabletop review and validation completed by the CSS. The Tabletop review is conducted as a part of the Assessment Procedure.

The Tabletop review is completed and the list of CDAs is validated. The CSS will then take the CDA list and group them, if applicable, by type or aggregation, or as a combination . The CSS use the attack vector method with respect to the system and CDA/CDA Group to acknowledge mitigation of any applicable attack vectors. A discussion on the attack vector method is found in Section 4.3.

Once CDAs and CDA Groups have been identified, the CSS determines the classification of the CDA/CDA Group.

The Audit Plan lists criteria to determine the classification of the CDA/CDA Group as one of the following:

- Emergency Response.
- Indirect.
- Direct Low Functionality.
- Direct -other.

If this determination results in the CDA being classified as "Emergency Response" or "Indirect," the CDAs will follow an Indirect/EP Cyber Security Assessment and the Direct Assessment is not necessary. If this determination results in the CDA being classified as a Direct CDA, the CDAs will follow a Direct Cyber Security Assessment and the Indirect Assessment will not be applicable. This distinction is shown in Fig.6, below.

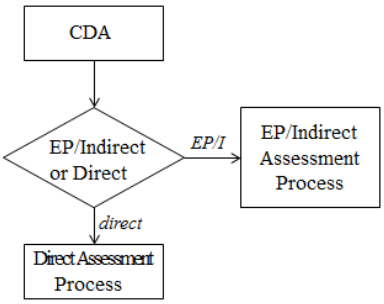


Fig.6 High Level Assessment Flow.

4.4.2 Assessment Implementation

4.4.2.1 Indirect/EP CDA Assessment

Indirect CDAs are CDAs protected under the NPP's CSP whose failure would not have a direct impact on the ability of the plant to maintain radiological health and safety. EP CDAs are those CDAs that are used to carry out the steps described in the NPP's Emergency Plan. These devices do not have a direct impact on radiological health and safety, and their function can be provided by alternate means; because the risk is lower they can be assessed using the less rigorous method in NEI 13-10 which has time and effort optimizations.

These CDAs are considered to be adequately protected by a set of minimum protection criteria. These minimum protection criteria are sufficient to provide high assurance that the CDAs are adequately protected against cyber attack. The minimum protection criteria that must be met are: [8]

- The Indirect CDA is located in the Vital Area or the Protected Area, or the cyber security controls in KINAC RS-015, Appendix 2, Section 2.4, "Physical and Operational Environment Protection" are addressed.
- The Indirect CDA and any interconnected assets do not have wireless networking communications technologies.
- The Indirect CDA and any interconnected assets are either air-gapped or isolated from Level 2 networks by a deterministic isolation device..
- The use of PMMD is controlled according to KINAC RS-015, Appendix 2, Control 1.1.16, "Access Control for Portable and Mobile Devices," in order to ensure the Indirect CDA will not be compromised as a result of the use of PMMD.
- Changes to the Indirect CDA are evaluated before implementation in accordance with the CSP.
- The Indirect CDA, or any interconnected equipment that would be affected by the compromise of the Indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks would include any routine checks performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks.

4.4.2.2 Direct CDA Assessment

Direct CDAs, as outlined below, must comply with the cyber security controls outlined in KINAC/RS-015 Appendix 2 . These controls may be satisfied by applying one of three approaches.

- Not applying the control because the associated attack vectors have been mitigated and therefore the control is not applicable.
- Applying alternate controls because the principal control cannot be implemented for technical reasons, or
- Applying the full control in KINAC RS-015 as written.

There are two methods to perform assessment of Direct CDA. These are called the logic tree method and the functionality assessment method.

4.4.2.2.1 Logic Tree Method

The logic tree methodology is a bottom-up, compliance based approach centered on the security controls of KINAC RS-015. The logic tree methodology is designed to ensure full compliance with the NPP's CSP. The security controls are grouped together into logical commonalities based on device capabilities and applied to the CDA to represent a consequence based assessment. If the CDA does not have the features and functions that the control is designed to

mitigate, the controls are then determined to be not implemented on the CDA.

4.4.2.2.2 Functionality Assessment Method

The functionality and access level of the device allows NPP licensees to streamline the Direct Assessment process based on the capabilities of a device. This approach was endorsed in Revision 2 of NEI 13-10 and expanded in Revision 5. A Direct CDA may be classified as "Low-Functionality, Direct Impact" or "Direct Impact." The Low Functionality level is further divided into six classes: A.1, A.2, A.3, B.1, B.2, and B.3. Each class defines a subset of the KINAC RS-015 Appendix 2 controls that are applicable to the device being assessed; the remaining controls are considered to provide no additional security. These controls are not applied to the device.

4.5 Assessment Remediation

Part of the assessment process is to address control failures. A control failure occurs when the Cyber Security Program does not address the particular applicable control. For each failure, a remediation recommendation is made to aid the CSS. Some remediation recommendations can be common across the entire system that addresses multiple cyber security control failures, where other recommendations may be specific to a single cyber security control failure. The failures along with their remediation recommendations are reported in the Assessment Report and also reported in the Corrective Action Program.

5 Conclusions

It is possible to take a brute force approach to identify applicable cyber security regulatory requirements for a CDA. This approach would consist of walking through the cyber security requirement statements one at a time, then determining whether or not each requirement is applicable.

Such a brute force approach, while possible to complete, would generally prove to be more time-consuming and less effective than first identifying attack surface attributes that drive cyber security regulatory requirements and then mapping the security control methods to the applicable requirements.

This paper proposes efficient methodology to assess CDA in NPP. Use of CDA Attributes and Logic Tree analysis greatly reduces the level of effort in assessment.

References

[1] Korea Institute of Nuclear Nonproliferation and Control (KINAC), "Cyber Security Activity Introduction1"; http://www.kinac.re.kr:8181/eng/busin/busin3.do

[2] Korea Institute of Nuclear Nonproliferation and Control (KINAC), "Cyber Security Activity Introduction2"; http://www.kinac.re.kr:8181/eng/busin/busin4.do

[3] NEI Conference 2016, "NEI 13-10:Overview, Results, and Need for Consistency",2016

[4] NEI Conference 2015, "Case Study: Logic Tree Method in Southern Company",2015

[5] Electric Power Research Institute(EPRI), "Cyber Security TAM;" https://www.epri.com/#/pages/product/3002008023

[6] Nuclear Energy Institute(NEI), NEI 10-09 Revision 0, "Addressing Cyber Security Controls for Nuclear Power Reactors",2011

[7] Nuclear Energy Institute(NEI), NEI 04-04 Revision 2, "Cyber Security Program for Power Reactors",2015

[8] Nuclear Energy Institute(NEI), NEI 13-10 Rev5. "Cyber Security Control Assessments", 2016