Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.877

원자력시설의 필수디지털자산에 대한 기술적 보안조치항목에 대한 연구

최 윤 혁,[1†] 이 상 진[2‡]
[1]한국전력기술, [2]고려대학교

A Study on the Implementation of Technical Security Control for Critical Digital Asset of Nuclear Facilities

Yun-hyuk Choi,[1†] Sang-jin Lee[2‡]
[1]KEPCO E&C, [2]Korea University

요 약

기술발전에 따라 원자력시설에 사용되는 장비가 아날로그 시스템에서 디지털 시스템으로 변경되는 추세이다. 컴퓨터와 디지털시스템의 비율이 증가함에 따라 원자력시설은 사이버 위협에 노출되었다. 그 결과 사이버보안에 대한 관심이 높아지고 사이버 공격으로부터 시스템을 보호해야 한다는 인식의 변화가 생겼다. 국내 규제기관에서 발행한 KINAC/RS-015는 필수디지털자산에 대해 101가지 사이버보안 통제항목을 제시하였지만 디지털자산의 특성을 고려하지 않은 일반적인 항목이다. 모든 사이버보안 통제항목을 필수디지털자산에 적용하는 것은 많은 작업량과 효율성을 떨어뜨린다. 본 논문에서는 필수디지털자산의 특성을 파악하고 적절한 보안조치항목을 제시함으로써 효과적인 사이버 보안 통제항목 적용을 제안한다.

ABSTRACT

As technology advances, equipment installed in Nuclear facilities are changing from analog system to digital system. Nuclear facilities have been exposed to cyber threats as the proportion of computers and digital systems increases. As a result, interest in cyber security has increased and there has been a need to protect the system from cyber attacks. KINAC presented 101 cyber security controls for critical digital asset. However, this is a general measure that does not take into account the characteristics of digital assets. Applying all cyber security controls to critical digital assets is a heavy task and can be lower efficient. In this paper, we propose an effective cyber security controls by identifying the characteristics of critical digital assets and presenting proper security measures.

Keywords: Nuclear facilities, Security control, Critical Digital Assets

I. 서 론

전력, 가스, 철도 등 산업플랜트를 운영하기 위해 사용되는 산업제어시스템은 기술의 발전에 따라 아날로그 시스템에서 디지털 시스템으로 변경되는 추세이다. 그런데 디지털시스템은 정보유출, 해킹, 서비스 방해 등 사이버공격에 쉽게 노출되어 있으며 침해되었을 때 그 피해가 심각하다.

국내 산업제어시스템도 마찬가지로 사이버 위협에 자유롭지 못하다. 그 중에서 발전소 운영에 이용되는 산업제어시스템은 외부와 단절된 폐쇄망을 이용하여 운전하도록 설계되어 사이버공격에 안전할 것으로 여

Received(10. 01. 2018), Modified(1st: 12. 13. 2018, 2nd: 03. 27. 2019), Accepted(05. 20. 2019)
† 주저자, engchoiyh@kepco-enc.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

겨졌으나 2010년 이란 원자력시설내 우라늄 원심분리기 가동을 중단시킨 스턱스넷(Stuxnet) 공격[1], 2011년 제어시스템의 정보 수집 및 유출을 목표로 한 듀큐(Duqu)[2] 등의 사례에서 알 수 있듯이 폐쇄망을 사용하더라도 사이버공격이 가능하다.

따라서 발전소 설계단계부터 사이버공격에 대한 대응을 고려해야 하는 시대가 되었다. 사이버보안을 위해 미국에서는 2007년 10CFR73.1 개정[3]을 통해 사이버보안 상위요건을 수립하였다. 이후에 원자력규제위원회(U.S NRC, U.S Nuclear Regulatory Commission)는 2009년 10CFR73.54의 개정[4]을 통해 원자력시설의 사이버보안 지침 적용을 요구하였으며 법규를 만족하기 위해 Regulatory Guide 5.71(RG 5.71)을 2010년에 발행하였다. RG 5.71은 미국에서 운영 중인 원자력시설에 대해 사이버보안계획(CSP, Cyber Security Plan)의 수립하였고, 정책을 비롯하여 설계, 구현, 시험, 설치 운영 등 생명주기 단계별로 조치해야 할 사항과 기술적, 운영적, 관리적 사이버통제 항목을 상세하게 제시하였다[5].

국내에서는 원자력시설 등의 방호 및 방사능방재 대책법 제40조(업무의 위탁)에 따라 한국원자력통제기술원(KINAC, korea Institute of Nuclear Nonproliferation and Control)에서 KINAC/RS-015를 발행하여 원자력시설 등의 컴퓨터 및 정보시스템 보안에 대한 국내 기술기준을 제시하였고 이에 따라 원자력시설에 대한 사이버보안 업무를 수행하고 있다. KINAC/RS-015에서는 원자력시설의 필수시스템(CS, Critical System)을 식별하고 디지털자산에 대해서도 필수디지털자산(CDA, Critical Digital Asset)을 식별하도록 요구하고 있다. 식별된 CDA는 기술적/운영적/관리적 보안조치 항목 101가지를 만족하고 있음을 보여야 한다.

본 논문에서는 CDA의 하드웨어 특성과 소프트웨어 특성을 고려하여 CDA를 그룹화하는 방법론을 제안하고 그룹에 따라 적용이 필요한 기술적 통제항목을 식별하여 효율적인 기술적 통제항목 적용방안을 제시하고자 한다.

II. 사이버보안 규제동향

2.1 국외 사이버보안 규제동향

2.1.1 Regulatory Guide 5.71[5]

미국의 원자력법 10CFR 73.54[4]에서는 원자력시설에 대해 안전기능, 보안기능, 비상대응기능에서 설계기준위협에 따라 영향을 받는 디지털 시스템에 대해 사이버보안을 고려하여 설계할 것을 명시하였다. 미국의 원자력규제위원회(NRC)는 원자력 시설에서 사용하는 디지털 컴퓨터와 통신, 네트워크를 사이버공격으로부터 보호하며 미연방법 10CFR73.54을 준수하기 위한 규제지침으로 RG(Regulatory Guide) 5.71을 발행하였다.

이 지침은 미국표준기술연구소(NIST, National Institute of Standards and Technology)에서 개발한 NIST SP800-53과 SP800-82을 활용한 사이버보안 표준과 보안조치항목을 이용하여 기술적, 운영적, 관리적 보안조치항목을 언급하고 있다. RG 5.71의 구성은 다음과 같으며 사이버보안 프로그램 수립, 이행 및 유지에 대해 기술하고 있다.

부록 A는 사이버보안계획 작성을 위한 양식을 제공하고 부록 B, C는 KINAC RS-015와 유사한 항목으로 표 1. RG 5.71 Technical Security Control, 표 2. RG5.71 Operational Security Control 및 표 3. RG5.71 Management Security Control로 되어있다.

사이버보안계획 중 보안조치활동은 사이버보안의 대상이 되는 CDA에 대해서 적용한다. CDA를 식별하기 위해서는 먼저 CS을 식별한 후 어떤 자산들이 CDA에 포함되는지 분석해야 한다. CDA는 안전, 보안 및 비상대응 (SSEP, Safety, Security, Emergency Preparedness Function) 기능을

Table 1. RG 5.71 Technical Security Control

No	Security Control	Details
1.1	Access Controls	23 Items
1.2	Audit and Accountability	12 Items
1.3	Critical Digital Asset and Communications Protection	22 Items
1.4	Identification and Authe-ntication	9 Items
1.5	System Hardening	5 Items

Table 2. RG 5.71 Operational Security Control

No	Security Control	Details
2.1	Media Protection	6 Items
2.2	Personal Security	2 Items
2.3	System and Information Integrity	11 Items
2.4	Maintenance	3 Items
2.5	Physical and Environmental Protection	9 Items
2.6	Defensive Strategy	1 Items
2.7	Defense-in-Depth	1 Items
2.8	Incident Response	8 Items
2.9	Contingency Planning	7 Items
2.10	Awareness and Training	10 Items
2.11	Configuration Management	9 Items

Table 3. RG 5.71 Management Security Control

No	Security Control	Details
3.1	System and Service Acquisition	6 Items
3.2	Security Assessment and Risk Management	3 Items

수행하는 디지털자산으로 다음의 기준으로 식별이 가능하다.

- SSEP 기능을 수행하는 디지털자산
- SSEP 기능에 악영향을 미치거나 SSEP 기능을 수행하는 CS 혹은 CDA에 악영향을 미칠 수 있는 디지털자산
- SSEP 기능을 수행하는 CS 혹은 CDA로 접근경로를 제공해주는 디지털자산
- CS 혹은 CDA를 지원하는 디지털자산
- 설계기준위협에 정의된 사이버위협으로부터 상기 시스템들을 보호하는 디지털자산

원자력발전소는 심층방호 전략을 적용하여 설계기준위협에서 정한 사이버 공격으로부터 디지털자산을 효율적으로 보호하여야 한다. CDA 사이버보안 등급을 Level 0에서 4까지로 총 5가지로 구분하여 각 경계에서 통신은 감시되고 숫자가 클수록 높은 사이버보안성이 수행되어야 한다. 등급에 따라 적절한, 탐지, 예방, 지연, 완화 및 복구를 위한 보안조치들이 적용되어야 한다. 심층방호 전략에서 방호전략 하나 또는 보안조치 실패가 SSEP 기능에 악영향을 끼치면 안된다. 이런 등급별 조치는 CDA에 사이버 공격이 시도되어도 침해영향 및 파급을 최소화하기 위함이다.

2.1.2 Regulatory Guide 1.152 Rev. 3 [10]

NRC는 Regulatory Guide 1.152 "Criteria for Use of Computers in Safety Systems of Nuclear Power Plant", Rev. 3 (2010)에서 기존의 Rev. 2에서 제시한 안전기능을 수행하는 디지털 기반 계측제어계통 및 기기를 대상으로 하는 사이버보안 내용을 삭제하고 악의적 행위에 대한 평가 부분도 삭제하였다. 이것으로 RG 1.152 Rev. 3은 비악의적 요소인 무작위 접근통제, 바람직하지 못한 작동으로부터 보호, 문서화되지 않거나 잘못된 프로그램 코드 작성으로부터 보호되는 개발환경에 대한 지침만을 제시한다. 또한 원자력발전소 개발 생명주기 단계 중 개념, 요구사항, 설계, 구현 및 시험단계에서 필요한 시스템형상과 개발활동에 대해서 기술하고 있다.

2.1.3 Nuclear Energy Institute

Nuclear Energy Institute는 미국 원자력 산업협회로 원자력업계에 영향을 미치는 주요 입법 및 규제문제에 대해 정책을 개발하고 있으며 원자력 산업에 대한 정확하고 적절한 정보를 제공하고 있다. NEI 08-09에서는 사이버공격으로부터 보호해야 하는 디지털자산 관리조치에 대한 방법을 제시하고 있다[9].

NEI 10-04에서는 원자력시설에 대한 CS와 CDA 식별 후 선별적인 통제항목 적용에 대한 방법론을 제시하였다. NEI 13-10에서는 CDA에 대한 사이버보안 조치를 처리하기 위해 중요도와 특성을 분석하여 간소화 할 수 있는 지침을 제공하였다.

제시된 방법론은 CDA의 영향평가를 수행하여 영향이 낮은 CDA에 대해 전체 보안조치 항목을 적용하는 대신 대안조치를 통한 최소한의 보안조치를 수행하는 방안이다[7]. 전체 CDA에 대한 영향평가 과정에서 직접필수디지털자산(Direct CDA)와 비직접필수디지털자산(Non-Direct CDA)를 분류하고

Non-Direct CDA은 비상대응(EP, Emergency Preparedness), 보조설비(BOP, Balance of Plant), 간접(Indirect) 세 가지로 구분한다. EP CDA는 EP 기능을 수행하는 독립된 대체수단을 보유하고 EP기능만을 지원하고 SSEP 기능을 지원하지 않는 CDA이다. BOP CDA는 Important-to-Safety 분석에 사용된 5가지 항목에 해당되진 않지만 원자력발전소의 반응도에 직간접으로 영향을 줄 수 있고 계획되지 않은 원자로 정지 혹은 과도상태를 초래할 수 있는 시스템인 경우 BOP CDA로 구분한다. Indirect CDA는 사이버 공격이 발생하더라고 안전 또는 안전기능에 악영향을 미치지 않으며 사용자가 대체할 수 있는 수단이 존재하는 CDA이다.

2.2 국내 사이버보안 규제동향

2.2.1 KINAC RS-015 [6]

원자력시설 등의 방호 및 방사능방재대책법 제9조(물리적방호에 대한 원자력사업자의 책임) 및 동법 시행령 제16조(원자력시설등의 방호요건), 동법 시행규칙 제5조(물리적방호규정등의 작성), 원자력안전위원회 고시 제2014-83호(물리적방호규정등의 작성내용의 항목별 세부작성기준)에 의거하여 원자력통제기술원에서는 원자력시설 등의 사이버보안 대응을 위해 2014년 10월에 규제지침 KINAC/RS-015를 발행하여 규제기준을 마련하였다.

원자력시설의 컴퓨터 및 정보시스템 보안에 대한 기술기준 KINAC/RS-015는 사이버보안계획의 수립 및 이행, CS/CDA 식별, 심층방호전략, 사이버보안조치, 비상사건 대응 및 복구, 사이버보안계획의 유지, 기록 유지 및 처리에 관한 사이버보안 심사 및 검사의 기준이 된다.

원자력사업자는 사이버보안계획을 수립한 후 효과적으로 대처하고 유지하기 위해 사이버보안 프로그램 수립, 적용, 감시, 보안프로그램 검토, 변경통제, 기록보존함으로써 지속적인 감시와 평가 및 변경 통제 활동을 수행하여 사이버보안 프로그램을 유지한다.

사이버보안 기술기준 만족을 위해 수행업무에 따라 1~7단계로 분류할 수 있으며 기술기준의 주요 내용은 다음과 같다.

- 사이버보안 조직구성 :사이버보안 업무 수행 조직과 비상사건 대응 조직구성
- CDA 식별 : CS와 CDA 식별
- 심층방호 및 비상대응 : CDA에 대한 심층방호 등급분류 및 분류기준 이행과 비상사건 대응 및 이행
- 매체통제 : 이동형매체 및 모바일기기에 대한 통제와 유지보수 및 시험장비에 대한 통제
- 무결성유지 : 시스템 및 정보의 무결성을 보장하기 위한 정책 수립과 정책을 이행하고 유지하기 위한 조치
- 보안조치 1 : 운영적, 관리적 보안조치이행
- 보안조치 2 : 기술적 보안조치 이행

KINAC/RS-015은 기술분야, 운영분야, 관리분야 세 가지로 구분하여 사이버보안 조치항목을 언급하고 이의 이행을 요구하고 있다. 기술적 보안조치는 5가지의 통제항목과 세부적으로 62개의 세부항목으로 구분되며 운영적 보안조치는 6가지의 통제항목과 세부적으로 31개의 항목이 있다. 그리고 관리적 보안조치는 2개의 통제항목과 8개의 세부항목으로 구성되어 있다.

III. 기술적 보안조치항목 분석

3.1 필수디지털자산 특성

규제지침에 따른 CDA 식별 방법을 통해 식별된 CDA은 보안조치항목 101가지를 이행해야 한다. 하지만 수천개의 CDA에 모든 보안조치항목을 이행하는 것은 CDA의 특성을 고려하지 않은 것으로 비효율적이다. CDA의 특성에 따라 보안조치항목을 구분할 수 있다면 사이버보안 규제지침 이행을 효율적으로 할 수 있다.

디지털자산은 운전원의 조치가 없더라도 다수의 수학적 계산 또는 논리연산을 포함하는 내부 저장 프로그램과 알고리즘을 수행하기 위한 하드웨어, 펌웨어, 소프트웨어의 조합을 사용하는 Programmable Device으로 구분할 수 있으며 데스크탑, 노트북, 전송기, 지시계 및 네트워크 스위치 등으로 구분된다. 이러한 디지털자산은 표4. 디지털자산 특성 같이 하드웨어와 소프트웨어 특징으로 구분할 수 있으며 이러한 특성에 따라 그림 1. CDA Additional Evaluation Process와 같은 순서도에 따라 분류가 가능하며 식별된 그룹에 따라 조치해야 할 통제항

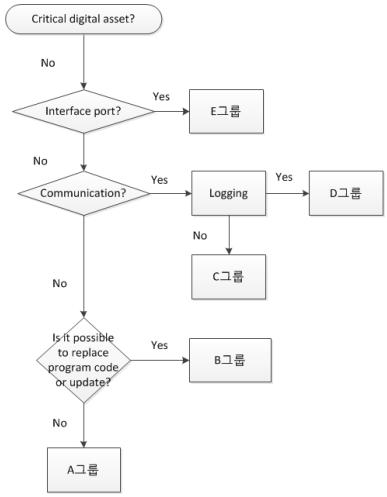

Fig. 1. CDA Additional Evaluation Process

목을 구분할 수 있다.

3.2 기술적 보안조치 불필요항목

KINAC/RS-015에 따라 CDA로 식별된 디지털 자산은 기술적보안조치 이행이 요구된다. 그림1과 같이 CDA의 특징에 따라 추가분류가 가능하며 분류된 CDA은 표4. Characteristics of digital assets과 같은 하드웨어와 소프트웨어 특징을 갖는다. 하드웨어 관점에서 컴퓨터, 외부포트, 통신기능 유무와 소프트웨어 관점에서 로그기능, 소프트웨어 수정 및 업데이트에 따라 보안조치가 필요하지 않는 항목이 존재한다. 예를 들어 필드에 설치되는 계측기는 해당정보를 아날로그(4~20mA) 또는 디지털(0 or 1) 신호를 실배선을 통해서 전송하고 있다. 통신 프로토콜을 사용하지 않기 때문에 통신기능 사용으로 발생할 수 있는 사이버공격으로부터 대비하고자 수립한 통제항목은 적용이 불필요하다.

Table 4. Characteristics of digital assets

Classification	Attributes
Hardware	Desktop, Laptop
	Network connectivity
	Data Communication port
	Human Machine Interface
Software	Logging
	Logical Security Mechanism
	Domain Name Service
	Software code can be altered /updated

3.2.1 인터페이스를 위한 포트

외부포트는 제어시스템의 주요 취약점 중 하나이다. 주요 사이버공격이 외부포트에 비정상적인 입력 데이터를 의도적으로 보내어 제어시스템 기능의 오작동을 유발하고 있다. 이란 원전시설을 공격한 스턱스넷도 외부포트인 USB를 통해서 시스템에 침투한 것으로 알려져 있다. 휴대용 매체 및 모바일 기기에 대한 사용제한을 위해 CDA에 접근 가능한 모바일 기기와 휴대용 매체의 사용제한에 대한 절차수립 및 이행을 요구하고 있다.

휴대용 매체 및 모바일 기기로는 CD, DVD, USB 및 노트북 등 디지털 저장장치가 해당되며 이러한 기기들은 원자력시설 조직에서 수립한 보안정책이 적용되지 않기 때문에 위험요소가 된다. 이런 휴대용 매체 및 모바일 기기는 CDA의 인터페이스를 위한 외부 포트를 통해 연결된다. CDA에 외부 포트가 존재하지 않는다면 휴대용 매체 및 모바일 기기 접근 통제항목을 이행할 필요가 없다. 인터페이스를 위한 포트가 존재하지 않을 때, 적용이 불필요한 조치항목은 다음과 같다.

- 휴대용 매체 및 모바일 기기 접근 통제

3.2.2 통신기능

많은 사이버 공격은 네트워크를 경유하여 시스템에 접근하며, 네트워크 설계 및 장비 취약점을 이용하여 데이터 변조, 삭제, 탈취한다. 규제지침에서는 통신기능으로 발생할 수 있는 사이버공격 예방을 위해 CDA의 데이터 이동 통제, 네트워크 접근통제와 통신의 보호 등 관련 이행방안을 제시하였다.

따라서 통신기능이 없는 CDA에 대해 적용이 불필요한 조치항목은 다음과 같다.

- 데이터이동 통제
- 네트워크 접근통제
- 안전하지 않은 프로토콜의 제한
- 무선연결 금지
- 특정 프로토콜 가시성
- 타임스탬프

- 공유자원
- 전송무결성
- 전송기밀성
- 신뢰경로
- 보안매개변수의 전송
- 세션의 보호
- 하드웨어 구성
- 외부시스템의 사용

3.2.3 로그 기능

로그 기능은 시스템 작동상태의 기록과 보존, 동작 분석 활용에 이용될 수 있다. 보안감사 로그는 로그인 활동 정보를 통해 보안 관련 정보를 제공해야 한다. 로그 관리를 적절하게 함으로써 시스템에 접속하는 사용자의 정보를 확보하여 불법적인 접속 및 사용을 금지할 수 있다. 보안조치항목 이행을 위해 로그 기능을 사용하는 항목은 11가지가 있다.

따라서 CDA에 로그 기능이 없을 경우, 적용이 불필요한 항목은 다음과 같다.

- 계정관리기능
- 접속실패 기록
- 시스템 사용공지
- 이전 접속기록 공지
- 세션잠금
- 식별이나 인증 없이 허가된 활동
- 로그 저장 용량
- 로그 저장용량 초과 시의 대응
- 감사대상 기록의 검토 분석 및 보고
- 감사대상 기록의 축약 및 생성
- 패스워드 요건

3.2.4 소프트웨어 코드 수정 및 업데이트

CDA가 소프트웨어를 사용하는 경우, 악의적인 의도에 의해 소프트웨어가 변경될 수 있다. 많은 소프트웨어 개발자 및 사용자들이 보안에 대한 인식이 부족한 상황이며 업데이트 체계에 취약점이 있으면 공격자에게 악용될 소지가 크다. 이러한 이유로 규제지침에서는 소프트웨어 관련 사이버보안을 위한 요구사항이 있다.

따라서 소프트웨어를 사용하지 않는 CDA은 이행이 불필요하다.

- 불필요한 서비스 및 프로그램의 제거
- 파일시스템 및 운영체제 변경 승인
- 운영체제, 응용프로그램 및 제3자 소프트웨어 설치 및 업데이트
- 모바일 코드
- 서비스거부 공격으로부터의 보호

3.3 관리적, 운영적 조치사항으로 이전이 요구되는 기술적보안조치

기술적보안조치항목 중에서도 세부적으로 분석하면 기술적인 조치보다는 관리적, 운영적 조치를 요구하는 사항이 존재한다. 이 항목들은 관리적, 운영적 보안조치 항목으로 이동을 제안한다.

3.3.1 제3자 제품사용

산업제어시스템을 사용하는 사용자나 공급사는 서드파티제품을 사용하는 경우에도 서드파티의 종속성을 문서화하지 않고 추적관리를 하지 않는 경우가 대다수이다. 또한 타사 제품에 대한 구성요소를 알지 못하기 때문에 사용자에게 제품에 대한 취약점을 알리기 어렵다.

따라서 규제요건에서는 서드파티제품으로 발생할 수 있는 사이버위협 대비를 위해 요건을 개발하였다. CDA에 서드파티제품을 일부 또는 전부에 대해 제3자가 개발한 제품을 사용하는 경우, 지속적인 보안기능 수행을 위해 서드파티와 계약체결 등 서비스를 지원받기 위한 방안을 요구하고 있다.

서비스 지원계약은 원자력시설 운영자와 기기공급사 또는 기기공급사와 서드파티 간 체결되어야 하는 행정적인 요소로 CDA의 현장설치 이후 관리적, 운영적 보안조치로 이행되는 것이 합리적이다.

3.3.2 식별자 관리

식별자 관리항목은 6가지 세부이행사항으로 이루어져있다. 세부사항으로는 사용자 식별, 신분검증, 공식적인 절차에 따른 사용자 식별자 발급, 30일간 사용이 없을 경우 식별자 사용 불가조치, 사용기록에 대한 유지 등이다. CDA를 사용하는 사용자 식별에 대한 이행사항으로 기술적으로 조치할 사항은 없으며 운영자가 행정적으로 조치를 수행해야 할 부분이다. 기술적으로 조치할 사항이 없는 행정적인 요구사항이

므로 관리적, 운영적 보안조치로 이행하여야 한다.

3.3.3 호스트기반 침입탐지시스템

호스트기반 침입탐지시스템(HIDS, Host Intrusion Detection System)은 침입탐지시스템의 한 종류로 컴퓨터 시스템의 내부를 감시하고 분석하는데 사용된다. IPS, IDS와 같은 외부 인터페이스를 감시하는 것과는 구별된다.

모든 CDA에 HIDS를 이행하는 것은 현실적으로 불가능하다. CDA 고유 기능 외에 다른 기능을 수행하는 것을 금지토록 KINAC/RS-015 2.6.5 최소 기능성에서 요구하고 있어 서로 요건이 상충되며 보안을 위한 프로그램 설치시 성능에 영향이 없음을 증명하는 것이 어렵다.

따라서, 별도로 HIDS의 적용이 필요한 CDA를 식별하고 HIDS를 위한 지침을 수립하여 관리적, 운영적으로 정책을 수립하는 것이 필요하다.

3.3.4 인증 불가한 보안

HMI(Human-Machine Interface)가 운영 여건상 인증 기능을 지원하기 어려운 경우에 적절한 물리적 보안 정책을 수립하여 조치사항 이행 후 사이버보안 측면에서 문제가 없음을 보여야 한다. 구체적인 요구사항으로는 사용자 승인, 식별, 사용에 대한 기록행위, 물리적으로 승인된 자에게만 접근 허용, SSEP 기능에 대한 악영향 검증, HMI 사용에 대한 기록을 별도록 유지이다. 이것은 CDA의 기능을 활용하여 조치하는 것이 아니라 물리적 보안조치를 수행하고 승인된 자에게만 접근을 허용하도록 하는 운영적, 관리적 측면의 조치사항이다.

IV. 그룹별 보안조치 적용결과

CDA를 특성별로 그룹화하여 각 그룹별로 적용해야 할 보안조치를 구분할 수 있다. CDA로 식별된 디지털자산을 그룹A~F까지 재식별한 후 적용해야 할 보안조치 항목 수의 경감결과는 표 5. Result of applying a security control to a CDA group와 같다.

APR 1400 모델에 적용 결과 3,195개의 필수디지털자산에 대해 A그룹 663개, B그룹 131개, C그룹 543개, D그룹 353개, E그룹 1,424개로 분류되었다. 결과적으로 그룹별로 CDA를 구분하여 보안조치를 적용하면 27~94%에 해당하는 비율로 보안조치를 줄일 수 있다. 보안조치를 CDA 특성에 맞게 최적화 한다면 사이버보안 규제지침을 이행하는 원자력시설 관련자의 업무 효율성을 증대시키고 불필요한 비용을 감소시킬 수 있는 효과를 기대할 수 있다. 그룹별로 원자력시설에 포함되는 기기들은 표 6. Example of Equipment list by grouping과 같이 정리할 수 있다.

Table 5. Result of applying a security control to a CDA group

Group	Number of security control before grouping	Number of security control after grouping	Reduction ratio (after/ before)
A	62 Items	22 Items	27%
B		33 Items	39%
C		26 Items	56%
D		37 Items	78%
E		40 Items	79%

Table 6. Example of Equipment list by grouping

Group	Example of Equipment
A	Indicator, Transmitter
B	Digital Controller, Control Panel
C	Digital Transmitter, Camera
D	Receiver box, Communication Control Unit
E	PLC, DCS

V. 결 론

디지털시스템 기술의 발전으로 원자력시설을 운영하기 위한 설비들은 디지털화 추세이며 그에 따라 성능향상과 운전원의 편의성은 증대되었지만 사이버공격의 위험에 노출되었다.

이러한 사이버보안 문제에 적극적으로 대응하고자 국내에서는 주요기반시설에 사용되는 디지털시스템에 대한 사이버보안 관련 정책이 수립되고 법제화되면서 원자력시설 또한 사이버공격에 대비할 수 있는 설계

가 요구된다. CDA는 사이버보안 조치사항을 이행해야 하는데 원자력시설에서 CDA의 기능과 특성을 고려하지 않아 비효율적인 면이 존재한다.

규제지침의 보안조치사항 연구결과 CDA의 특성에 따라 적용이 필요없는 항목이 있음을 식별하였고 적용하지 않더라도 사이버보안을 약화시키지 않음을 확인할 수 있었다. 의미있는 보안조치 감경은 사이버보안 업무를 수행하는 책임자에게 효율성과 편의성을 증대할 수 있을 것으로 기대한다.

향후 과제로는 CDA에 대한 기술적 조치사항을 이행하기 위한 방안으로 계통레벨에서의 대안조치 방안, 관리적 대안조치 방안에 대한 연구가 필요하다.

References

〔1〕 "W32.Stuxnet Dossier", Symantec, 2011
〔2〕 "W32.Duqu", Symantec, 2011
〔3〕 U.S NRC 10CFR73.1 "Physical Protection of Plants and Materials", U.S NRC, 2008
〔4〕 U.S NRC 10CFR73.54 "Protection of Digital Computer and Communication System and Networks", U.S NRC, 2009
〔5〕 U.S NRC Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities", NRC, 2009
〔6〕 "Regulatory Standard 015", KINAC, 2016
〔7〕 NEI, "Cyber Secuirty Control Assessments", NEI 13-10, 2017
〔8〕 NEI, "Identifying Systems and Assets Subject to the Cyber Security Rule", NEI 10-04, 2012
〔9〕 NEI, "Cyber Security Plan for Nuclear Powr Reactors", NEI 08-09, 2010
〔10〕 U.S NRC Regulatory Guide 1.152 ″Criteria for Use of Computers in Safety Systems of Nuclear Power Plants″, U.S NRC, 2010
〔11〕 "Common Cyber security Vulnerabilities ICS", DHS, 2011
〔12〕 "SIMATIC NET Profibus Network Manual", SIEMENS
〔13〕 "SMQ320C32 Digital Signal Processor", Texas Instrument
〔14〕 NIST Special Publication 800-53 Rev.3, "Recommended Security Controls for Federal Information Systems and Organizations", NIST, 2009

〈저자소개〉

최 윤 혁 (Yun-Hyuk Choi) 정회원
2009년 8월: 한양대학교 전자공학과 졸업
2019년 2월: 고려대학교 정보보호대학원 석사
2010년 8월~현재: 한국전력기술 디지털보안팀장
〈관심분야〉 정보보호, 전자공학, 통신공학

이 상 진 (Sang-Jin Lee) 종신회원
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학 대학 조교수
2008년 3월~현재: 고려대학교 정보보호연구원 디지털포렌식연구센터장
2017년 3월~현재: 고려대학교 정보보호대학원장
〈관심분야〉 대칭키 암호, 정보은닉이론, 컴퓨터 포렌식