Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.2, Apr. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.2.229

가동 중 원자력시설의 SBOM(Software Bill Of Materials)구현방안 연구*

김 도 연,[1†] 윤 성 수,[1] 엄 익 채[2‡]
[1,2]전남대학교 (대학원생, 교수)

Study on the Implementation of SBOM(Software Bill Of Materials) in Operational Nuclear Facilities*

Do-yeon Kim,[1†] Seong-su Yoon,[1] Ieck-chae Euom[2‡]
[1,2]Chonnam National University (Graduate student, Professor)

요 약

최근 APR1400 노형과 같이 원자력발전소의 디지털 기술 적용에 따라 "이블 PLC"같은 원자력시설 대상의 공급망 공격이 증가하는 추세이다. 원자력 공급망 보안에 있어 산업 특성상 수많은 공급업체가 존재하기에 이를 체계적으로 관리할 수 있는 자원 관리 시스템이 필요하다. 하지만, 제어시스템 특성상 소프트웨어 자산의 긴 생명 주기로 인해 속성 정보가 일관되지 않게 관리된다는 문제점이 존재한다. 또한, 운영 환경의 가용성 문제로 인해 형상 관리 자동화 도입이 미흡한 상태에서 입력 오류와 같은 한계점이 존재한다. 본 연구에서는 SBOM(Software Bill Of Materials)을 적용한 체계적인 자산 관리 방안 및 자연어처리 기법을 적용한 입력 오류에 관한 개선 방안을 제안한다.

ABSTRACT

Recently, supply chain attacks against nuclear facilities such as "Evil PLC" are increasing due to the application of digital technology in nuclear power plants such as the APR1400 reactor. Nuclear supply chain security requires a asset management system that can systematically manage a large number of providers due to the nature of the industry. However, due to the nature of the control system, there is a problem of inconsistent management of attribute information due to the long lifecycle of software assets. In addition, due to the availability of the operational technology, the introduction of automated configuration management is insufficient, and limitations such as input errors exist. This study proposes a systematic asset management system using SBOM(Software Bill Of Materials) and an improvement for input errors using natural language processing techniques.

Keywords: OT, Nuclear Power Plant, Supply Chain, SBOM, Asset Management

Received(01. 16. 2024), Modified(03. 28. 2024), Accepted(04. 02. 2024)

* 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(IITP-2022-0-01203)

* 본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No. 2106061)

* 본 논문은 2023년도 한국정보보호학회 호남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임

† 주저자, ehdus928@jnu.ac.kr

‡ 교신저자, iceuom@jnu.ac.kr(Corresponding author)

I. 서 론

최근 원자력발전소의 디지털 기술 적용에 따라 APR1400 노형과 같은 디지털화된 시스템 도입이 증가하고 있다. 하나의 디지털 기기는 여러 단계의 공급망을 통해 외부에서 제작된 후 공급된 기기들과 산업에서 활용되는 소프트웨어의 조합을 통해 최종적인 자산이 만들어진다[1]. 이러한 단계를 수행하는 과정에 있어 결함이 생겨 사이버 보안 위협을 포함한 최종 자산이 만들어질 가능성이 존재한다.

위와 같이 생성된 소프트웨어 및 펌웨어 등의 자산들은 더욱 정교해진 공급망 사이버 공격에 활용될 수 있다. 이에 대한 예시로 원자력시설에서 필수디지털자산으로 분류되는 PLC(Programmable Logic Controller) 자산에 '이블 PLC'라는 공급망 관련 공격[2]이 수행되었다. 해당 공격은 PLC를 공급망 공격을 통해 무기화하여 엔지니어링 워크스테이션을 손상시키는 과정으로 공격이 수행된다. 이후, 무기화된 PLC를 활용하여 원자력발전소 주요 인프라에 대한 사이버 위험을 발생시킨다.

이처럼, 주요기반시설에 해당하는 원자력발전소의 공급망 관련 안전과 보안을 유지하는 측면에 있어 자산을 체계적으로 관리하는 시스템을 요구한다.

하지만, 제어시스템 특성상 시스템 설계 및 변경의 제약으로 인해 소프트웨어 패치 및 설비 교체 시기가 매우 길기 때문에 자원에 관한 문서 작성자나 담당자의 역할이 일관되게 할당되지 않는다[3]. 그리하여 자산 정보에 관한 서술은 작성자에 따라 세부적으로 다를 수 있다는 한계점이 존재한다.

또한, 운영 환경 측면에서 관리 시스템의 자동화는 시스템 가용성에 위협을 초래할 가능성이 있으므로 문서 작성자가 수동으로 문서화를 진행하기 때문에 입력 오류와 같은 한계점이 존재한다[4].

이에 대해 본 논문은 원자력발전소의 자산 관리 체계를 수립하기 위해 운영 환경 기반의 SBOM (Software Bill Of Materials, 소프트웨어 자재명세서) 속성을 활용하여 원자력발전소 디지털 기기에 대한 일관된 정보 관리 방안을 제안한다. 또한, 입력 오류 한계점에 대해서는 자연어처리 기법을 활용한 N-gram 알고리즘 기반의 자산 관리 체계 방안을 제안한다.

II. 관련 연구

기존 운영 환경 공급망 보안 연구 및 원자력시설 공급망 공격벡터 분석을 통해 SBOM 기반의 자산관리체계 수립의 필요성을 언급한다. 이를 위해 운영 환경 기반 자산 관리 표준 및 가이드별 자산 유형 분류와 속성 정보를 파악한다. 또한, 국내외 자산 관리 체계 현황 및 한계점과 본 논문에서 활용할 SBOM의 현황에 대해 언급한다.

2.1 운영 환경 공급망 보안 관련 연구

2.1.1 운영 환경 공급망 보안 관리 모델

미국 바이든 행정부는 소프트웨어 보안을 강화하는 행정명령을 내렸고, 미국 CISA에서는 SBOM을, EU에서도 공급망 보안을 중시하고 있다.

이와 같이 공급망 보안에 관한 이슈가 중요시되고 있는 시점에서 미국 원자력 관련 사업자인 PSEG Nuclear LLC는 〔Fig .1.〕과 같은 사이버 보안 공급망 통합 관리 모델을 제시하였다.

PSEG Nuclear LLC는 PSEG Power LLC의 자회사 중 하나로 상업용 원자력 자산 운영을 마케팅 사업 및 연료 공급 기능과 통합하는 에너지 공급 회사이다. 이는 시설 운영 및 공급과정에서 일반적인 원자력 산업 표준을 활용한다[5].

관련 내용으로는 공급업체의 자산 기본 사양 정의 및 사용자 권한, 계정 활성화 여부, 물리적 접근 제한을 고려한 보안조치 관련 사항 등이 존재한다.

또한, 공급망 보안 관련하여 MITRE 社에서는 소프트웨어 공급망 보안을 수행하는 데 있어 SBOM 활용의 필요성을 제시한다[6].

Fig. 1. PSEG's Internal Cyber Security Supply Chain Integration Model

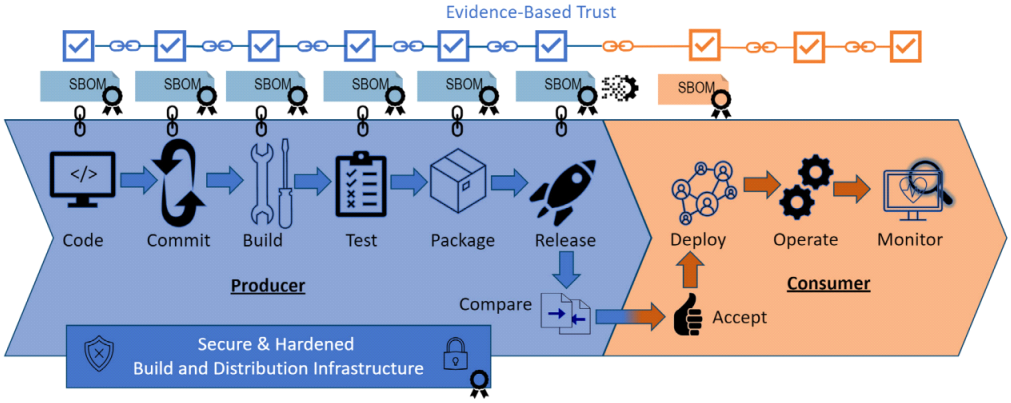


Fig. 2. Previously Proposed Framwork for software supply chain integrity by MITRE

이는 개발 및 운영, 보안을 개발 프로세스 전반을 내재화하는 DevSecOps를 강조하며, 〔Fig. 2.〕와 같이 SBOM 활용 공급망 보안 방식을 제시하였다.

해당 방식은 소프트웨어 제품의 모든 구성요소 구조, 출처, 무결성을 증명할 수 있는 표준화된 공급망 메타데이터 접근 방식이다. 그리하여 소프트웨어 수명 주기에서의 투명성을 제공하고, 자산 출처 정보를 활용하여 공급망의 무결성을 보장하는 데 활용된다.

이와 같이 공급망 보안은 공급업체 정보부터 자산의 속성까지의 모든 범위에서의 관리를 요구하며, 이는 SBOM을 활용한 관리의 필요성을 보여준다.

2.1.2 운영 환경 공급망 공격벡터

원자력시설 디지털 자산과 관련된 펌웨어, 하드웨어, 소프트웨어 등은 각각 설계 및 개발부터 최종 반환 처리 단계를 포함하는 공급망을 가지고 있다.

이에 대한 각 구성요소의 공급망 흐름 및 관계를 다음 〔Fig. 3.〕와 같이 보여준다. 이를 통해 공격 지점을 식별하여 발생할 수 있는 공급망 관련 공격도 식별할 수 있다[7]. 일반적으로 하드웨어, 펌웨어 및 시스템 정보는 장치 설치나 작동 중보다 공급망 활동 중에 손상되기 쉬운 반면, 소프트웨어는 전체 수명 주기 전반에 걸쳐 취약하다.

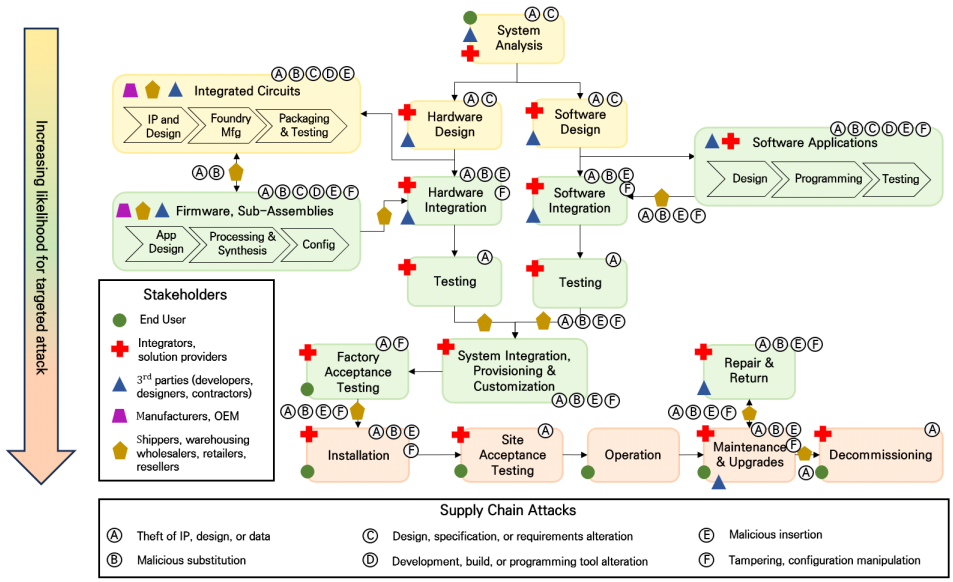


Fig. 3. Previously Proposed Supply chain attack vectors for digital assets in NPP

이로써 본 연구에서는 소프트웨어 관련 자산 혹은 특정 자산 내 활용되는 소프트웨어를 관리하기 위해 SBOM 속성에 기반하여 수명 주기 전반을 관리하는 자산 관리체계를 정의하고자 한다.

2.2 제어시스템 공급망 보안을 위한 자산 관리 표준 및 가이드

2.2.1 IEC 62443-4-2

국제전기기술위원회에서 발표한 국제 표준인 IEC 62443-4-2[8]는 산업제어시스템 보안 국제 표준인 IEC 62443의 일부로서 산업제어시스템 컴포넌트의 기술적 보안 요구사항을 명시하는 표준이다.

이는 4가지 종류의 자산 유형(소프트웨어 애플리케이션, 임베디드 디바이스, 호스트 디바이스, 네트워크 디바이스) 별로 분류된 장치 정보를 제공한다.

또한, 각 자산 유형에 대한 기본 보안 요구사항 및 관련된 상세한 기술적 제어시스템 컴포넌트 요구사항을 제공한다.

2.2.2 NEI 08-09

원자력에너지연구소에서 발표한 지침인 NEI 08-09[9]는 원자력 원자로에 대한 사이버 보안 계획을 명시한다. 이는 NIST 800-82 및 NIST SP 800-53의 내용인 산업제어시스템 보안 가이드, 권장 보안조치를 기반으로 하는 방어 아키텍처와 보안조치로 구성된 방어 전략을 설명한다.

공급망 관련하여 '11. SYSTEM AND SERVICES AQUISTION' 항목은 자산 수명 주기 동안의 문서화와 공급과정의 신뢰성을 언급한다.

또한, 필수디지털자산에 관한 공급망 보안을 위해 시스템 검증 및 테스트, 형상관리에 관한 보안조치 사항들을 명시한다.

2.2.3 Kaspersky

러시아 사이버 보안 회사인 Kaspersky는 산업 시스템 보안 솔루션으로 "Kaspersky Industrial CyberSecurity for Network"[10]를 발표하였다.

이는 산업용 네트워크에 연결된 자산 관리를 위해 자산 테이블을 생성하는 솔루션이다. 이는 다음 [Table 1]과 같이 자산 분류 유형을 나타낸다.

Table 1. Kaspersky Asset types

Asset types	Description
PLC	Programmable logical controllers
IED	Intelligent electronics
HMI / SCADA	Computer installed for HMI or SCADA system
Engineering workstations	Computers used by ICS engineers
Server	Device with server software installed
Network devices	Network devices, such as routers and switches
Workstations	Personal computer or production workstation
Mobile device	Portable electronic devices with computer functionality
Others	Devices not in categories listed above

[Table 2]는 [Table 1]에서 분류된 자산들로부터 수집하는 정보 목록 즉, 자산 속성에 해당한다.

해당 정보를 활용하여 자산 활동을 모니터링하고 네트워크 패킷으로 수신된 데이터를 기반으로 자산 정보의 변경 사항을 추적할 수 있다.

Table 2. Kaspersky Asset Attribute information

Asset information	Description
Name	Asset name in the application
Asset ID	Kaspersky Assigned Asset ID
Status	Status information about an asset to determine whether the asset is active or not. (authorized, unauthorized, archived)
Address information	MAC, IP address of the asset
Category	Category names determined by the purpose of the asset
Group	Name of the group
Security state	Determined by the severity level of the event (Critical, Warning, OK)
Last seen	The date and time the last activity was recorded

Asset information	Description
Last modified	The date and time the information was last modified.
Creation date	Date and time the asset was added to the asset table
OS	Name of system installed on the asset
Vendor	Name of the manufacturer
Model	Product information
Network name	Name of the asset on the network
Labels	List of labels assigned to the asset

2.2.4 INCIBE-CERT

INCIBE-CERT는 스페인 국립 사이버 보안 연구소이며, "Guide for an asset inventory management in industrial control systems" 문서[11]를 활용하여 산업제어시스템 자산관리체계를 설명한다.

이를 활용하여 산업제어시스템 보안의 프로세스와 관련된 모든 자산 목록을 포함하여 소프트웨어 및 펌웨어 버전과 같은 각 자산에 대한 상세 정보를 수집한다. 이는 다음 [Table 3]에서 제시한 자산 분류 유형에 따라 나타난다.

보안 및 위험 관리 측면에서 각 자산에 대한 상세 정보를 저장하는 것이 중요하다. 해당 문서에서 명시하는 중요 자산 속성 정보는 다음 [Table 4]와 같이 나타난다.

이를 통해 시스템에 설치된 버전 정보, 제품 정보를 통해 시스템의 취약점을 쉽게 관리할 수 있고, 넓은 범위에서 운영 프로세스와 관련된 모든 자산을 파악하여 체계적인 관리가 용이하다.

Table 3. INCIBE-CERT Asset types

Asset types	Description
Hardware	Physical equipment used in industrial process development
Software	Applications for managing processes
Employee	People who work for your organization
Information	Data created, collected, managed, transferred, and destroyed
Network	Network-connected equipment
Techniques	The equipment you need to manage your company and business
Assistive equipment	Communication functions direct, non-communication functions direct, indirect, BOP, emergency response, non-critical digital assets
Facilities	Where your company's critical equipment is located

Table 4. INCIBE-CERT Asset Attribute information

Asset information	Description
Identifier	The only code that identifies each asset
Name	Product information, trademarks, versions, etc.
Manufacturer	Manufacturer or developer
Description	Usage information for assets
Type	Type & model name of the asset
Owner	Who is responsible for asset decisions
Manager	Who is responsible for managing the asset's operability and access
Location	Where the asset is located
Version of Software	Summary of installed software on your device
Asset evaluation	Assess the impact and importance of assets in your system

2.3 국내외 원자력시설 자산 관리 체계 현황

2.3.1 국외 원자력시설 자산 관리 체계 현황

국외 원자력시설 자산 관리는 관련 연구에서 언급했던 Kaspersky와 INCIBE-CERT와 같이 분류 유형 및 자산 속성 정보를 도출하며 진행 중에 있다.

또한, 현재 건설이 진행되거나 시운전 중인 미국의 Vogtle 원자력발전소, 아랍에미리트 Barakah

Table 5. International nuclear power plant Asset Attribute information

Asset information	Details
Firmware	Firmware version and description
OS	Description of the OS and update versions and methods
Software	Software version and patch levels and how to update
Physical communication ports and terminals	Connect all physical communication ports and terminals
Portable media and portable devices	All removable media and portable devices
HMI functions	All HMI features
Available data communication protocols	Communication protocols and methods available for all data types
Data files, software objects	All data files, software objects, services, and logical ports installed on the asset.
Active scans used to retrieve asset attributes	Search tools used to perform active searches and the types of searches performed
Installed features that can be removed that affect all attacks	Installation features and options to remove or disable impact on all attack vectors
Ability to install third-party software	Setup and data flow

원자력발전소 등 신형 원자력시설[12]에서 보안 취약점 평가 용도로 자산 속성 정보를 다음 [Table 5]와 같이 수집하였다.

하지만, 미국 원자력발전소 운영 사업자인 테네시 강 유역 개발 공사가 2016년에 원자력 자산 중 약 6%만이 운영체제를 사용한다는 결과를 공개하였다. 이는 대부분의 장치가 임베디드 장치로 활용되기 때문에 자산 내 패치가 어렵다는 것을 의미하는 것이다[13]. 즉, 해당 자산의 업데이트 수행 시 자산 내의 소프트웨어에 관한 문서를 관리하는 것이 어렵다는 의미도 존재한다.

2.3.2 국내 원자력시설 자산 관리 체계 현황

국내 원자력시설 자산 관리에 있어 정보 수집 방식은 일반 정보 기술 환경과는 달리 운영 환경 특성을 고려해야 한다. 이에 대해 다음 [Fig. 4.]과 같은 방안으로 정보 수집 방식을 결정한다[14].

"Configuration Analysis"는 기기 설정 파일이나 자산 파일을 구문 분석하는 방법으로 최신 상태의 파일을 활용한다. 이는 수명 주기가 긴 원자력시설 자산 특성으로 업데이트 반영에 있어 어려움이 있다.

"Active Scanning" 및 "Passive Scanning"는 스캐닝 도구 활용으로 인해 가용성을 중시하는 원자력시설 내 자산에 치명적인 영향을 배제할 수 없기에 적용하는 데 어려움이 존재한다.

"Physical Inspections"는 수작업 과정이기에 시간이 많이 소요되거나 조사 과정 중 구성요소 혹은 시설의 누락이 발생할 수 있다는 문제점이 존재한다. 하지만, 운영 환경 특성상 사람이 직접 관리하는 것이 보안적인 면에서는 가장 적합한 방안으로 선택된다. 그리하여 원자력시설 내 디지털 자산의 조사 방법은 물리적 조사 방법으로 제한된다.

위 조사 과정 기반으로 자산을 관리하는 데 있어 NVD(National Vulnerability Database) 내 CPE(Common Platform Enumeration) 정보를 활용한다. CPE[15]는 기업의 컴퓨팅 자산이 사용하는 하드웨어, 운영체제, 애플리케이션 식별 및 표준화된 방법이다.

이를 통해 자산에 대한 취약성을 식별할 수 있으며, NVD에서 제공하는 취약점 정보도 즉각적으로 확인 가능하다. 또한, 이는 구조화된 형식을 지니기에 자산 관리에 필수적으로 활용되는 요소이다.

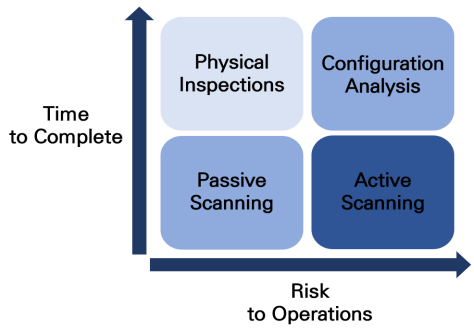


Fig. 4. Time and Risk Graph Based on Asset Management Information Collection Process

Table 6. CPE Attribute information

CPE Attribute	Description
cpe_version	cpe defined version - 2.3
part	Asset types
vendor	Manufacturers and suppliers of assets
product	Asset name
version	Versions of systems, packages, and components
update	Update information for assets
edition	Current version information for the asset
language	User interface supported languages
sw_edition	User specific information
target_sw	Requirements for the software environment
target_hw	Hardware environment requirements for the product

CPE는 cpe:〈cpe_version〉:〈part〉:〈vendor〉:〈product〉:〈version〉:〈update〉:〈edition〉:〈language〉:〈sw_edition〉:〈target_sw〉:〈target_hw〉:〈other〉와 같은 구조를 가지며, 다음 〔Table 6〕에서 각 요소를 설명한다.

해당 정보를 활용하여 자산 관리를 하는 데 있어, 실제로 자산은 존재하지만, 'SooSan', 'WOORI'와 같은 국내 공급업체의 정보는 CPE에 존재하지 않아 자산 정보를 수집하는 데 있어 오탐 및 미탐을 일으킬 수 있는 "CPE 내 제품 부재" 문제점이 존재한다.

국내 원자력시설에는 자산 관리 체계가 존재하지만, 물리적 조사 즉, 수동적 조사를 통한 '자산 구성요소 및 시설 누락의 문제점'이 존재한다. 또한, 해당 자산 정보를 CPE 정보로부터 얻어올 수 없는 'CPE 내 제품 부재'에 대한 문제점이 존재한다.

이에 본 연구는 입력 오류 개선 방안을 위한 자연어처리 방안 및 CPE 정보 수집 개선을 위한 SBOM 기반 자산 상세 정보 도출 방안을 제안한다.

2.4 소프트웨어 자재명세서 (Software Bill Of Materials, SBOM)

소프트웨어 자재명세서는 소프트웨어의 구성요소, 버전, 출처, 상세 내역, 개별 컴포넌트 정보 등 소프트웨어의 모든 항목을 확인할 수 있는 문서이다.

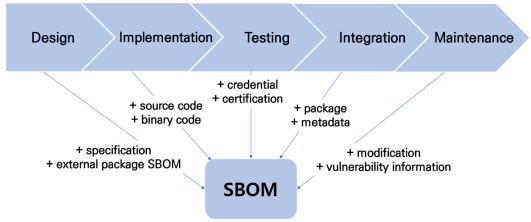


Fig. 5. SBOM Information According to the Software Development Lifecycle

위 항목들을 활용하여 다음 〔Fig. 5.〕와 같은 소프트웨어 수명 주기를 관리함으로써 소프트웨어의 투명성, 라이선스 준수, 의존성 분석, 취약점 관리 등을 통해 공급망의 복잡성과 위험을 관리한다.

SBOM을 작성하는 데 있어 활용되는 데이터 필드는 자원 구성요소, 공급업체 이름, 구성요소 간의 연관관계 등의 여러 정보가 활용되며, 기본 속성 정보로 다음 〔Table 7〕과 같이 정의된다〔16〕.

이와 같은 형식을 기반으로 하여 현재 미국은 2021년 '국가 사이버보안 개선' 행정명령(EO 14028호)을 발표한 것을 계기로 각 제품에 대한 SBOM을 공개적으로 게시하고 있다.

이처럼 SBOM은 컴포넌트의 종류와 버전 정보를 확인하여 취약한 컴포넌트를 관리하는 등의 취약점

Table 7. Fundamental Attributes of SBOM

SBOM Attribute	Description
Author Name	The name of the SBOM author
Timestamp	The date and time of the last update to the SBOM
Supplier Name	The name or other identifier of the supplier of the component in the SBOM item
Component Name	The name or other identifier of the component
Version String	The version information of the component
Component Hash	The cryptographic hash value of the component
Unique Identifier	Additional information that helps uniquely define the component
Relationship	Relationship information between SBOM components

관리에도 활용될 수 있다[17].

하지만, 원자력시설 특성을 고려하지 않고, SBOM 기본 속성만을 활용하여 원자력시설의 취약점 분석을 하는 것은 한계점이 존재한다.

이에 본 연구는 원자력시설 특성을 반영하여 SBOM 속성을 재구성하는 방안을 제안한다.

III. 원자력시설 내 자산관리체계 구축을 위한 SBOM 구현방안

본 연구는 원자력시설 자산 관리를 위해 운영 환경 특성을 고려한 자산 속성 정의 및 자산 입력 오류 문제에 관한 자연어처리 알고리즘 활용 방안을 통해 [Fig. 6.]과 같은 SBOM 구현방안을 제안한다.

3.1 SBOM 속성 정보 도출

원자력시설 공급망 보안 요구사항 분석은 [Fig. 5.]와 같은 흐름으로 설계, 제작, 납품, 설치 등의 전 단계에 걸쳐 사이버보안 통제를 요구하고 있다.

이에 요구사항에 대한 자산 정보를 관리하기 위해 SBOM 기반의 25가지 속성 정보를 [Table 8]과 같이 정의한다.

우선 SBOM의 기본 속성과 운영 환경 기반 자산 관리 표준의 속성들을 연계하여 “Asset types”, “Manufacturer / Supplier”, “Asset registration name, “Model Version”, “Asset type details”, “Whether wireless communication is enabled & Wireless communication type”, “Whether to communicate encrypted”, “Communication connectivity”, “Application service availability”와 같은 SBOM 속성이 도출된다.

이는 자산에 대해 제조사, 이름, 버전 등의 식별 정보와 무선 통신의 유무, 통신 암호화, 통신 연결성, 응용 서비스의 사용 가능성인 기본 통신 정보를 정의한다.

하지만, 기본 속성들로만 구성된 SBOM의 활용은 유지보수 관점에 있어 패치 상태에 대한 관리 부재 및 해당 정보의 정확성을 검증할 수 있는 방법이 부재되었다는 문제점이 존재한다.

그리하여 디지털자산에 대한 유지보수 관리 측면

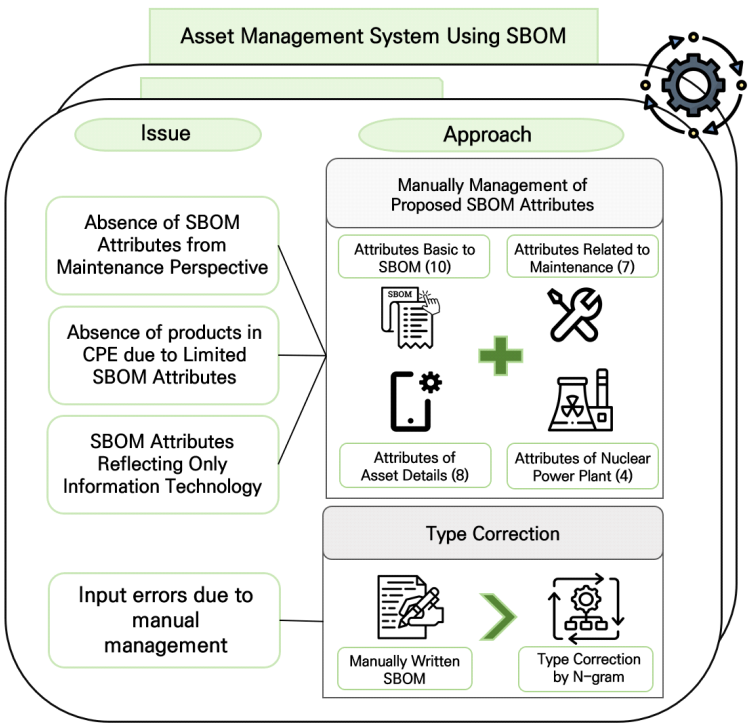


Fig. 6. Asset Management System Using Proposed SBOM Attributes

Table 8. Proposed SBOM attributes

Category	Asset Attribute	Attribute Information
Attributes Basic to SBOM	Asset types	Hardware, Software, Network Device, Information Security Device
	Asset type details	PLC, SCADA, Database, Router, Firewall, etc.
	Manufacturer / Supplier	〔Manufacturer / Supplier name〕
	Asset registration name	〔Asset name〕
	Model Version	〔Model Version〕
	Communication connectivity	O,X
	Whether wireless communication is enabled	O,X
	Wireless communication type	Wifi, Bluetooth, etc.
	Application service availability	O,X
	Whether to communicate encrypted	O,X
Attributes Related to Maintenance	Whether the media connection port is physically blocked	O,X
	Whether the device connection port is physically blocked for maintenance	O,X
	Whether to connect media (USB, etc.)	O,X
	Whether to use a connected device for maintenance	O,X
	Asset access rights	Administrator, Operator, No permission
	Whether to approve a task	O,X
	Whether you have account management capabilities	O,X
Attributes of Asset Details	interfaces	Ethernet, JTAG, Fiber Optic, etc.
	protocols	TCP/IP, TCP/UDP, etc.
	OS name	〔OS name〕
	OS version	〔OS Version〕
	Firmware name	〔Firmware name〕
	Firmware version	〔Firmware Version〕
	Application name	〔Application name〕
	Application version	〔Application Version〕

연결 포트 관리에서의 “Whether the device connection port is physically blocked for maintenance”, “Whether to use a connected device for maintenance”와 유지보수를 위한 공급업체의 접근 기록을 관리하는 “Whether to approve a task”가 존재한다.

또한, 소프트웨어 자재명세서이기에 물리적 측면에서의 소프트웨어 위협을 분석하는데 있어 충분한 정보를 제공하지 않기에 추가적인 정보가 필요하다.

물리적 접근에서의 자산 관리를 위해서는 “Whether the media connection port is physically blocked”, “Ability to connect media (USB, etc.)와 자산에 대한 접근 권한 부여 및 식별을 위한 “Asset access rights”, “Whether you have account management capabilities”가 존재한다.

마지막으로 국내 원자력 시설 자산 관리 체계의 한계점으로 언급했던 “CPE 내 제품 부재”에 대한 한계점의 개선 사항으로 자산 내 활용되는 디지털 기기에 대한 세부 속성 정보를 활용한다.

이는 “OS name & version”, “Firmware name & version”, “Application name & version”, “interfaces & protocols” 속성 정보가 존재하며, 이를 활용하여 자산 내 기기 식별을 함으로써 내재된 취약점 관리에도 활용될 수 있다.

3.2 원자력 환경 특성을 반영한 속성 정보 도출

원자력 시설은 주요기반시설에 해당하기에 일반 정보 기술에서 활용한 SBOM 속성만을 활용하여 자산을 관리하는 데 한계점이 존재한다. 이에 운영 환경에서 적용되는 Purdue 모델, 원자력시설에서 적용되는 필수디지털자산의 식별 및 위치 정보 등 4가지 자산 속성 정보를 〔Table 9〕와 같이 활용한다.

“Physical location of assets”는 원자력 시설에서의 자산이 위치한 구역을 기준으로 어느 영역에 위치해있는지를 나타내는 지표이며, 〔Fig. 7.〕와 같이 식별된다.

이는 원자력에너지연구소와 국제 원자력기구의 물리적 방호 권고안인 INFCIRC/225/Rev.5', 미국 원자력 규제 위원회(nuclear regulatory commission)의 원자력 시설의 물리적 방호 규정 '10CFR73.55'에 근거하여 원자력 시설에 맞게 적용

Table 9. Proposed SBOM attributes reflecting nuclear power plant environment

Category	Asset Attribute	Attribute Information
Nuclear Power Plant Attribute	Physical location of assets	Core zone, protected zone, owner-controlled zones
	Network security layers	Level 0~5
	Whether to communicate one-way	O,X
	Consequence Classification	Direct CDA, EP CDA, BOP-CDA(Trip), BOP-CDA(Transient), Indirect CD

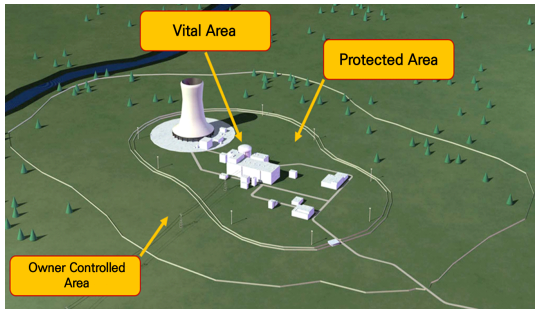


Fig. 7. Nuclear Facility Asset Locations

하였다.

자산 위치별로 취약점 발생 시 영향 정도의 차이가 발생하기에 이는 자산 관리에 있어 “Physical location of assets” 속성을 활용할 수 있다.

“Network security layers” 및 “Whether to communicate one-way”는 ISA-99에서 PERA (Purdue Enterprise Reference Architecture)로부터 도입해 채택한 모델인 Purdue 모델〔18〕 관련 자원 관리 속성이다.

Purdue 모델은 〔Fig. 8.〕와 같이 구성되며, IT(Information Technology) 영역인 외부망과 OT(Operational Technology) 영역인 내부망으로 이루어져 있다. “Network security layers”는 Purdue 모델의 계층을 나타내며, 내부망의 취약점 관리를 위해 해당 자산 속성을 활용한다. 또한, “Whether to communicate one-way”는 취약점 관리 면에서 외부망에서 내부망으로의 통신을 통해

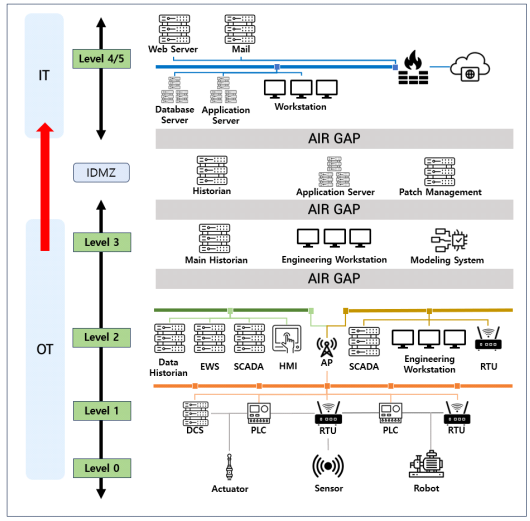


Fig. 8. Purdue model

외부 위협 발생 가능성을 의미하기에 자산 속성으로 정의한다.

마지막으로 원자력발전소 환경 특성인 SSEP(Safety, Security, Emergency Preparedness)기능 수행 단계에 따라 식별되는 필수디지털자산의 분류 정보를 활용한다.

이는 원자력에너지연구소에서 발표한 NEI 13-10 내 필수디지털자산 식별 절차[19]를 활용한다. 5가지 자산 형식으로 구분되며, SSEP 기능에 따라 자산의 중요도가 변화하기에 이는 취약점 관리에 용이할 것으로 보여 자산 속성인 "Consequence Classification"으로 활용한다.

3.3 입력 오류 개선을 위한 자연어처리 활용

원자력 시설 자산은 "Physical Inspections" 조사를 통해 관리된다. 조사 과정 중 구성요소 혹은 시설의 누락이 발생한다는 문제점이 발생한다. 이에 자연어처리 기반으로 자산 관리 체계인 CPE 를 활용하여 입력 오류 문제를 해결하고자 한다.

자연어처리를 수행하는 알고리즘으로는 N-gram 알고리즘[20]을 활용한다. 이는 카운트 기반의 통계적 접근법을 활용한 SLM(Statistical Language Model)의 일종이다.

N-gram은 임의의 개수 n개의 연속적인 단어 나열을 의미한다. 입력값인 corpus에서 n개의 단어 단위로 끊어서 이를 하나의 토큰으로 간주한다.

[Fig. 9.]와 같은 과정으로 수행되며, 입력받은 문자열인 "cosmo"를 통해 n=2일때의 예시를 진행하였다.

입력값을 통해 나올 수 있는 토큰값은 "co", "os", "sm", "mo"가 존재하며, 각 토큰의 문자열 순서도를 고려하여 도출될 수 있는 실제 존재하는 단어를 교정 문자열 후보로 선정한다.

이후, 입력값의 토큰들과 교정된 문자열의 토큰들 값을 비교하여 Jaccard 유사도[21]를 산출한다.

$$J(A,B) = \frac{|A \cap B|}{|A \cup B|} = \frac{|A \cap B|}{|A| + |B| - |A \cap B|} \quad (1)$$

Jaccard 유사도는 0과 1사이의 값으로 두 집합 사이의 유사도를 측정하는 방법으로, 1에 가까울수록 두 집합이 비슷한 성질을 가지고 있다는 의미이다. 이는 위 정의식을 활용하여 측정할 수 있다.

산출된 유사도 중, 가장 높은 교정 문자열 후보를 최종 교정 문자열로 선택하게 된다.

본 논문은 해당 알고리즘을 활용해 올바른 CPE 정보와 오입력된 자산 정보 비교를 통한 오탈자 교정을 수행하여 원자력시설의 입력 오류 한계점을 개선하고자 한다.

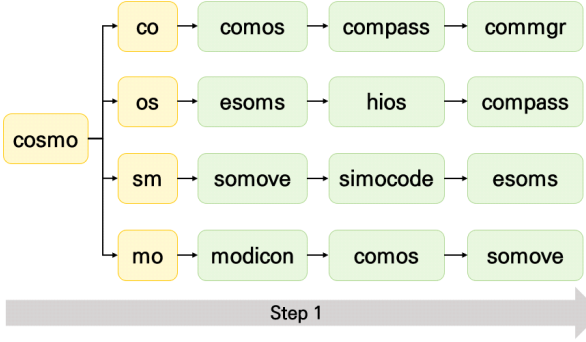
IV. 사례 연구

4.1 SBOM 속성 정보를 활용한 취약점 관리

4.1.1 CPE 제품 검색을 위한 SBOM 속성 정보 적용

해당 사례 연구는 SBOM 기본 속성 적용 및 제안된 SBOM 속성 적용을 비교 분석하여 효율성을 검증하고자 한다. 이에 취약점 관리 측면에서 검증을 위해 취약점 정보와 연계된 CPE 체계를 활용한다.

사례 연구에서 활용되는 자산 정보는 국내 원자력시설에서 사용되어지는 필수디지털자산 중 일부이며,



N-gram of Input string(A)	N-gram of correction string(B)	Number of Nested strings (A ∩ B)	Similarity of Nested N-gram ((A ∩ B)/(A ∪ B))
cosmo / 4	comos / 4	3	0.6
	compass / 6	1	0.11
	commgr / 5	1	0.13
	esoms / 4	0	0.13
	hios / 3	1	0.17
	somove / 5	1	0.13
	simocode / 7	2	0.2
	modicon / 6	2	0.25

Step 2

Fig. 9. The process of calculating N-gram nested similarity

〔Table 10〕과와 같이 명시된다.

각 제조사 혹은 자산명에 대해 CPE 내 자산 존재 여부를 판단해본 결과 국내 제조업체인 WOORI를 제외하고 모두 존재하는 것을 알 수 있다.

CPE 내 자산 정보가 없다는 것은 자산에 대한 취약점 정보를 얻을 수 없기에 취약점 관리 면에서 충분한 정보를 얻기에 어려움이 존재함을 나타낸다.

하지만, 본 논문에서 제안한 SBOM 속성 정보를 활용하면 추가적인 정보를 통해 CPE 정보와 연계될 수 있다.

이에 대해 WOORI 제조사의 OPERASYSTEM 1400 자산은 비안전 시스템 개발을 위해 VxWorks 운영체제가 존재한다〔22〕. 이를 CPE 체계 적용 시 “CVE-2023-38346”, “CVE-2022-3877”, “CVE-2021-43268”과 같은 총 17개의 취약점이 발견됨을 알 수 있다〔23〕.

이를 통해 본 연구에서 제안한 SBOM 속성 정보는 기본 속성만을 활용했을 때보다 상세한 정보를 제공하여 추후 발생할 수 있는 자산에 대한 취약점 관리에 용이하다는 것을 나타낸다.

Table 10. Case Asset Information

Manufacture	Asset name	Version
Advantech	WebAccess/SCADA	-
BlackBerry	QNX OS for Safety Version	1.0.1
Schneider	EcoStruxure Control Expert	v15.0 SP1
WOORI	OPERASYSTEM 1400	-
Siemens	SCALANCE X202	-

4.1.2 원자력시설 취약점 관리를 위한 SBOM 속성 정보 적용

해당 사례 연구는 본 논문에서 제안한 SBOM 속성 정보 기반으로 원자력시설 내 자산 정보에 적용하여 취약점 관리 측면의 효율성을 검증하고자 한다.

다음 〔Table 11〕은 제안하는 SBOM 속성에 맞게 원자력시설 내 자산 정보를 입력한 것이다.

해당 자산의 “Asset registration name” 정보 기반으로 ICS CERT Advisory 연계〔24〕를 통해 자산에서 발생할 수 있는 공통 취약점이 식별된다.

식별된 취약점들의 description 정보와 SBOM

Table 11. Application of the proposed SBOM on the assets of nuclear facilities

SBOM Attribute	Description
Asset types	Hardware
Asset type details	HMI
Manufacturer / Supplier	Siemens
Asset registration name	simatic_hmi_basic _panels
Model Version	-
Whether the media connection port is physically blocked	X
Whether the device connection port is physically blocked for maintenance	O
Ability to connect media (USB, etc.)	O
Whether to use a connected device for maintenance	X
Communication connectivity	O
interfaces	Ethernet, USB Port, RS-485, PS-2, Fiber Optic
protocols	TCP/IP
Whether wireless communication is enabled	-
Wireless communication type	-
OS name	QNX
OS version	6.4.1
Firmware name	-
Firmware version	-
Application service availability	O
Application name	NVIDIA TrustZone software DRM application
Application version	-
Whether to communicate encrypted	X
Asset access rights	Administrator
Whether to approve a task	O

SBOM Attribute	Description
Whether you have account management capabilities	O
Physical location of assets	Protected Area
Network security layers	level 2
Whether to communicate one-way	O
Consequence Classification	B-Class Direct CDAs

속성 정보를 비교 분석한 결과, “CVE-2020-7592”는 SBOM “Whether to communicate encrypted” 속성에서 표기된 암호화 통신을 하지 않는 점을 이용하여 일반 텍스트 통신을 캡처하고 민감 정보에 접근하는 취약점이다.

또한, “CVE-2015-2823”과 “CVE-2020-15786”은 원격 공격 기반 취약점이지만, SBOM “Whether wireless communication is enabled” 속성에서 표기된 무선 통신 기능의 비활성화 상태를 통해 해당 자산에는 유효하지 않은 취약점임을 알 수 있다.

이처럼 같은 자산임에도 불구하고, 제조사가 공급 전 미리 취약점에 수행한 조치 사항 및 원자력 점검 주기 동안 변경 사항을 SBOM을 통해 관리함으로써 취약점 관리에 용이하다는 것을 나타낼 수 있다.

또한, 해당 자산의 공격벡터가 무엇인지, 더하여 어떤 취약점을 이용해서 악용될 수 있는지에 관한 정보를 제안된 SBOM을 활용하여 얻을 수 있다.

추가적으로, 원자력 환경 기반의 취약점 심각도 점수를 평가할 때 원자력시설 특성을 반영한 4가지 속성 정보를 활용하는 방안도 존재한다.

4.2 오입력 자산 정보 교정

해당 사례 연구는 오입력 자산을 입력값으로 받아와 본 연구에서 제안한 N-gram 방안을 적용하는 방식으로 제안하는 바에 대한 검증을 수행한다.

오입력된 자산은 제조사명과 자산 등록 명칭만을 활용하여 각각 “adventeh”, “iviw” 문자열을 입력값으로 활용하였다.

이를 본 연구에서 제안한 N-gram 방식 (n=2)에 적용해보았을 때 〔Table 12〕과 같은 과정을 통해 “advantech”이라는 제조사가 가장 높은 유사도로 측정되어 도출된다.

Table 12. "adventeh" manufacturer typo correction algorithm case study

N-gram Input string(A)	N-gram correction string(B)	Number of Nested strings ($A \cap B$)	Similarity of Nested N-gram ($(A \cap B)/(A \cup B)$)
adventeh	advantech	4	**0.36**
	myscada	1	0.08
	prodox	0	0
	davolink	0	0
	invensys	2	0.18
	aveva	1	0.11
	novatech	1	0.08
	centreon	2	0.18
	prominent	2	0.17
	detcon	0	0
	intel	1	0.11
	jantek	2	0.2
	fernhill	0	0

자산 등록 명칭을 활용한 N-gram 방식에서는 〔Table 13〕과 같이 “iview”라는 자산이 가장 높은 유사도로 측정된다. 이와 같이 최적의 교정 자산 속성 도출이 가능하다.

하지만, 다른 예시로 실제 관리자가 제조사에 대해 “adventeh”이 아닌 “nocatech”라는 정보를 입력했을 때〔Table 14〕와 같이 기대하는 값과는 다르게 “novatech”이 결과로 나오는 것을 볼 수 있다.

이에 대해서는 CPE 정보를 활용하여 해당 제조사에 대해 “iview“라는 모델명의 존재 여부를 판단하

Table 13. “iviw” asset name typo correction algorithm case study

N-gram Input string(A)	N-gram correction string(B)	Number of Nested strings ($A \cap B$)	Similarity of Nested N-gram ($(A \cap B)/(A \cup B)$)
iviw	iview	2	**0.4**
	siveillance	1	0.08
	LVIS	1	0.2
	kingview	1	0.11
	mxview	1	0.14
	amegaview	1	0.1

여 적절한 교정 결과인지를 판단하게 된다.

〔Table 14〕와 같이 "novatech"이 결과로 도출되어도 CPE 정보에는 해당 모델명으로 "iview"가 존재하지 않기에 잘못된 교정으로 판단한다. 두 번째 우선순위인 "advantech"의 CPE 연계 결과, "iview" 모델 명의 존재로 인해 올바른 교정으로 판단하는 방식으로 자산 정보 교정이 진행된다.

제조사, 자산 명칭뿐 아니라 모든 문자열 데이터의 오입력 자산을 교정할 수 있다. 이로써 CPE 정보와의 연계 여부 판단으로 취약점 관리를 수행한다.

Table 14. "nocatech" manufacturer typo correction algorithm case study

N-gram Input string(A)	N-gram correction string(B)	Number of Nested strings $(A \cap B)$	Similarity of Nested N-gram $((A \cap B)/(A \cup B))$
nocatech	novatech	5	**0.56**
	advantech	3	0.25
	canonical	2	0.15
	synology	1	0.08
	novell	1	0.09
	nordex	1	0.09
	carefusion	1	0.07
	intel	1	0.1
	jentek	1	0.09
	centreon	0	0
	detcon	0	0

V. 결 론

최근 원자력발전소의 디지털화된 시스템 도입 증가에 따라 "이블 PLC"와 같은 공급망 피해도 증가하는 추세이다. 공급망 보안 관리에 있어 원자력발전소 특성상 수많은 공급업체가 존재하기에 이를 체계적으로 관리할 수 있는 자원 관리 시스템이 필요하다.

하지만, 원자력시설은 소프트웨어 패치 및 설비 교체 시기가 매우 길기 때문에 자원 관리가 일관적인 형식으로 수행되지 않는다는 문제점이 존재한다. 또한, 관리 시스템들의 자동화는 가용성을 중시하는 운영 환경에서 활용이 불가능하기에 자산 관리가 수동으로 실행되어 입력 오류와 같은 한계점이 발생한다.

이에 본 논문은 일관적이며 체계적인 자원 관리 시스템을 위해 소프트웨어 자재명세서인 SBOM 구현 방안에 대해 제안한다. 기존 SBOM 속성에 환경 특성을 고려한 추가 속성을 적용하여 관리하도록 하며, 입력 오류와 같은 문제를 N-gram 모델을 활용하여 정확한 정보를 관리하도록 한다.

사례 연구에서와 같이 취약점 관리 면에서의 자원 관리는 중요하다. 추후 연구로는 해당 자산 관리 체계를 활용하여 각 자산에 해당하는 취약점을 원자력 시설 환경에 맞게 정량적인 평가가 가능한 심각도 점수를 산출하고자 한다. 추가적으로, 취약점 관리를 위해 수행해야 하는 보안조치를 관련 규제 및 가이드를 통해 연계하여 도출하는 연구를 향후 연구로 진행하고자 한다.

References

〔1〕 LIM, SOO MIN, KIM, ARAM & SHIN, ICKHYUN. International Nuclear Power Digital Asset Supply Chain Cybersecurity Regulatory Trends. Jonornal of The Korea Institute of information Security & Cryptology, 26(1), 54-60. Feb. 2016

〔2〕 DATANET, "Evil PLC" https://www.datanet.co.kr/news/articleView.html?idxno=182329. Apr. 2024

〔3〕 KIN, "KINS/GI-N001", Vol.4, Rev.6 p.779. Dec. 2020

〔4〕 Do-Yeon Kim. Security Criteria for Design and Evaluation of Secure Plant Data Network on NuclearPower Plants, 9(2), 267-271. Feb. 2014

〔5〕 PSEG, "PSEG Nuclear LLC", https://investor.pseg.com/investor-news-and-events/financial-news/financial-news-details/2019/PSEG-Power-Names-Eric-Carr-to-Replace-Pete-Sena-as-PSEG-Nuclear-President--and-Chief-Nuclear-Officer/default.aspx. Apr. 2024

〔6〕 MITRE Corporation, "DELIVER UNCOMPROMISED: SECURING CRITICAL SOFTWARE SUPPLY CHAINS" p.9. Jan 2021

〔7〕 Eggers, S. A novel approach for analyzing the nuclear supply chain

cyber-attack surface. Nuclear Engineering and Technology, 53(3), 879-887. Aug. 2020

〔8〕 International Electrotechnical Commission "ICS Security" Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components. Feb. 2019

〔9〕 Nuclear Energy Institute. "NEI 08-09 Cyber Security Plan for Nuclear Power Reactors" Rev.6. Apr. 2010

〔10〕 Kaspersky. "Kaspersky Industrial CyberSecurity for Networks." 2024

〔11〕 INCIBE-CERT. Guide for an asset inventory management in industrial control systems(pp. 8-13). INCIBE-CERT. Mar 2020

〔12〕 Korea Energy Economics Institute, "World Nuclear Power Market INSIGHT", p.8, p.35 Sep. 2021

〔13〕 Chowdhury, N. CS measures for nuclear power plant protection: A systematic literature review. Signals, 2(4), 803-819. Nov 2021

〔14〕 SANS, "Asset Management", https://www.sans.org/blog/consequence-driven-ics-risk-management/ Apr. 2024

〔15〕 NIST, " Common Platform Enumeration" https://nvd.nist.gov/products/cpe. Apr. 2024

〔16〕 Hyeong-Dong Lee. "A Study on Factors Affecting the Intention to Adopting Software Bill of Materials for Cyber Security." ,Jun 2023.

〔17〕 The KOREA INDUSTRY DAILY, "SBOMM & CVE" https://kidd.co.kr/news/234144. Apr. 2024

〔18〕 Pascal Ackerman, Industrial Cybersecurity: Efficiently secure critical infrastructure systems (ISBN 9781788395151) p.41-43. Oct 2017

〔19〕 Nuclear Energy Institute, NEI 13-10, Rev. 5, Cyber Security Control Assessments, Feb 2017

〔20〕 Vatanen, T., Väyrynen, J. J., & Virpioja, S. . Language Identification of Short Text Segments with N-gram Models. In LREC. pp. 3423-3430. (2010, May)

〔21〕 Ivchenko, G. I., & Honov, S. A. On the jaccard similarity test. Journal of Mathematical Sciences, 88, 789-794.(1998)

〔22〕 Acronym, A. P. R. "Status Report 103 - Advanced Power Reactor (APR1000)."

〔23〕 NIST, "VxWorks CPE" https://nvd.nist.gov/products/cpe/detail/F46FF171-5FC4-442F-B350-B35431ECF559, Apr. 2024

〔24〕 CISA, "ICS-CERT Adviories", https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A95. Apr. 2024

〈저자소개〉

김 도 연 (Do-yeon Kim) 학생회원
2022년 8월: 전남대학교 물리학과 학사 졸업
2022년 9월~현재: 전남대학교 정보보안융합학과 석사과정
〈관심분야〉 정보보호, 산업제어시스템 보안, 원자력 보안, 취약점 분석, 인공지능

윤 성 수 (Seong-su Yoon) 학생회원
2021년 2월: 전남대학교 소프트웨어공학과 학사 졸업
2023년 2월: 전남대학교 정보보안협동과정 석사 졸업
2023년 3월~현재: 전남대학교 정보보안융합학과 박사과정
〈관심분야〉 정보보호, 인공지능, 산업제어시스템 보안

엄 익 채 (Ieck-chae Euom) 종신회원
2003년 8월: 전남대학교 컴퓨터정보학부 학사 졸업
2015년 2월: 한국과학기술원 소프트웨어대학원 석사 졸업
2019년 2월: 전남대학교 정보보안협동과정 박사 졸업
2003년~2007년: LG이노텍, 주임연구원
2007년~2019년: 한전KDN, 차장
2019년 10월~현재: 전남대학교 시스템보안연구센터 소장, 데이터사이언스대학원 교수
〈관심분야〉 제어시스템보안, 스마트그리드 보안, 원자력 보안, 취약점 분석, 차세대인프라 보안, 스마트시티·공장 보안, AI기반 이상징후 탐지, 지능형 보안