정 보 보 호 학 회 지
제26권 제1호, 2016. 2

국외 원전 디지털자산 공급망 사이버보안 규제 동향

임 수 민*, 김 아 람**, 신 익 현***

요 약

기업들의 생산 공정이 세분화되면서 하나의 디지털 기기는 여러 단계의 공급망을 통해 원자력 발전소 외부에서 제작된 후 공급된 기기들과 소프트웨어의 조합으로 최종 완성품이 제작된다. 이러한 공정 과정을 거치는 다양한 나라, 회사에서 제작된 수많은 부품들과 소프트웨어의 조합은 어느 하나의 단계에서 발생한 의도되거나 의도되지 않은 결함 또는 사이버 위험을 포함한 최종제품이 될 가능성을 가지고 있으며 실제로 공급망을 위협하는 사례가 발생하기도 하였다. 이러한 결과로 공급망을 통한 사이버공격의 보안 위험 사례를 관리하는 것이 디지털화가 급격하게 진행되고 있는 원자력발전소와 같은 주요기반시설의 안전과 보안을 유지하는데 고려해야하는 중요한 요소가 되고 있다. 본 논문에서는 공급망을 통한 사이버보안 위험 사례와, 원자력발전소 디지털 자산 공급망 위험관리를 위한 해외 사례를 살펴보고자 한다.

Ⅰ. 서 론

2000년대 들어 디지털 기술의 발전에 따라 산업계에서는 디지털 기기들을 적극적으로 사용하고 있다. 원자력발전소의 경우 원자력발전소의 두뇌와 신경망에 해당하는 계측제어시스템 뿐만 아니라 보안시스템, 비상대응 시스템 등 많은 디지털 기기들을 사용하며, 원자력발전소의 운영을 디지털 기기에 의지하고 있다. 특히나 국내에서 설계하고 건설된 APR1400 노형은 세계최초로 100% 디지털화된 인간-기계연계시스템 (MMIS,Man Machine Interface System)을 도입하여 주제어실을 구성하는 대부분의 기기가 디지털장비로 구성되어 있다. 이러한 디지털기기의 도입은 이전에는 고려하지 않았던 사이버공격에 대한 대비책을 필요로 한다. 원자력발전소와 같은 국가 핵심시설을 대상으로 하는 사이버 공격은 핵물질의 노출 또는 원자력시설의 파괴, 손상으로 인한 공공의 건강, 안전 및 환경을 위태롭게 할 수 있는 심각한 결과를 야기할 수 있으므로 원자력발전소 사이버공격 대비책은 더욱 중요하다 할 수 있다. 전통적으로 원자력발전소에서 사용되는 디지털기기는 디지털기기의 안전한 운영을 위해 기기 안전성 확인 및 검증이 필수적으로 수행되어 왔다. 소프트웨어 확인 및 검증과 더불어 기존 설계에서 고려하지 않았던 사이버공격 및 위험에 대한 설계 요건을 고려하도록 사이버보안 규제지침을 개발하고 관계 법령을 개선하고 있다.

원자력 발전소를 구성하는 많은 기기들 중 특히 원자로 안전에 중요한 기기들은 안전 관련 기준이 적용되며 미국원자력사업자의 연구단체인 미국 원자력연구소(NEI)에서는 원자력발전소에 공급되는 기기들을 원자력 제조 기준 및 품질 보증 요구사항에 따라 원자로건물(Nuclear Island), 터빈(Turbine Island), 보조설비계통(Balance of Plant) 및 소외계통 (Site develpoment and consturction)의 안전관련제품 (Safety-related Products), 보조품질제품 (Supplemental Quality Products) 및 표준품질제품 (Standard Quality Products) 으로 구분하였다. 이에 본 논문에서는 원자력발전소의 공급망에서 발생할 수 있는 위험 사례를 알아보고 국내외의 공급망 요건 동향을 소개해 보고자 한다.

본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No.1305034)

* 원자력통제기술원 (s2min@kinac.re.kr)
** 원자력통제기술원 (aramkim@kinac.re.kr)
*** 원자력통제기술원 (ihshin@kinac.re.kr)

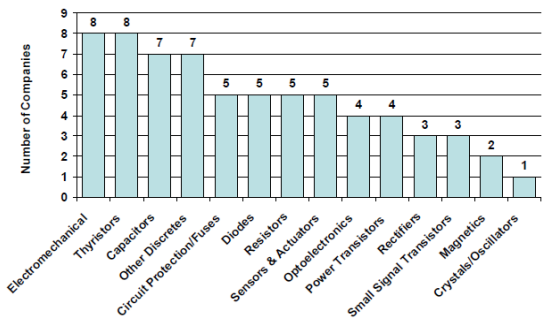
Ⅱ. 공급망 보안위험 사례

2.1. 공급망 위험 사례 분석

이번 절에서는 디지털시스템 도입 과정에서 공급망을 통해 위·변조된 제품이 공급된 사례에 대해서 알아보도록 한다.

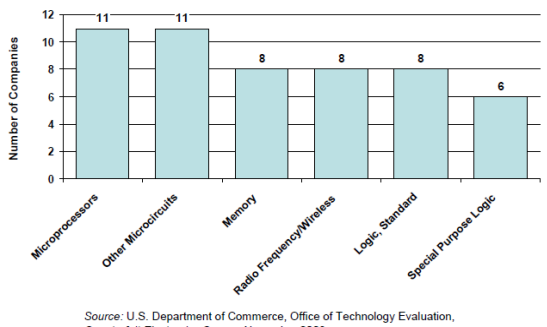
2.1.1. 미국 상무부 분석 자료

미국 해군성은 위조되거나 결함 있는 전자장비들이 국무부의 공급망을 통해 공급되어 그들의 무기시스템의 신뢰성에 영향을 끼치고 있다고 의심하여 2007년 미국 상무부 산하의 산업안전국에 국방 산업과 관련된 위조 전자기기에 대한 조사를 수행하고 보고서를 발행하였다[1]. 조사 결과 캐퍼시터, 다이오드와 같은 개별 부품에서부터 마이크로프로세서, 메모리와 같은 마이크로회로에 이르기 까지 다양한 종류의 위조되거나 감염된 부품



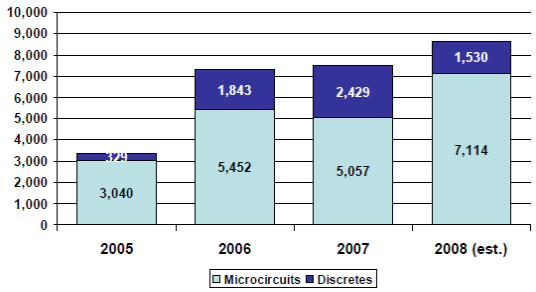
Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

〔그림1〕 위조된 것으로 확정/의심된 부품 종류 (개별부품)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

〔그림2〕 위조된 것으로 확정/의심된 부품 종류 (마이크로회로)



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

〔그림3〕 원제조사별 총 위조사건 발행 빈도

을 탑재한 전자기기가 그들의 무기시스템에 공급되어 사용되고 있는 것을 확인 할 수 있었다[그림 1~그림 3].

2.1.2. 위조 네트워크 장비 공급

2010년 5월 미국 법무부는 FBI, 이민·관세수사청, 국경보호대가 합동으로 수행한 5년간의 작전을 통해 Ehab Ashoor라는 텍사스에 거주하는 사우디 국적의 남자를 위조 네트워크 장비 판매협의로 기소하고 115대의 위조 네트워크 장비를 압수하였다[2]. Cisco Raider라는 불린 이 작전은 해커들이 위조된 네트워크 장비를 사용해 미국 정부 데이터베이스에 접근하려는 움직임이 있다는 우려에 따라 실시되었다. 조사 결과 중국에서 제작된 네트워크 장비가 Cisco의 네트워크 장비로 위장되어 국방부 납품을 시도했던 것으로 밝혀졌다. Cisco의 제품으로 위조된 네트워크 장비는 이라크에 주둔하는 미국 해병대를 비롯한 미국 정부 기관에 납품되어 사용되어 왔던 것으로 알려졌다. FBI는 위조된 이들 네트워크 장비를 통해 미국 정부 네트워크가 외부에 무방비 상태로 노출됐을 것을 우려하고 있다.

2.1.3. 위조 Xcode를 통한 모바일 앱 감염

모바일 분야에서 35.43%의 점유율[3]을 차지하는 Apple의 iOS는 AppStore를 통해 앱을 검색하여 설치할 수 있도록 하고 있다. 미국 기반의 보안회사인 Palo Alto Network는 그들의 블로그를 통해 39개의 iOS 앱이 XcodeGhost에 감염되었다고 밝혔다[4]. 애플은 자사 공식 앱스토어를 통해 이를 공식적으로 확인하였다. 공개된 목록에는 인기 메시지앱 WeChat과 중국 최대 콜택시 앱 DiDi Taxi, 인기게임 앵그리버드2등이 포함

되어 있다. 이들 앱에 감염된 악성코드는 사용자의 개인 정보를 다른 서버로 빼돌리거나 애플의 클라우드 서비스인 iColud의 비밀번호를 훔치는 기능을 가진 것으로 알려졌다. XcodeGhost는 조사결과 Apple의 앱 개발 소프트웨어인 Xcode를 조작하여 인터넷에 올려놓고, 다운로드 속도가 빠른 Xcode 버전을 받으려는 개발자들이 감염된 Xcode를 설치하고 이를 통해 앱을 개발할 때 앱에 멀웨어가 포함되게 하는 것으로 알려졌다.

2.1.4. 핵잠수함 위조 부품 공급 사건

미국 메사추세스주 메수엔(Methuen)에 위치한 Tytronix inc. and Epic International Electronics의 대표 Peter Picone은 2007년부터 2012년 까지 250만 달러어치의 위조 반도체를 다수의 고객들에게 판매한 협의로 체포되었다[5]. 사법당국에 따르면 그는 중국, 홍콩 등지에서 재생되어 위조 상표를 붙인 반도체를 구입하여 이를 National Semiconductor Inc.나 Motorola Inc.와 같은 유명 기업들에 판매한 것으로 밝혀졌다. 이들 위조 반도체 칩들은 악성 코드나 백도어를 포함하고 있을 수 있어, 이들 부품을 사용하였을 경우 시스템 불능이나, 통신 자료 유출 또는 네트워크 침입등의 사이버 공격에 악용 될 수 있다. 이들은 위조된 반도체 부품 100개를 2012년 2월 Groton에 위치한 잠수함 기지에 판매하였고, 이는 새로운 잠수함 개발에 사용 된 것으로 알려졌다. 하지만 해군은 이들 반도체를 사용 전 검사를 통해 이들이 위조되었음을 밝혀냈던 것으로 알려졌다.

Ⅲ. 원자력발전소 공급망의 위험 관리 지침

원자력발전소의 사이버보안을 위한 공급망 관련 대책 다루는 문서로는 NRC R.G. 5.71, NRC R.G. 1.152 및 NIST SP 800.53, IAEA TECDOC-919,1169등이 있다.

3.1. RG 5.71

미국 원자력규제위원회(NRC)는 원자력 시설의 디지털 컴퓨터와 통신 시스템, 네트워크를 사이버공격으로부터 보호하기 위해 규제치짐(RG 5.71)을 발간하였다[6]. RG 5.71은 미연방법 10 CFR 73.54[7]에서 명시한 사이버보안에 대한 법령을 구체화한 규제지침으로서 원자력시설에서 사용하는 안전, 보안 및 비상대응(Safety, Security & Emergency Preparedness) 기능을 수행하는 디지털자산에 대한 사이버보안 관련 지침을 제공한다. 이에 따라 미국 전역에서 운영 중인 원자력시설들은 우선 7단계에 걸쳐 RG 5.71을 준수하여 2012년까지 사이버보안계획을 제출하고, 미국 원자력규제위원회는 2015년까지 이를 검사하기로 계획하였다. 또한 7단계로 나눠진 사이버보안계획 검사 이후에는 2017년까지 전체 사이버보안계획을 검사하기로 계획되어 있다[8].

RG5.71은 적용해야하는 보안 조치를 관리적, 운영적, 기술적의 3가지로 분류하는데, 공급망 관리에 대해서는 관리적 보안 조치을 다루는 Appendix C의 C.12.2 Supply Chain Protection를 통해 제공한다. 이에 따르면 원자력발전소 공급망에 대한 규제 지침을 다음과 같이 설명하고 있다.

⊙ 사업자는 공급망을 위험 및 취약점으로부터 보호하여 정의된 필수디지털자산의 무결성을 유지하기 위한 다음의 조치를 고려한다.
- 신뢰할 수 있는 유통 경로 구축
- 기기 공급사의 검증 절차 수립
- 변조 방지 제품 요구 및 요구제품의 변조방지를 위한 봉인 조치

⊙ 사업자는 각각의 제품 구매 과정에서 제품이 규제지침 5.71에서 기술된 요구사항을 만족하는 보안 조치를 이행하는지 분석을 통해 결정 한다.

⊙ 사업자는 단일 기기공급사의 제품의 사용에서 우려되는 취약점을 완화하기 위해 이종성을 사용한다.

3.2. RG 1.152

미국 원자력규제위원회(NRC)에서 작성한 RG 1.152[9]는 원자력발전소에 사용되는 안전계통에서 사용하는 컴퓨터의 사용에 대한 기준을 제공한다. 안전계통은 방사능의 유출과 같은 사고를 막기 위해 원자로를 정지시키고 원자로를 안전정지 상태로 유지하는 기능을 수행[10]하는 시스템을 뜻한다. RG 1.152는 사이버보안을 위한 지침은 아니지만, 안전계통에서 디지털 컴퓨터를 사용하는데 있어 높은 성능 신뢰도, 설계 품질과 보안성이 확보된 개발과 운영 환경(SDOE)에 대한 지침을 제시한다. RG 1.152는 악의적 행위에 대응하기 위한 RG 5.71과는 달리 의도하지 않은 비 악의적 행위 및

접근에 대응하기 위한 지침이며, 원자력발전소의 건설을 위해서는 안전계통에 대해서 설계 단계부터 운영에 이르는 모든 생명주기 동안 공급망 행위자(Actors)인 설계사, 제작사, 운용사 등이 적용해야 하는 지침이다. RG 1.152의 생명주기별 지침은 다음과 같다.

〔표 1〕 RG 1.1.52 생명주기별 지침

	보안 개발 환경	보안 운영 환경
개념 단계	안전한 운영환경을 구축하기 위한 계통의 설계특성을 식별 생명주기에 걸쳐 운전 신뢰성을 저하시킬 수 있는 외부 연결계통의 부주의한 접근 및 원치 않는 행위에 대한 잠재적인 민감성을 평가 안전한 운영환경과 동 계통의 개발단계 중 안전한 개발환경을 유지하는 데 나타날 수 있는 잠재적 장애요소를 식별 평가 결과는 안전한 운영환경과 이를 유지하는 보호수단을 마련하기 위한 설계특성 요건을 수립하는데 사용 원격접근 불허	
요건 단계	불필요한 코드를 생성시킬 수 있는 요건을 도입하지 않아야 함	안전한 운영환경을 위한 기능적 성능요건과 계통 구성을 정의 품질, 인간공학, 데이터 정의, 소프트웨어 및 하드웨어 문서, 설치 및 인수, 운영 및 실행, 유지보수 등에 대한 요건과 계통의 외부 연계설비들에 대해 정의 설계특성 요건은 절체 계통 요건에 포함
설계 단계	원치 않거나 불필요한 코드를 생성시킬 수 있는 설계특성 혹은 기능의 도입을 막을 수 있는 수단	안전한 운영환경을 위한 설계특성은 동 계통 설계명세서 내의 특정 설계형상항목으로 구현 설계형상항목은 1) 기능에 대한 물리적이고 논리적인 접근방법, 2) 서비스의 사용, 3) 타 계통과의 데이터 통신등에 대한 통제사항을 다루어야 함 기성 소프트웨어가 포함된 설계형상항목은 동 소프트웨어가 어떻게 안전계통의 안전한 운영환경에 악영향을 미치지 않는지를 평가
구현 단계	개발된 계통에 대한 비인가 접근이나 사용, 그리고 부적절하거나 신뢰할 수 없는 작동을 유발할 수 있는 문서화되지 않는 코드 또는 기능에 대한 적절한 시험을 포함한 안전한 개발환경 관련 표준 및 절차를 개발 코드에 내장된 숨겨진 기능 및 취약성, 이러한 기능의 존재 이유, 이러한 기능이 건전성 및 신뢰성에 미치는 영향 등을 확인 기성 제품은 계통의 신뢰성을 저하시키지 않도록 하기 위해 운영체제의 특성이 안전한 운영환경을 위해 요구되는 설계특성을 손상시키지 않은음 보장	계통 설계명세서가 정확하고 완전하게 안전한 운영환경과 설계형상항목으로 전환됨을 보장
시험 단계	비인가 경로를 확인하고 계통 건전성을 확보하기 위해 계통 하드웨어 아키텍처, 외부통신장치, 구성 등을 시험	신뢰할 수 있는 계통 운전을 보장하기 위한 안전한 운영환경 설계요건 및 형상항목은 전반적인 계통 요건 및 설계형상항목에 대한 검증의 일부로 포함
운영 단계	하드웨어 및 소프트웨어 형상관리	운영중 안전한 운영환경 설계특성 유지

3.3. NIST SP 800.53 Rev. 4

NIST SP 800.53은 특정 산업기관의 장비, 또는 정보의 흐름을 검사하는 절차와 개념을 설명하기 위해 미국 상무부에서 발행한 지침이다[11].

해당 기술지침은 원자력산업을 포함한 특정 조직의 임무, 작업 환경 및 사용되는 기술에 따라 요구되는 기준에 맞춰 보안 제어, 기준 및 지도에 해당하는 포괄적이고 세부적인 보안적 조치를 제공한다. 정보 시스템에 대한 보안 통제의 적절한 선택이 필요한 조직을 지원하기 위한 보안적 제어기준선 개념을 정립하는데 도움을 주는 기술지침이다.

특히나 미국원자력위원회는 미연방법 10 CFR 73.54

에 해당되는 시스템의 포괄적인 사이버보안 접근 방식을 활용하여 사이버보안 규제지침 RG 5.71를 개발하였다.

NIST SP 800-53은 "FIPS(Federal Information Processing Standards) Publication 200, 연방 정보 및 정보 시스템에 대한 최소 보안 요구 사항"의 보안 요구사항을 충족하기 위해 연방 정부의 집행 기관을 지원하는 조직과 정보 시스템에 대한 18가지로 분류된 보안 조치의 가이드 라인을 제공한다. 18가지에 포함되는 보안조치에는 접근 제어(Access Control, AC), 미디어 보호 (Media Protection, MP), 인지 및 교육 (Awareness and Training, AT), 물리적 및 환경 보호 (Physical and Environmental Protection, PE), 계획(Planning, PL), 감사 및 회계(Audit and Accountability, AU), 형상 관리(Configuration Management, CM), 위험 평가(Risk Assessment, RA) 및 공급망 관리 내용이 포함된 시스템 및 서비스획득 (System and Service Acquisition) 등이 포함된다. 분류된 보안 조치는 다음의 표와 같으며 공급망 제어에 해당하는 내용은 SA(System and Service Acquisition)-12에 기술되어 있다.

공급망 제어 및 서비스 취급에 대한 내용은 SA-12에 해당되며 다음과 같은 지침을 제공한다.

〔표 2〕 NIST 800-53에서 제공하는 보안 조치 분류

식별자	Family
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Configuration Management
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Service Acquisition
SC	System and Communications Protection

⊙ Penetration Testing Analysis of Elements Processes and Actors
- **조치 내용** : 조직 분석, 독립적인 제3자 분석, 침투 시험 조직 구성 및 침투 테스트, 조직 역할 정의 시스템구성 요소 정의 (예, 정보시스템, 또는 정보 시스템 서비스) 공급 사슬 요소정의, 프로세스 및 주체의 독립적 인 제3자 침투 시험을 적용하도록 한다.
- **조치 방법** : 공급망 프로세스에서 사용되는 하드웨어, 소프트웨어 및 펌웨어의 개발프로세스, 물품 배송 및 처리절차, 사용자 및 물리적 보안프로그램, 출처를 유지하기 위한 조치 및 공급망의 생산 및 분배 요소와 연관된 프로그램, 프로세스 및 절차 등의 단계별 과정을 포함 하도록 한다. 공급망의 행위자(Actors)는 공급망 에서 특정 역할과 책임을 수행하는 개인을 의미한다.

⊙ Inter-organizational Agreements
- **조치 내용** : 조직은 정보시스템, 시스템구성 요소, 또는 정보 시스템 서비스에 대한 공급망에 관련된 개체와 조직 간의 계약과 절차를 확립하도록 한다.

⊙ Critical Information System Components
- **조치 내용** : 해당 조직은 조직에 중요한 정보 시스템구성 물품의 충분한 공급을 위해 사전에 정의된 보안 안전장치를 사용하도록 한다.
- **조치 방법** : 공급망의 다중의 공급자들이 사용하는 주요 부품을 식별 하고 업무 핵심 시간대에 운영을 보장할 수 있는 예비 부품을 비축하도록 한다.

⊙ Identity and Traceability
- **조치 내용** : 조직은 정보시스템의 구성 요소, 또는 정보시스템 서비스의 공급망 요소, 프로세스 및 고유 식별정보를 정의하여 관리 한다.
- **조치 방법** : 일련번호를 사용한 라벨링 혹은 RFID를 이용한 식별 태그를 사용하도록 한다.

⊙ Processes to Address Weaknesses or Deficiencies
- **조치 내용** : 조직은 독립적 혹은 조직 평가와 같은 평가 중에 발견된 공급망의 요소의 취약점이나 결함 요소를 해결하기 위한 프로세스를 확립한다.
- **조치 방법** : 침투 시험, 감사, 인증 및 검증 활동의 문서화하여 기록하도록 한다.

3.4. IAEA TECDOC 966 과 1169

IAEA TECDOC 966[12]은 원자력시설의 운영 및 유지보수를 위한 구매활동 및 공급망을 관리하기 위한 지침을 제공 하며 IAEA TECDOC 1169[13]는 IAEA 에서 제시한 안전 요건에 따라 공급망에 포함된 다중 프로세스 및 조직에서 발생 하는 위조 및 의심 품목의 사용 및 구매를 방지하기 위한 세부적인 방법 및 실제 지침을 제공한다.

IAEA TECDOC 966 및 IAEA TECDOC 1169는 기존의 공급프로세스에서 원자재 상세 조건 지정 및 주문 단계에서 필요한 내부의 구매 공정, 책임, 인터페이스가 중심이 되는 바탕정보를 제공지만 현안으로 고려되고 있는 구매 기기의 컴퓨터 보안, 노후화, 역공학 등을 다루기 위한 정보의 보충 및 추가가 필요하다.

이에 따라, IAEA는 기술보고서 NP-T-3.21을 통해 소프트웨어 및 디지털 기기 구매 및 원자력 산업계에서 확산되고 있는 표준 이하의 위조 및 사기 품목에 대한 관리를 만족하기위한 문서를 개발 중이다.

IAEA TECDOC에 따라 공급자에 대한 식별, 검증 및 감사하는 절차가 필요하며 산업계는 감사결과를 공유할 수 있도록 해당 절차를 표준화 해야 한다. 또한 식별,검증 및 감사에 수반되는 허용기준을 개발해야 한며 상용 등급의 물품을 사용하기위해 다음의 방법을 이용하여 안전성을 적용하여 구매할 수 있도록 하도록 예시를 통해 권고하고 있다.

⊙ 수용 가능한 방법을 식별할 수 있는 기술평가를 수행
⊙ 수용 가능한 방법들의 예시
- 방법 1: 특별 시험 및 검사
- 방법 2: 상용 등급 물품에 대한 공급자 설문 조사
- 방법 3: 출처 검증
- 방법 4: 허용 공급업체 및 상품 실적 기록 검토

상위 방법을 적용한 물품 구매 예시는 IAEA TECDOC 1169 Annex 3에 보다 자세하게 기술되어 있다.

Ⅳ. 결 론

전 세계적으로 사이버보안에 대한 우려가 커지면서 원자력시설의 디지털 기기 및 소프트웨어 구매에 대한 체계적인 접근이 필요하다.

특히 디지털화되고 있는 원자력발전소는 기존의 아날로그 기기에 대한 사용과 시스템 연계가 어려워지고 소프트웨어 및 디지털 산업의 짧은 수명과 빈번한 코드의 업데이트는 기존의 구매 요건과는 다른 구매 평가 방법과 요건 개발을 필요로 한다.

본 논문은 이러한 구매 프로세스 및 공급망의 변화와 더불어 기존 산업계에서도 확산되고 있는 위조 및 변조된 기기들이 공급망에 끼칠 수 있는 영향을 사례를 통해 확인하고 미국에서 운영 및 건설하는 모든 원자력발전소을 대상으로 실제 적용되는 규제 지침[6][9]들을 소개하였다.

NIST SP 500.53 또한 미국 국가 보안 프로그램 및 시스템이 준수해야할 지침으로 원자력발전소 이외의 주요기반시설 공급망의 위험관리지침을 개발하는데 사용가능할 것으로 사료된다.

이러한 사례를 기반으로 앞으로 발생 가능한 사이버 위험 대비를 준비하고 보다 체계적이고 선제적인 사이버 위험 접근을 위해서는 원자력분야 뿐만이 아닌 산업계 전반의 제어시스템 공급망 관련 사례들을 살피고 원자력발전소에 대한 사이버 위험에 대응할 수 있는 실질적인 공급망의 보안 강화가 필요하다.

참 고 문 헌

[1] Department of commerce, “Defense industrial base assessment: Counterfeit electronics”, January 2010

[2] Department of justice, http://www.justice.gov/archive/opa/pr/2008/February/08_crm_150.html

[3] NetMarketShare, “*Mobile/Tablet Operating System Market Share*”, December 2015

[4] Palo alto networks, http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/

[5] Dailymail, http://www.dailymail.co.uk/wires/ap/article-2647551/Man-pleads-guilty-counterfeit-sub-parts-case.html

[6] NRC Regulatory Guide 5.71, “*Cyber Security Programs for Nuclear Facilities*”, January 2010

[7] NRC, 10 CFR 73.54, "*Protection of digital computer and communication systems and network*", November 2009

[8] NRC, http://www.nrc.gov/public-involve/conference-symposia/ric/past/2014/docs/posters/53-nsir-current-status-of-cyber-security-implementation.pdf

[9] NRC Regulatory Guide 1.152, "*Criteria for use of computers in safety systems of nuclear power plants Rev 3*", July 2011

[10] NRC, http://www.nrc.gov/reading-rm/basic-ref/glossary/safety-related.html

[11] NIST SP 800.53, "*Security and Privacy Controls for Federal Information Systems and Organizations*", February 2014

[12] IAEA-TECDOC-919 *"Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Power Plants"*, December 1996

[13] IAEA-TECDOC-1169 *"Managing Suspect and CounterFeit Items in the Nuclear Industry"*, August 2000

〈저 자 소 개〉

사 진

임 수 민 (LIM SOO MIN)
정회원

2010년 2월 : 고려대학교 산업공학과 졸업
2012년 2월 : 고려대학교 정보보호학과 석사 졸업
2012년 2월~2015년8월 : 한국전력기술(주) 연구원
2015년8월~현재 : 원자력통제기술원 연구원
관심분야 : 정보보호정책, 제어시스템 보안, 기반시설 보안

사 진

김 아 람 (KIM ARAM)
정회원

2005년 2월 : 고려대학교 컴퓨터학과 졸업
2008년 2월 : 고려대학교 컴퓨터학과 석사 졸업
2007년 12월~2015년8월 : 한국전력기술(주) 책임연구원
2015년8월~현재 : 원자력통제기술원 선임연구원
관심분야 : 제어시스템 보안, 기반보호 정책, 사이버보안 전략

사 진

신 익 현 (SHIN ICKHYUN)
정회원

2004년 8월 : 뉴욕시립대학교 컴퓨터 사이언스학과 졸업
2014년 8월 : KAIST 정보보호대학원 석사 졸업
2005년8월~현재 : 원자력통제기술원 선임연구원
관심분야 : 제어시스템 보안, 기반보호 정책, 사이버보안 전략