Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.3, Jun. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.3.537

원전 제어시스템 사이버보안 위험 분석방법의 효율성 개선

이 신 우,[1†] 이 중 희[2‡]
[1,2]고려대학교 (대학원생, 교수)

Improving the Efficiency of Cybersecurity Risk Analysis Methods for Nuclear Power Plant Control Systems

Shin-woo Lee,[1†] Jung-hee Lee[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

국내 원전은 방사능방재법에 의거하여 '정보시스템 보안규정'이 수립됨과 함께 조직구성부터 자산의 기술적/운영적/관리적 보안조치에 이르는 사이버보안 체계를 도입하여 운영하고 있다. 단계별 접근법, 물리적방호체계의 대안조치 등이 시도되고 있지만, 관리대상의 감소는 이루어지지 않기 때문에 현장의 한정된 인력으로 운영하기엔 보안 역량의 부담이 가중되고 있다. 본문에서는 원전 안전기능을 수행하는 A1 유형 자산에 대해 정비규정(MR, Maintenance Rule), EPRI 기술적 평가 방법론(TAM, Technical Assessment Methodology)를 활용하여 정비적인 측면과 기기 특성에 대한 측면으로 분석하였다. 이를 통해 사이버침해로 인한 자산기능의 영향을 재분석하는 방안을 제시한다.

ABSTRACT

Domestic nuclear power plants operate under the establishment of the "Information System Security Regulations" in accordance with the Nuclear Safety Act, introducing and implementing a cybersecurity system that encompasses organizational structure as well as technical, operational, and managerial security measures for assets. Despite attempts such as phased approaches and alternative measures for physical protection systems, the reduction in managed items has not been achieved, leading to an increased burden on security capabilities due to limited manpower at the site. In the main text, an analysis is conducted on Type A1 assets performing nuclear safety functions using Maintenance Rules (MR) and EPRI Technical Assessment Methodology (TAM) from both a maintenance perspective and considering device characteristics. Through this analysis, approaches to re-evaluate the impact of cyber intrusions on asset functionality are proposed.

Keywords: Critical Digital Asset, Maintenance Rule, Technical Assessment Methodology

I. 서 론

국내 원전에서는 2016년 '정보시스템 보안규정'의 수립과 동시에 물리적방호 체계와 함께 제어시스템 사이버보안 체계는 원자력시설의 안전을 보장하는 방향으로 진행되어 왔다. NRC, NEI, KINAC 에서 발행된 기술기준 및 심·검사기준을 참조하여 조직구성, 필수디지털자산의 식별, 심층방호 구조, 최종적으로 기술적/운영적/관리적 보안조치에 이르는 사이버보안체계가 도입되었다. 체계가 심화됨에 따라 사업소별 1000~2000개가 넘는 필수디지털자산이 식별되었고, 각 자산마다 101가지 보안조치의 적용이 수반되었다. 자산 평가 결과에 따른 단계적 접근법,

Received(04. 18. 2024), Modified(1st: 05. 28. 2024, 2nd: 05. 29. 2024), Accepted(05. 30. 2024)
† 주저자, blac4coffee@korea.ac.kr
‡ 교신저자, j_lee@korea.ac.kr(Corresponding author)

기존의 원전 물리적방호체계의 대안조치 도입을 통해 효율적인 보안조치 이행이 시도되고 있지만,[18][19][20][21] 원천적인 관리대상의 감소는 이루어지지 않고 있다.

본 논문에서는 안전기능에 영향을 미치는 필수디지털자산 중 단계가 가장 낮은 A1 유형의 자산에 대해 정비체계 관점과 자산특성 기반의 사이버보안 관점으로 분석을 수행하고, 보안조치의 부담을 낮출 수 있는 방안을 살펴보고자 한다.

II. 기존 자산식별 및 보안조치

2.1 NRC 필수디지털자산 식별기준

원자력규제위원회(NRC, Nuclear Regulatory Commission)는 연방규정[1]에 따라 원자력사업자에게 설계기준위협을 포함하는 사이버공격으로부터 안전 및 보안과 관련한 디지털자산이 보호받도록 보장해야 함을 요구하며, 대상 자산을 '필수디지털자산(CDA, Critical Digital Asset)'으로 정의한다.

CDA를 식별하기 위해선 자산이 속한 계통이 SSEP 기능을 수행 또는 지원하는 지에 대해 평가해야 한다. 평가기준에 부합하는 계통을 '필수계통(Critical System)'으로 정의하며, 여기서 SSEP는 안전(Safety), 보안(Security), 비상대응(Emergency Preparedness)을 의미한다. Fig 1. 은 필수계통의 평가 프로세스를 다이어그램으로 나타낸 것이다.

CDA 는 Fig 2. 와 같이 필수계통 내의 디지털자산을 분석함으로써 평가한다. 해당 자산이 ① SSEP 기능의 수행, ② SSEP 기능으로의 악영향, ③ SSEP 기능에 악영향을 줄 수 있는 경로제공, ④ 필수계통 및 CDA 지원, ⑤ 사이버공격으로부터 보호 총 5가지 기준 중 하나에 해당하면 CDA 로 식별된다.

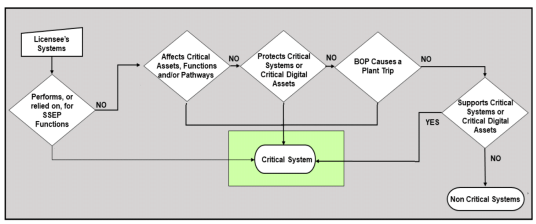


Fig. 1. Evaluation Process for determining Critical System[2]

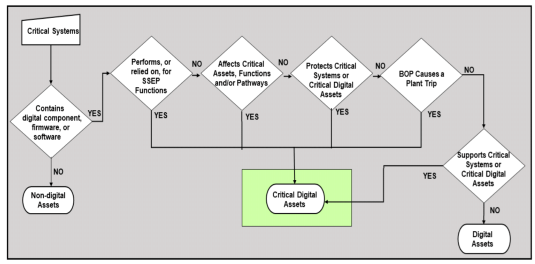


Fig. 2. Evaluation Process for determining CDA[2]

2.2 NEI 필수디지털자산 식별 및 보안조치 기준

미국원자력협회(NEI, Nuclear Energy Institute)는 NRC 연방규정에 따른 원자력발전소 사이버보안 규제요건을 충족하기 위해 사업자가 이행할 수 있는 식별과 보안조치에 관한 기술기준을 제시한다.[3][4]

NEI 13-10 은 식별된 필수디지털자산을 중요도에 따라 평가하고, 결과에 따른 보안조치 적용 방법을 제시한다.[4]

Direct CDA는 A1~B3 까지의 유형으로 분류하는데 유형을 구분짓는 자산특성은 Table 2. 와 같이 확인할 수 있다.

Table 1. Consequence Assessment of CDA[4]

Type	Assessment Standard
EP CDA	1. Only supports an EP function 2. Alternate means that do not adversely affect EP function 3. Requirements - Perform EP Function, including offsite communication - One or more of the alternate means - Performing intended function & an appropriate response - Using by trained personnel - Implement baseline protections
BOP CDA	SSCs in balance of plant could directly or indirectly affect reactivity at a nuclear power plant and could result in an unplanned reactor shutdown or transient.
Indirect CDA	1. No adverse impact on Safety, Security 2. Not assets solely relied-on for making decisions. 3. The compromise can be detected, Compensatory measures taken prior to adverse impact

Table 2. Direct CDA Class Descriptions[4]

Type	Description
Common	[Software] ▪ Program code (instruction-level) [HMI] ▪ Operational parameters can be changed ▪ Does not support multi-users and individual authentication for users ▪ Configuration changes can also be made using a maintenance tool ▪ Firmware updates not supported (except B3 class) ▪ Only contains vendor's software ▪ Does not perform event logging [Hardware] ▪ PROM, RAM, EEPROM and possibly integrated components ▪ Certain bulk storage for data
B3	▪ Support firmware update/replacement ▪ Configuration changes by local port ▪ Support bulk data extraction ▪ The functionality and configuration of the CDA can also be altered via these communication link ▪ The CDA has a local, special purpose communications interface
B2	▪ Communication limited
B1	▪ Communication limited
A3	▪ No communication
A2	▪ No communication
A1	[Software] ▪ Program code cannot be altered and does not utilize or support operating system or application software ▪ Changes to operational parameters or operational settings can only be implemented using maintenance and test equipment [Hardware] ▪ No HMI ▪ No peripherals, interfaces or ports

2.3 국내 필수디지털자산 식별 및 보안조치 적용

국내 법령[원자력안전위원회고시 제2022-6호]에 따른 안전기능은 ① 원자로냉각재압력경계의 건전성 확보, ② 원자로의 안전정지 및 정지상태 유지, ③ 소외피폭선량 제한치를 초과할 우려가 있는 상황을 예방하거나 완화시키는 기능으로 정의되어 있다. 원전에서는 최종안전성분석보고서(FSAR) '표 3. 2-1 구조물,계통 및 기기 등급분류 목록'에 위 법령의 기준을 적용하여 안전등급을 분류한다. 국내 제어시스템 사이버보안 심검사기준[KINAC/RS-015]을 적용하여 필수계통을 식별할 때, FSAR 와 동일한 안전등급 기준을 적용한다.

50. - Feedwater Pump Turbine System						
1) Feedwater Pump Turbine	NNS	D	Non-1E	A	Ⅲ	30) F
2) Other devices	NNS	D	Non-1E	A	Ⅲ	30) F
3) Other piping	NNS	D	N/A	S	Ⅲ	
51. FW- Main Feedwater System						
1) From the steam generator to the main steam valve penetration anchor	2	B	1E	Q	I	
2) Other feedwater piping	NNS	D	N/A	S	Ⅲ	
3) Feedwater pump	NNS	D	Non-1E	A	Ⅲ	30) F
4) Feedwater booster pump and electric motor	NNS	D	Non-1E	A	Ⅲ	30) F
5) Startup feedwater pump and electric motor	NNS	D	Non-1E	S	Ⅲ	
6) Feedwater heater	NNS	D	N/A	A	Ⅲ	30) F

Fig. 3. Shin-Kori #3,4 FSAR Table 3.2-1

CDA 로 식별된 자산은 Fig 4. 와 같이 중요도 평가 (Consequence Assessment)를 거쳐 자산 유형을 결정한다.

비상대응(EP, Emergency Preparedness)기능 평가는 방사선 비상대응체계에 근거한다. 방사선 비상계획의 수립에 관한 세부기준[방사능방재법 시행규칙 제13조]에 따라 백색, 청색, 적색 비상에 대한 세부기준이 마련되어 있다. 이들 비상은 Fig 5. 의 다이어그램으로 구성되어 있으며, 해당 조건이 충족되었을 때 방사선비상이 발령된다. 그러므로 이러한 조건에 해당하는 기능으로만 구현된 설비는 EP 기능만을 위한 자산으로 설계되었음을 알 수 있다.

ITS-5 기능평가 기준은 '원자력발전소 반응도에 직·간접적으로 영향을 줄 수 있고 계획되지 않은 원자로 정지 혹은 과도상태를 초래할 수 있는 보조 설비의

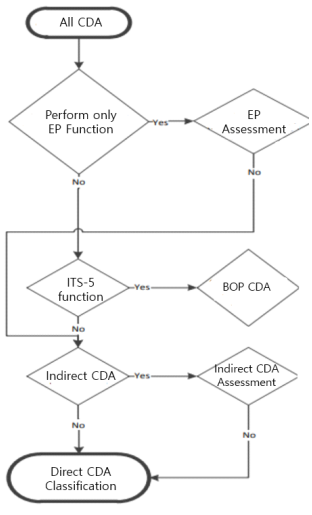


Fig. 4. Consequence Assessment[4]

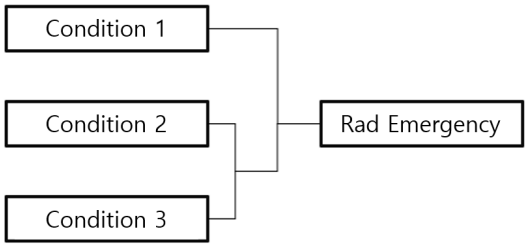


Fig. 5. Radiation emergency declaration diagram

구조, 계통 또는 기기'로 명시되어 있으며 이에 대한 근거는 원자력시설의 인허가문서 중 최종안전성분석 보고서를 통해 판단할 수 있다.

EP CDA, BOP CDA 로 식별되지 않는다면 Indirect CDA 중요도 평가를 적용할 수 있다. NEI 13-10 의 기준을 바탕으로 수행하며, 평가 항목은 아래와 같다.

① CDA 가 안전 또는 보안결정을 내릴 때 참조하는 유일한 지시계(Indicator) 또는 경보계(annuciator)인가

② CDA가 손상될 경우 안전 또는 보안 기능에 즉시 악영향을 주는가

②-1 탐지 전략 평가

②-2 악영향 제거를 위한 보상조치 전략 평가

②-3 탐지 및 보상조치 전략 시간 평가

Direct CDA의 유형 분류 과정은 Table 3. 과 같이 PC 설비인 C 유형부터 마지막 A1 유형까지 순서대로 진행된다. B3 유형은 시리얼통신 외의 다른 통신포트 또는 USB/메모리카드를 통한 구성 및 펌웨어 업데이트가 가능한 경우 해당한다. 여기서 B3 유형에 해당하지 않으나 시리얼통신을 통하여 프로그램 변경이 가능하면 B2, 변경이 불가하면 B1 유형으로 분류된다. A3 유형은 내장된 HMI에 의해 내부설정(운전변수 포함) 변경이 가능한 경우 해당한다. 내부설정(운전변수 제외) 변경이 불가한 경우에는 A2 유형에 해당한다. 최종적으로 운전변수 변경이 불가하거나 로컬/일체형 HMI가 없는 경우에는 A1 유형으로 분류한다.

본 논문은 원전의 대표적인 A1 유형 자산인 APT3700N 전송기를 대상으로 세부 분석을 수행한다. 해당 전송기는 원전에서 안전기능을 수행하기 위한 요건을 만족하며, 발전소 공정 중 발생하는 압력, 수위, 유량을 측정하여 상위 시스템으로 4~20mA 신호전달 기능을 수행한다. 전송기 내부의 설정 관리를 위해 HART 통신기능을 갖고 있다.[6][7]

APT3700N 전송기를 대표 자산을 설정하는 이유

Table 3. CDA Attributes for types

CDA Attributes			A1	A2	A3	B1	B2	B3	C
S/W	Replacement /Install	By vendor	○	○	○	○	○	○	○
		By user in workplace	X	X	X	X	X	○	○
	Operational Parameters Change	Using maintenance tool	○	N/A	N/A	N/A	N/A	N/A	N/A
		Local HMI	X	○	○	○	○	○	○
	Configuaration Change	Using maintenance tool	○	○	○	○	○	○	○
		Local HMI	X	X	○	○	○	○	○
		USB,Console port,Comm.	X	X	X	X	X	○	○
	HMI Access Control	Support	X	X	○	○	○	○	○
		Multi user/Authentication	X	X	X	X	X	X	○
		Perform logging	X	X	X	X	X	X	○
	Support Firmware update/replacement		X	X	X	X	X	○	○
	Comm. software	Support	X	X	X	X	○	○	○
		Change Configuration	N/A	N/A	N/A	X	X	○	○
H/W	HMI		X	○	○	○	○	○	○
	Supports only communications		X	○	○	○	○	○	○
	Contains a console port and restricted port		X	X	X	○	○	○	○
	Data storage	local	N/A	○	○	○	○	○	○
		external interface	N/A	X	X	X	X	○	○
	Physical access protection		X	X	○	○	○	○	N/A
	Communication	RS-232/422/485	X	X	X	○	○	○	○
		Other	X	X	X	X	X	○	○
		Change configuraiton	X	X	X	X	○	○	○

는 최신 노형 발전소에서 A1 유형 자산의 90~100%를 차지할 뿐만 아니라 특정 모델을 지정함으로써 논문의 모호성을 최대한 줄이고자 하기 때문이다.

중요도 평가가 완료되면 사업자는 자산별로 유형에 따라 기술적/운영적/관리적 보안조치를 이행하고 있다. 총 101가지에 해당하는 보안조치를 이행하게 되는데, A1 유형 자산은 이 중 32개의 보안조치를 이행하여 55건의 결과물을 도출해야 한다.

A1 유형 자산은 모든 기술적 보안조치의 적용에서 제외되어 있기에 많은 부분에서 원전의 운영체계나 정비체계로 관리되고 있다. 따라서 실제 현장 설비담당자는 인식의 제고와는 별개로 불필요한 업무의 일환이 될뿐더러, 디지털 네트워크 연결을 통해 위협 가능성이 더 높은 B1~C 유형 자산의 보안관리에 소홀해질 수 있다는 현실적인 문제에 직면한다.

Table 4. The A1 ratio by systems, assets

NPP Type	OPR-1	OPR-2	APR-1	APR-2
All CS	98	94	109	109
CS for A1	9	9	12	10
Ratio	9%	9%	11%	9%
All CDA	1787	1483	1901	2642
A1 CDA	150	84	138	154
Ratio	8%	5%	7%	5%

Table 5. Security measures for A1 type assets

Type	Controls	Results
Operational	Personnel Security	3
	System and Information Integrity	5
	Performing Maintenance	1
	Physical & Environmental Protection	17
	Cyber Security Awareness and Training	6
	Configuration Management	8
Administrative	System&Services Acquisition	10
	Evaluate And Manage Cyber Risk	5
Total		55

III. A1 유형 자산의 분석방법 개선

3.1 정비규정 관점에서의 자산 분석

3.1.1 정비규정 개요

정비규정은 원자력사업자에게 원전 구조, 계통, 기기(이하 SSCs)에 대한 정비 효율성 감시요건을 규제한다. SSCs 가 고유기능을 원활하게 수행하여 안전에 적합한지, 산업 전반의 운전경험이 고려되었는지 확인하는 것을 목표로 한다.

개발단계에서는 발전소 전 계통에 대한 기능을 안전 관련과 비안전 관련으로 구분하여 대상범위를 결정한다. 이후 안전중요도를 선정하고 성능기준을 설정한다.

이행단계에서는 설정된 성능기준을 기반으로 성능감시를 수행하면서 성능기준의 초과, 반복적인 기능고장 및 불만족스러운 성능변화 추이가 발생할 경우 집중감시 체제로 전환하며 감시가 효과적인 것으로 판단되면 일상감시 체제로 환류하는 프로세스가 수립되어 있다.

정비규정은 정비 효율성 감시를 위한 프로그램이다. 국내 원전의 원자력시설 '사보타주(Sabotage)'는 컴퓨터 및 정보시스템의 사이버공격으로 인해 발생할 수 있는 것으로 정의하고 있기 때문에 사이버 침해로 인한 구조, 계통, 기기의 의도치 않은 동작은 정비규정의 범주에 포함되는 것으로 판단할 수 있다. 또한 미국 원자력규제위원회는 정비규정과 제어보안의 근간이 되는 '10CFR50.65', '10CFR73.54' 모두 연방규정[10CFR50.2] 의 '안전관련(Safety-related)' 개념을 공유하고 있기 때문에 규제의 목적을 동일한 맥락에서 분석할 수 있다.

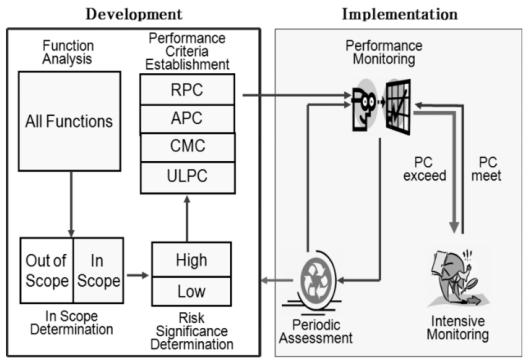


Fig. 6. Process diagram of maintenance rule[12]

3.1.2 A1 유형 자산에 대한 정비규정 개발

전송기 신호는 발전소 비상운전절차에서 일차성공경로 및 원자로 안전정지를 달성하는 데 필요한 정보를 운전원에게 제공하는 변수임을 설정하였다. 정비규정은 계통수준의 기능을 먼저 분석하고, 기능과 관련한 자산 관리대상으로 선정하여 감시한다. 따라서 A1 유형 자산이 속한 계통은 사고대응과 관련하는 원자로 냉각과 관련되어 아래 서술할 정비규정 프로세스에 따른 관리 대상에 속하는 것으로 설정하였다.

정비규정 대상범위를 선정하기 위해서는 계통 별로 기능을 분류하고 정의한다. 최종안전성분석보고서 및 설계문서, 도면, 운영절차서, 비상운전 절차서 등을 참고문서로 기능경계, 설계기준, 대상 SSC 및 배열이 결정되며 상세 분석내용이 작성된다. 최종적으로 전문가위원회를 거쳐 명시된 기준에 따라 대상범위를 선정할 수 있다.

안전중요도 결정은 대상범위에 포함된 관리대상에 대해서 성능기준 및 성능감시 수준을 설정하기 위해 수행하며 확률론적안전성분석평가(이하 PSA)와 델파이 중요도평가 방법을 통해 종합하여 결정한다. PSA 는 노심손상빈도, 위험도감소가치, 위험도증가가치를 통해 평가하는 정량적인 기법이다. 델파이 중요도평가는 전문가위원회를 통해 Table 6. 과 같이 사고대응 4개, 정상운전 6개 항목으로 나눠 기능 간의 상대적인 중요도를 고려하여 평가하는 기법이다. 항목별 가중치를 적용하고, 경계치에 근접하거나 전문가 평가 간 편차가 큰 경우 재평가를 수행할 수 있다. 전문가위원회에서는 PSA와 델파이 중요도평가 모두를 종합하여 검토하고 최종 안전중요도 결과를 도출한다.

Table 6. Delphi Assessment

Cat	Function Description
Incident Response	Shut down the reactor and maintain it in a safe shutdown state
	Maintain the integrity of the pressure boundary of the reactor coolant system
	Removal of atmospheric heat and radioactive substances from the containment vessel
	Function to remove heat from the reactor
	Shut down the reactor and maintain it in a safe shutdown state
Incident Response	Maintain the integrity of the pressure boundary of the reactor coolant system
	Removal of atmospheric heat and radioactive substances from the containment vessel
	Function to remove heat from the reactor
Normal Operation	Primary side heat removal function.
	Power conversion function
	Pressure control function of primary side, secondary side, or containment vessel
	Supply of cooling water, equipment, or containment cooling
	Supply of cooling water, equipment, or containment cooling
	Supply of drive and control power

안전중요도의 고저에 따라 신뢰도 성능기준(RPC), 이용도 성능기준(APC), 상태감시 성능기준(CMC), 호기수준 성능기준(ULPC)을 수립한다. 각 성능기준은 RPC는 운전 중 고장횟수, APC는 시험 및 정비로 인한 이용불능시간, CMC는 RPC, APC 수립이 어려운 경우, ULPC는 비계획 원자로정지, 출력감발, 안전계통 작동횟수를 기반으로 수립된다.

각 성능기준의 관계는 Fig 9.와 같이 안전중요도

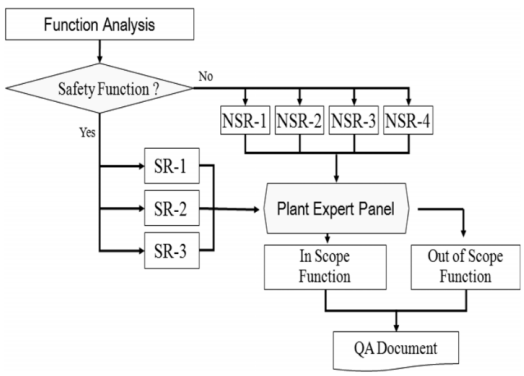


Fig. 7. Scope determination flow[12]

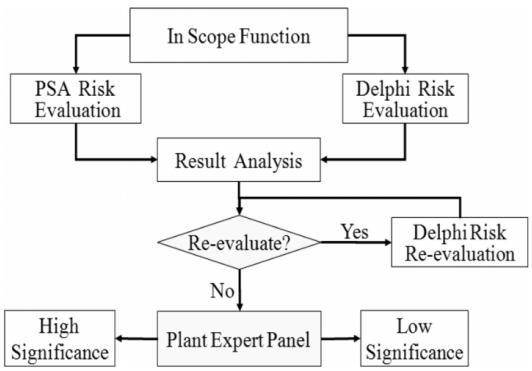


Fig. 8. Risk significance determination[12]

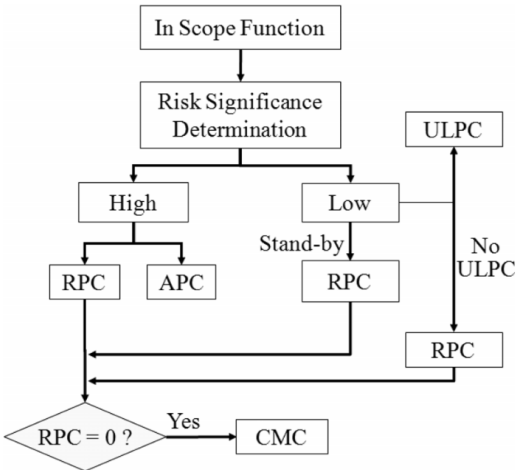


Fig. 9. Performance criteria establishment[12]

가 High일 경우 RPC 및 APC, Low일 경우 대기 상태(Stand-by) 를 유지하면 RPC 상시운전이라면 ULPC를 수립한다. ULPC가 적용되지 않는 기능은 RPC를 수립하고 RPC가 "0"인 경우에는 CMC를 수립한다.

성능기준을 반영한 A1유형 자산의 정비규정 개발은 Table 7. 과 같이 요약될 수 있다. 결과적으로 A1유형의 자산은 분석내용에 해당하는 기능을 수행하는 SSC 이기 때문에 관리대상으로 최종분류되어 정비규정을 이행한다.

Table 7. Result of performance criteria establishment

Scope	Description			Target SSC
SR-3	capability to prevent or mitigate the conse quen ces of accidents			pump,valve, sensor
PSA	Delphi Assessment			Performance
	ER	NO	Final	
H	425	68	H	RPC/APC

3.1.3 A1 유형 자산에 대한 정비규정 이행

감시 수행 중 기능고장이 발생하면 고장유형을 분류하여 정비규정에 정의된 기능을 수행할 수 있는 지 여부를 판단하고 신뢰도에 반영될 수 있도록 집중조치 계획을 수립한다. 여기에는 근본원인분석 및 재발을 예방할 수 있는 시정조치계획이 포함된다. 또한

Table 8. the Type of Function Failures[13]

Definitions	Descriptions
MRFF (Maintenance Rule Function Failure)	Failure to perform the functions defined in the maintenance rule
MPFF (Maintenance Prevnetable Function Failure)	Unintended event or condition resulting from the failure to perform appropriate maintenance actions, rendering it unable to perform its function
RMPFF (Repetitive Maintenance Prevnetable Function Failure)	Failure occurring on the same equipment due to the same root cause that occurred previously

매 2년마다 주기적으로 정비규정을 평가함으로써 감시하는 성능기준의 적합성을 입증하고 있다.

위에서 분석한 바와 같이 정비규정은 자산의 설계된 기능에 초점을 맞춰 활용한다. 개발 및 이행의 일관성을 확보하기 위해 자산의 특성보다 기능을 기반으로 기준이 구현되어 있고, 계통의 고유특성을 반영하여 적절한 조치를 통해 의도한 기능을 원활하게 수행할 수 있도록 체계를 수립할 수 있다. 아울러 Fig 10. 과 같이 정비규정의 이행을 통해 안전 관련(Safety-related) 기능의 의도치 않은 고장에 대해서도 신뢰도, 상태, 이용도 측면에서 감시와 예방이 수행된다는 점도 확인이 가능하다.

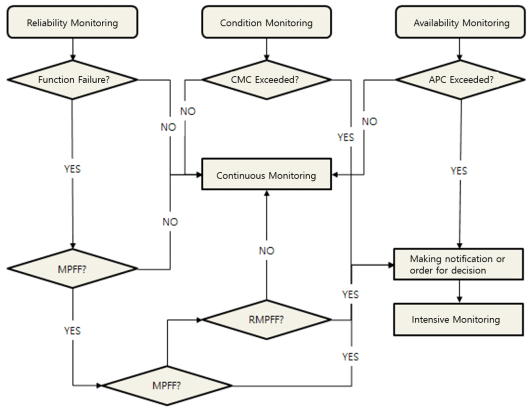


Fig. 10. Performance Monitoring

3.2 EPRI TAM을 이용한 자산분석

3.2.1 EPRI TAM 개요

미국 EPRI(Electric Power Research Institute)에서 개발한 사이버보안 기술평가 방법론(TAM, Technical Assessment Methodology)은 발전소의 사이버보안 체계를 평가하고 적용하기 위해 마련된 방법론이다. 자산의 기술적 구성을 검토하고 실질적인 공격표면에 효율적인 보안통제를 적용하고자, 위험 기반의 차등적인 접근방식을 사용한다.

EPRI TAM 은 개별 자산에 기준을 적용하여 자산 자체의 보안수준을 측정하고 공격표면에 효과적인 사이버 보안조치들을 식별한다. 이러한 자산별 차등적인 접근방식은 계통 기능에 따른 식별결과를 보완 또는 개선할 수 있는 분석 방법이 될 수 있다.

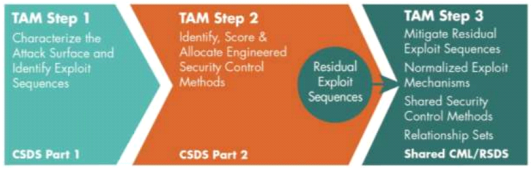


Fig. 11. EPRI TAM

3.2.2 TAM 1단계 : 공격표면 특성화 및 취약성 공격 시퀀스 식별

1단계에서는 평가범위의 제한(Bound the Assessment Scope), 공격표면의 특성화(Characterize the Attack Surface), 취약성 공격 시퀀스 식별(Identify Exploit Sequences) 순으로 수행된다.

평가범위 제한은 자산의 구성과 분해, 기술 정보 가용성 수준(TIA, Technical Information Availability Level) 산정, 설치된 구성 및 데이터 흐름, 중요데이터 확인의 순으로 수행된다.

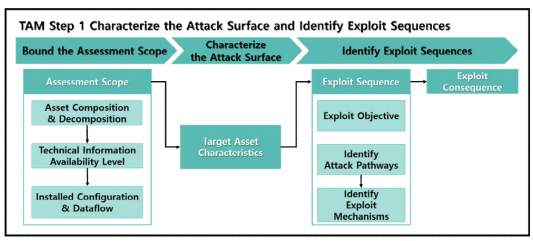


Fig. 12. TAM STEP 1[16]

자산의 구성과 분해는 Table 9. 와 같이 평가범위 결정을 위한 자산 단위를 정하기 위해 물리적 구성 및 형태를 특정한다. 회로 또는 칩 단위로 분해하는 과정은 데이터 흐름을 파악하고 각 소자별 저장되는 데이터를 이해하는 데 사용된다.

기술정보 가용성 수준 산정을 통해 적용되고 있는 객관적인 기준에 대한 질적등급을 이해할 수 있다. 따라서 유효성있는 분석은 최소 TIA 1 수준을 만족해야 한다. ① 수준1 은 현장 또는 워크벤치에서 공격표면 분석을 수행할 수 있으며, 법적 또는 운영상

Table 9. Asset Compositon&Decomposition

Category	Description
General	1. Overview ▪ Measures pressure (PT), level (LT), and flow rate (FT) during the process at the nuclear power plant ▪ Transmits signals of 4-20mA to the upper system ▪ Manages configuration using the HART Protocol ▪ The set pressure range can be verified through communication with the HART communicator ▪ Changes to the set pressure range can be made through button functionality and reconfiguration using the HART Communicator 2. Exterior 
Document ation	▪ M3700N-K01E, APT3700N Intelligent Transmitter User Manual for Nuclear Power Plants
Install	▪ Installed on the wall inside the power plant using a Wall Type bracket
Decompos iton Level	▪ Sensor section composed of sensors, A/D converter, and EEPROM for storing input data ▪ MCU section composed of a microprocessor for data processing and D/A converter

Table 10. TIA Level

Description
〔TIA Level 2〕 ▪ For safety system assets, direct inspection of assets outside of preventive main tenance periods is not feasible. However, indirect inspection through manufacturer manuals, power plant procedures, or on-site checks is possible

제약때문에 자산을 내부적으로 검사하거나 직·간접적으로 조사할 수 없음을 의미한다. ② 수준2 는 현장 또는 워크벤치에서 공격표면 분석을 수행할 수 있으며, 법적 또는 운영상 제약 내에서 자산을 내부적으로 검사하거나 직·간접적으로 조사가능함을 의미한다. ③ 수준3 은 연구소에서 공격표면 분석을 수행할 수 있으며, 자산을 내부적(OEM, 설계정보)으로 검사하거나 직·간접적으로 조사가능함을 의미한다.

설치구성 및 데이터 흐름은 예상되는 공격벡터와 취약점을 결정할 수 있는 중요한 내용이다. 운전 또는 정비 중에 구성되는 기능 및 네트워크 연결에 대해 확인하고, 사용되는 모든 접근에 대해 작성한다.

중요데이터에 대한 예방 및 공격완화는 사이버보안의 궁극적인 목표다. 자산 사이에 이동하는 데이터나 내부에 저장된 데이터를 파악하여 보호해야 할 데

Table 11. Installed configuration and data flow

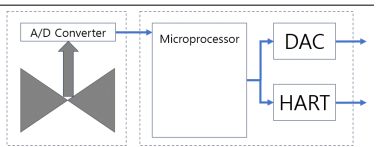
Category	Description
Installed configuration	〔Normal Operation〕 Measuring pressure (PT), level (LT), and flow rate (FT) during the process and transmitting 4-20mA signals to the upper system 〔Maintenacne & Temporary OP〕 Through the test terminals, you can verify the transmitter output. Calibration can be performed via HART device, and devices supporting the APT 3700N allow operation without the need for separate software support
Data Flow	

Table 12. Identify Critical Data

Category	Description
Critical Data	〔Operational process data : Y〕 ▪ Process variables are stored in EEPROM through the sensor ▪ Settings and logic are stored in the microprocessor. 〔OEM program/configuration data : Y〕 ▪ Firmware is embedded in the microprocessor 〔User program/configuration ata : N〕 〔Security Operational data : N〕 〔Security OEM program/configuration data : N〕 〔Security User program/configuration data : N〕

이터를 확인할 수 있다. ① 운영 공정데이터는 온도, 압력, 유량 제어신호, 지시, 경보 등의 가동 중 발생하는 데이터를 의미한다. ② 프로그램/설정 데이 터는 제조사나 사용자에 의해 설치된 로직, 매크로, 스크립트, 설정치, 펌웨어 등을 의미한다. ③ 보안 운영데이터는 사용자명, 패스워드, 보안로그 등을 의미한다. ④ 보안 프로그램/설정 데이터는 보안소프트웨어, 접근권한, 계정 관리, 접근통제 목록, 방화벽 규칙 등의 기기보안 데이터를 의미한다.

공격표면의 특성화는 공격표면(Attack Surface)에 영향을 미칠 수 있는 자산의 특성, 기능 분석을 통해 기술적 취약점과 다 수의 공격벡터를 결정하는데 필요한 단계이다. 공격표면은 기술적 취약점, 공격벡터의 적용, 공격경로 메커니즘을 나타낼 수 있고, 이러한 공격표면의 특성화는 기기 특성, 중요데이터와 그 구조 및 흐름, 접근점(Access Point)을 이해함으로써 달성할 수 있다. TAM에서 공격표면의 특성화는 대상 자산의 특성(Target Asset Characteristics) 단계를 통해 수행된다.

취약성공격 시퀀스(Exploit Sequence)는 공격자가 목적(Exploit Objective)를 달성하기 위한 공격경로(Attack Pathway)와 취약성공격 방법(Exploit Mechanism)의 조합을 의미한다.

여기서 취약성공격 방법은 공격자가 공격경로를 통해 목적을 달성할 수 있도록 하는 가능한 수단으로 정의할 수 있다. 이러한 취약성공격 시퀀스는 악의적인 사건(Adverse Incident)에 대하여 시스템적이고 더 정확한 공격표면 분석이 이루어질 수 있도록 연결될 수 있다.

기술적 취약점을 공격하기 위한 수단, 즉 공격벡

Table 13. Attack Surface Characterization

Category	Description
Firmware Description	Firmware R23 ▪ If the version is low, the transmitter used may not be compatible with the HART communicator. In such cases, a dedicated software (Device Descriptor) can be obtained from the vendor or manufacturer and loaded onto the HART communicator for use. ▪ To upgrade the firmware, the EPROM on the MCU board must be physically replaced.
Installed Configuration & Maintenance Method	▪ Using the HART communicator via the HART protocol. Only functions such as setting parameters, calibration, and testing that are configured in the communicator menu are allowed
Communication Ports and Terminals	▪ Analog +/- terminal ▪ Test + terminal
Media and Portable Devices	▪ HART Communicator (HART 275, 375, 475)
Data Commnication Protocol	▪ HART Revision5, PV with status, Device Status, Broad casting Messaging, Device Configuration, 4-20mA Analog Loop Check
Site Characteristics	▪ Located at points for detecting power plant pressure/flow/ level ▪ Configured with control systems and analog loops ▪ No digital connections other than HART communicator for maintenance purposes
Site Characteristics	▪ Located at points for detecting power plant pressure/flow/ level ▪ Configured with control systems and analog loops ▪ No digital connections other than HART communicator for maintenance purposes
Access control and Authentication	▪ Transmitter Security DIP Switch

터가 존재한다는 것은 사이버공격이 이동하는 공격경로가 있음을 의미한다. 특정한 보안통제 방법을 결정하기 위해서는 이러한 공격경로가 정확하게 식별되어야 한다. TAM에서는 NEI 10-09 "Addressing Cyber Security Controls for Nuclear Power Plant"를 참고하여 취약점을 전파하는 경로에는 다음의 5가지 공격벡터가 있음을 언급한다.

1) Direct Network Connectivity
2) Wireless Network Capability
3) Portable Media and Equipment
4) Supply Chain
5) Direct Physical Access

Table 14. 는 APT3700N 에 대하여 공격표면 정보를 기반으로 공격벡터와 경로를 기술한 표이다.

공격자는 목적을 달성하기 위해 하나의 가능한 공격경로와 자산능력을 파악하여 적용하려 한다. 공격경로는 공격표면과 연관하여 분석하였다. 특정한 자산능력은 공격자가 취약성공격 목적을 달성하는데 허용한다. 각각의 경로, 방법, 목적의 조합은 취약성공격 시퀀스가 될 수 있다.

TAM 에서는 기본적인 데이터 정보의 원칙에 따라서 공격목표를 도출한다. ① 저장데이터와 전송데이터, ② 실행가능한 코드와 데이터값, ③ 자산기능과 보안통제에 관한 실행코드, 그리고 멀웨어 등과 같은 허가받지 않은 코드, ④ 공급업체에서 통제하거나 사용자 정의에 의해 제작된 소스코드, ⑤ 자산기능과 보안통제에 대한 데이터값, ⑥ 데이터의 변조 또는 탈취에 따른 사이버공격, ⑦ 사이버공격으로써 자산에 직접적인 영향을 줄 수 있는 행동. 기준을 적용하면 4개의 직접적인 영향과 전송/저장되는 6가지 중요데이터의 탈취와 변조에 대해 총 28개의 항목으로 구분할 수 있다.

Table 14. Attack Path

ID	Attack Vector	Physical Interface	Protocols	Description
A01	Direct Physical Access	Analog Terminals/ Cables	None	Power, Analog Signal
A02	Portable Media& Equipment	Analog Terminals/ Cables	HART	HART Communicator
A03	Supply Chain	None	None	Supply chain

Table 15. APT3700N Exploit Sequence

Category	Exploit Objective			Attack Path way	Exploit Mechanism
Exploit Objective associated with Direct Action Against the Asset	Immediate execution/failure of assets			A01	X01. Failure due to power disconnection
	Failure due to latency factors of assets			-	No delay factor setting function
	Denial of Service (DOS)			-	Bulk HART data cannot affect transmitter operation
	Malware			-	Firmware is installed by the manufacturer
Exploit Objective associated with the Critical Data types	Operational process data	In Transit	Theft	A02	X01. Variables can be checked via HART communicator.
			Alternation	-	Real-time process data cannot be tampered with.
		At Rest	Theft	A02	X01. Variables can be checked via HART communicator.
				A03	X01. Design drawings and manuals managed by subcontractors leaked through the supply chain.
			Alternation	-	Stored process data cannot be tampered with.
	OEM program/ configuration data	In Transit	Theft	-	Firmware cannot be changed or reinstalled during operation.
			Alternation	-	Firmware cannot be changed or reinstalled during operation.
		At Rest	Theft	-	No firmware copying function installed.
			Alternation	A03	X02. Transmitter replacement and delivery from subcontractors are tamper-proof.
	User program/ configuration data	In Transit	Theft	A02	X01. Settings (Range, Unit, Zero, Span) can be checked via HART communicator
			Alternation	-	Settings cannot be changed during transmitter operation.
		At Rest	Theft	A02	X01. Settings (Range, Unit, Zero, Span) can be checked via HART communicator
			Alternation	A02	X01. Settings (Range, Unit, Zero, Span) can be checked via HART communicator
	Security operational data	No Security Data			
	OEM Security program/ configuration data				
	User Security program/ configuration data				

취약성공격 목표(Exploit Objective)와 취약성 공격 경로(Attack Pathway)를 조합하고, 그에 대한 취약성공격 방법(Exploit Mechanism)을 기술함으로써 최종적으로 취약성공격 시퀀스(Exploit Sequence)를 도출해 낼 수 있다. Table 15. 는 APT3700N 전송기의 취약성공격 시퀀스를 도식화한 내용이다.

3.2.3 TAM 2단계 : 기술적 보안통제 방법 식별, 점수화 및 할당

2단계에서는 1단계에서 분석한 자산에 적용가능한 보안조치를 식별, 점수화, 할당한다. 최선의 보안조치 이행을 통해 취약성 공격시퀀스를 완화시켜 목표수준의 통합보안 효율성을 달성하는 데 목적으로 두고 있다. 특정 사이버보안통제 요건을 적용하거나, 좀 더 효율적으로는 TAM 1단계 결과에 따른 취약성 공격 시퀀스를 완화하기 위한 보안조치를 탐색/평가하는 방법을 통해 보안조치를 식별할 수 있다. 보안조치는 다음의 3개 보안기능인 ① 보호(Protect), ② 탐지(Detect), ③ 대응 및 복구 (Respond & Recover) 중 하나 이상을 만족한다. 이러한 보안조치는 보안효율성(Security Effectiveness)점수와 효능(Efficacy)점수로 산출된다.

보안효율성의 점수는 이행 효율성(Implementation Effectiveness)과 취약성 공격 난이도(Exploit Difficulty)의 총합으로 산출된다. 이행효율성은 이행유형과 보안기능으로 나눠 구분하는데 이행유형은 관리적(Administrative), 운영적(Operational), 기술적(Technical)으로, 보안기능은 보호, 탐지, 대응 및 복구로 나눠 구분된다. 취약성공격 난이도는 구성 (Configuration), 정보(Information), 인증(Authentication), 지속성(Persistence)로 나눠 구분된다. Table 16. 은 각 평가요소 별 할당된 측정값을 나타낸다.

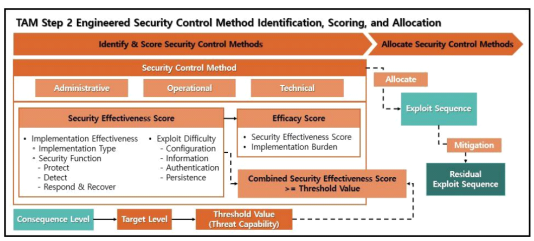


Fig. 13. TAM STEP 2[16]

Table 16. Security Effectiveness Criteria

Criteria						
Implementaion Effectiveness	Type		Admin (1.0)	Oper (1.05)	Technic (1.25)	
	Security Function	Protect	None (0.0)	Low (0.927)	Medium (1.2)	High (1.7)
		Detect	None (0.0)	Low (0.927)	Medium (1.2)	High (1.7)
		Respond and Recover	None (0.0)	Low (0.927)	Medium (1.2)	High (1.7)
Exploit Difficulty	Configuration			Low (0.34)	Medium (0.67)	High (1.0)
	Information			Low (0.34)	Medium (0.5)	High (0.66)
	Authentication			Low (0.0)	Medium (0.5)	High (0.66)
	Persistence			Low (0.34)	Medium (0.5)	High (0.66)

보안효율성 점수는 평가요소 별 측정값을 기반으로 다음과 같은 기대값으로 계산된다. 수식에서 보듯이 각각의 평가요소는 보안효율성의 총량을 나타내는데 독립적으로 적용됨을 알 수 있다.

$$E = \log_2(\alpha) + \log_2(D) + \log_2(I)$$

E : 보안효율성
α : 환산계수
D : 취약성공격 난이도 값
I : 이행효율성(이행유형*보안기능)

높은 점수의 보안효율성은 공격자가 보안통제를 뚫기 위해 기기, 계통, 통제방법, 세밀한 취약성 분석 등 더 높은 수준의 능력이 필요함을 의미한다.

효능점수는 보안효율성(Security Effectiveness)와 이행부담(Implementation Burden)의 조합으로 산출된다. 초기(Initial) 이행부담과 지속적인 운영/유지 이행 부담을 가중치에 따라 합산한다. 가중치를 적용한 이행부담과 보안효율성을 점수에 따라 구간별로 분류하고 조합에 따라 효능점수를 측정할 수 있다. 아울러 자산 또는 시스템 운영과 충돌할 수 있기에 충돌(Conflict) 영역을 두어 보안조치 이행 금지를 권고할 수 있다. 효능점수가 높을수록 높은 효율성과 적은 이행부담으로 보안조치의 효과가 높다는 것을 의미한다.

이러한 보안조치의 효능점수를 산정하는 목적은 취약성공격 시퀀스를 완화시킬 수 있는 최적의 보안

조치를 할당하기 위함이다. 이를 위해 잠재적인 공격 결과에 따라 목표 수준을 선정하고, 시퀀스 별 보안기능에 따라 보안조치를 적용함으로써 종합 보안효율성 점수가 목표수준을 충족할 수 있도록 한다. 단일 보안조치를 적용 결과 점수가 충분하지 않을 경우, 복수의 보안조치를 적용함으로써 보완한다.

보안조치 할당결과, 목표수준을 만족하지 못하면 TAM 3단계에서 추가적인 조치를 수행한다.

Table 17. Security Efficacy Criteria

Efficacy Score		Implementation Burden		
		High (2.3〈B≦3.0)	Medium (1.3〈B≦2.3)	Low (0.0〈B≦1.3)
Security Effectiveness	None	None		
	Low (0.1〈E≦1.0)	1	2	3
	Medium (1.0〈E≦2.0)	2	3	4
	High (2.0〈E≦3.0)	3	4	5

Table 18. Combined Secuirty Efficacy Criteria

Potential impact level	Target	Combine Efficacy score Needed
5 (High impact)	A	A ≧ 3.30
4	B	2.60 ≦ B 〈 3.30
3	C	2.00 ≦ C 〈 2.60
2	D	1.30 ≦ D 〈 2.00
1 (Low impact)	E	0.70 ≦ E 〈 1.30

3.2.4 TAM 3단계 : 공유 보안통제 방법 식별, 점수화 및 할당

3단계에서는 2단계에서 목표 수준을 만족하지 못한 잔여 취약성공격 시퀀스를 완화를 목적으로 한다. 자산 간의 관계집합을 구성하고, 관계집합 간의 표준화된 취약성공격 메커니즘에 대해 공유보안조치(를 적용하여 잔여 취약성 공격 시퀀스를 완화시킨다.

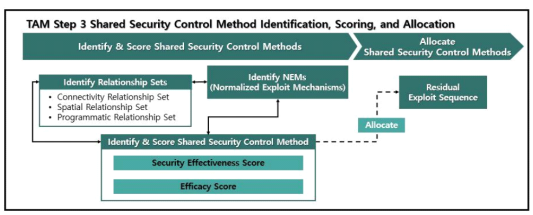


Fig. 14. TAM STEP 3[16]

Table 19. Relationship set and Shared control method

Relationship Set	Description	Example of Share control method
Connectivity	▪ Logical connections ▪ Network Protocols ▪ Attack paths provided	▪ Network rules ▪ Firewall rules
Spartial	▪ Same physical location ▪ Similar lock mechanisms	▪ Notification cabinets and locks ▪ Card readers ▪ Physical boundary controls
Programming	▪ Assets managed by configuration management or policies and procedures	▪ Program policies such as configuration management or portable media

관계집합은 취약성에 대한 공통 방어체계의 보장, 공유보안조치의 효율적인 적용, 표준화된 취약성공격 메커니즘의 식별을 할 수 있다는 장점을 갖고 있다. 관계집합은 ① 연결성(Connectivity), ② 공간적(Spartial), ③ 프로그래밍(Programmatic)의 3가지로 구분한다.

표준화된 취약성공격 메커니즘은 1단계에서의 취약성공격 메커니즘을 포괄하는 개념이다. 관계 집합과 메커니즘을 바탕으로 관계집합에 적용할 수 있는 공유 보안조치를 식별 및 점수화 할 수 있다. 이후에는 보안효율성 점수의 합이 잔여 취약성공격 시퀀스의 목표수준 이상이 될 때까지 공유 보안조치를 할당한다.

3.3 국내 원전자산의 상세분석 방안

정비규정에 의한 고유기능 감시는 발전소 운영에 필수적인 안전기능과 비안전기능으로 구분하여 적절한 성능감시를 수행하고 기능고장 유형에 따라 정비가 이루어질 수 있도록 하고 있다. 국내 보안조치 결과와 정비규정 적용의 비교가 가능했던 점은 안전관련 (Safety-related) 개념을 공유하고 있기 때문인데, 사이버침해에 의한 사보타주 (Sabotage), 기기의 고장과 같은 원인의 차이일 뿐 설계된 기능을 적절하게 수행해야 하는 의도는 동일했다. 따라서 현장

측면에서 A1유형 자산과 같이 기술적 검토가 불필요한 자산은 운영적/관리적 보안조치를 정비규정에 의한 성능감시 이행으로 갈음할 수 있는 경우가 많다.

EPRI TAM은 분석결과 총 8개의 시퀀스를 도출할 수 있었다.

〔전원을 통한 공격경로〕
① 물리적 차단에 따른 전송기 장애

〔HART 통신기를 통한 공격경로〕
② 전송 중인 운영 공정데이터의 탈취
③ 저장 중인 운영 공정데이터의 탈취
④ 전송 중인 사용자 프로그램/설정데이터의 탈취
⑤ 저장 중인 사용자 프로그램/설정데이터의 탈취
⑥ 저장 중인 사용자 프로그램/설정데이터의 변조

〔공급망을 통한 공격경로〕
⑦ 저장 중인 운영공정데이터(도면, 매뉴얼) 탈취
⑧ 저장 중인 OEM 프로그램/설정데이터 변조

①,⑦,⑧ 의 시퀀스는 기존 원전 운영체계의 품질검증절차 및 인수테스트에서 관리되고 있기 때문에 여타의 조치는 불필요한 것으로 판단할 수 있다. 또한 ②~⑥ 의 시퀀스는 HART 통신기로 인한 공격경로로 인하여 분류되었으나, 원전 내부의 구역설정과 접근권한 부여를 고려했을 때 추가적인 보안조치를 필요로 하지 않는다.

A1유형 자산의 선정결과와 TAM의 취약성공격 시퀀스 선정결과를 토대로 보안조치의 부담을 낮추기 위해서는 '사이버침해로 인한 사보타주 발생' 여부를 확인해 볼 필요가 있다. 중요도평가 결과에 따라서 A1유형의 자산은 직접적인 안전기능을 수행하는 직접 필수디지털자산의 하나로 분류된다. 또한 TAM의 취약성공격 시퀀스는 기기 자체의 취약성 분석을 통해 보호조치 대상을 결정한다. 이렇게 결정된 자산은 기기장애 또는 데이터 탈취/변조 등이 사보타주에 직간접적으로 영향을 미쳐야 한다. 예를 들어 APT3700N 출력신호가 안전관련 기능(원자로 정지, 방사능 누출 등)과 연관되어 적합한 대응 결정을 하는데 필요치 않다면, 사보타주와의 연관성을 재분석해야 한다. 원자로정지 또는 방사능 누출이 수반되는 사고의 대응 과정에서 자산의 기능이 명확하게 사용하는 것을 판단하는 것이 중요하다. 이에 대해 판단근거로 PSA 의 사건수목 또는 사고에 대한 운전

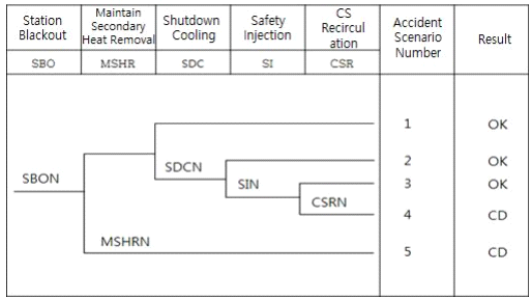


Fig. 15. Incident Monitoring in PSA

원의 조치단계를 기술한 비상운전절차서를 적합한 자료로 사용할 수 있다. 이들 자료에는 조치 간 요구하는 기능과 변수 및 자산이 상세히 명시되어 있기 때문에 선정결과에 대한 명확한 근거 확립에 도움이 될 것이다.

IV. 결 론

본 논문은 국내 필수디지털자산 식별 기준에 따른 A1유형 자산 분석방안의 완성도 제고를 위해 기존 자산식별 및 보안조치 현황을 설명하고, 정비규정과 EPRI TAM관점의 자산분석과 적용을 통해 그 결과를 보완한다. 필수디지털자산 식별, 중요도 평가, 보안조치 결정 순서로 A1유형 자산의 분류와 수행해야 할 보안조치에 대해 살펴보았으며, 결과적으로 운영·관리적 보안조치에 대하여 55건의 이행 결과물이 도출됨을 확인할 수 있었다. 정비규정은 사이버보안 관련 기준과 같이 "안전관련(Safety-related)" 개념을 공유하고 있기 때문에 계통의 기능분석을 통해 대상을 선정하고 조치한다는 부분에서 유사한 맥락으로 분석을 수행할 수 있었다. 분석결과, 정비효율성 감시를 위해 수립된 정비규정 프로그램은 설계된 기능의 의도치 않은 고장에 대해 감시와 예방이 수행된다는 점을 확인할 수 있었다. TAM을 통한 분석결과, 유지보수를 위한 HART 통신기로의 취약성공격 시퀀스로 식별되었다. 다만 이러한 공격경로가 A1유형 자산의 안전관련 기능 수행에 영향을 줄 수 있는지는 원자력시설의 기능불능을 초래하는 '사보타주'와의 연관성을 분석할 필요가 있다. 이는 PSA 의 사건수목 또는 비상운전절차서를 근거로 하여 자산이 요구하는 기능, 지시하는 변수 등이 포함되어 있다면 추가적인 분석을 수행하는 데 도움이 될 수 있다. 다만 원전의 사건수목과 비상운전과 같은 정보들은 원전의 특수성

에 기인하고 있고, 내외적으로 접근성이 부족하다. 따라서 본 논문을 활용하여 원전안전과 제어보안 측면을 모두 충족할 수 있는 가이드라인을 제시한다면 현장의 보안조치 부담을 경감할 수 있는 방법이 될 것이다.

References

[1] NRC, "Protection of Digital Computer and Communication System and Networks", 10CFR73.54, March 2021, NRC Regulations Title 10, Code of Federal Regulations, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html, May 2024.

[2] NRC, "CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES", Regulatory Guide 5.71, Revision1, Feb 2023, Document Collections, https://www.nrc.gov/docs/ML0903/ML090340159.pdf, May 2024.

[3] NEI, "Identifying System and Assets Subject to the Cyber Security Rule", NEI 10-04, Revision2, Jul 2012, Document Collections, https://www.nrc.gov/docs/ML1218/ML12180A081.pdf, May 2024.

[4] NEI, "Cyber Security Control Assessments", NEI 13-10, Revision6, Aug 2017, Document Collections, https://www.nrc.gov/docs/ML1723/ML17234A615.pdf, May 2024.

[5] EPRI, "Cyber Security Technical Assessment Methodology", 3002016907, Revision1, Jul. 2019, Technical Assessment Methodology (TAM) Revision 1: Computer Based Technology Transfer Module (CBTT), https://www.epri.com/research/products/000000003002016907, May 2024.

[6] DUON System, "APT3700N Operation Manual for Nuclear Power Plant Differential Pressure Transmitter", M3700N-K01C.

[7] DUON System, "APT3700N Operation Manual for Nuclear Power Plant Pressure Transmitter", M3700N-K01E, Revision1, Oct 2010.

[8] Kim, C., & Kim, J., "Development Trends of HART Communication", Doon System Co., Ltd. Subsidiary Research Institute, Instrumentation Technology, pp. 106-112 , Jan. 2016.

[9] NRC, "Requirements for monitoring the effectiveness of maintenance at nuclear power plants", 10CFR50.65, Mar 2021, NRC Regulations Title 10, Code of Federal Regulations, https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0065.html, May 2024.

[10] NRC, "MONITORING THE EFFECTIVENESS OF MAINTENANACE AT NUCLEAR POWER PLANTS", Regulatory Guide 1.160, Revision4, Aug 2018, Document Collections, https://www.nrc.gov/docs/ML1822/ML18220B281.pdf, May 2024.

[11] Kim, G., Hwang, M., & Jang, S., "A Study of Adopting Maintenance Rule in the Korean NPP", Journal of the Korean Society of Safety, 16(2), pp.110-116, May. 2001.

[12] Yeom, D., Hyun, J., & Song, T., "Development of Maintenance Effectiveness Monitoring Program for APR1400 Safety Related Systems", Energy Engineering, 23(2), Jun. 2014.

[13] Ryu, J., "A Study on the Engineering Programs used for Improving Equipment Reliability in NPPs", Master's Thesis, Busan National University, Feb. 2018.

[14] Kwon, K., "Research for Digital Asset Analysis Methodology for Cyber Security of Nuclear Power Plant", Master's Thesis, Ajou University, Aug 2013

[15] Kim, I., Byun, Y., & Kwon, K., "Analysis of the Application Method of Cyber Security Control to Develop Regulatory Requirement for Digital Assets in NPP", Korea

Institute of Nuclear Nonproliferation and Control, Journal of the Korea Institute of Information Security & Cryptology, 29(5), Oct. 2019.
〔16〕 Jung, D., "A Study on the Use of TAM for the Assessment and Application of Cyber Security Controls for Critical Infrastructure", Master's Thesis, Gachon University, Feb 2022.
〔17〕 Park, J., Park, J., & Kim, Y., "Cyber Security Consideration on Digital Instrumentation and Control System Development Process in Nuclear Power Plants", Korea Computer Congress 2012, pp.354-356, Jun. 2012.
〔18〕 Kim, S., "A Study on the Effectiveness of Grouping of the Critical Digital Assets at the Nuclear Facilities", 2017 Korea Institute of Communication Sciences Winter Conference, pp. 656-657, Jan. 2017.
〔19〕 Cha, G., Noh, J., Kim, G., & Chae, M. "A Study on Effective Implementation of Security Controls to Critical Digital Assets in NPPs", CICS `17 Information and Control Conference, pp.271-272, Oct. 2017.
〔20〕 Choi, Y., & Lee, S. "A Study on the Implementation of Technical Security Control for Critical Digital Asset of Nuclear Facilities", Journal of the Korea Institute of Information Security & Cryptology, 29(4), Aug. 2019.
〔21〕 Lee, S., "A Study on Alternative Security Measures for Control Systems in Nuclear Power Plants", 2021 Korea Energy Society Spring Conference, pp.150, Apr. 2021.

〈저자소개〉

이 신 우 (Shin-woo Lee) 정회원
2022년 9월~현재: 고려대학교 정보보호대학원 사이버보안학과 석사과정
2014년 4월~현재: 한국수력원자력 재직 중
2013년 8월: 중앙대학교 전자전기공학부 졸업
〈관심분야〉 시스템 및 네트워크 보안

이 중 희 (Jung-hee Lee) 종신회원
2021년~현재: 고려대학교 정보보호대학원 부교수
2019년 3월~2021년: 고려대학교 정보보호대학원 조교수
2014년 8월~2019년 1월: University of Texas at San Antonio 조교수
2003년 3월~2008년 8월: 삼성전자 연구원
〈관심분야〉 시스템 및 네트워크 보안