정 보 보 호 학 회 지
제25권 제5호, 2015. 10

# 위험관리 측면에서의 제어시스템 보안 표준 동향

박 소 현*, 이 용 주**, 이 경 호***

요 약

최근 산업제어시스템에 대한 중요성이 강조되는 반면 사이버 보안 위협은 증가하고 있다. 전 세계적으로 제어시스템에 대한 보안 표준 개발에 집중하고 있으며 미국을 비롯한 나라에서는 산업제어시스템에 대한 표준 및 가이드라인을 공개하고 있다. 본 논문에서는 산업제어시스템에 대한 특징을 알아보고 관련 보안 표준 및 가이드라인을 분석하여 우리나라의 산업제어시스템을 보호하기 위해 나아가야 할 개선 방향에 대해 논하고자 한다.

## Ⅰ. 서 론

최근 다양한 산업분야 및 우리의 실생활에 널리 사용되고 있는 산업제어시스템은 에너지, 금융 등의 산업시설 뿐만 아니라 전력, 자원운송 등 주요정보통신 기반시설 및 빌딩, 공항 등의 시설에 적용된 시스템을 말하며, 원격에 있는 설비를 제어하기 위해 설비 정보를 수집함과 동시에 제어 명령을 설비에 전달하는 기능을 가진다. 이런 산업제어시스템은 감시 제어데이터 수집시스템이라고 불리는 SCADA(Supervisory Control and Data Acquisition), 분산제어시스템인 DCS (Distributed Control Systems), PLC(Programmable Logic Controllers) 및 센서 등 다양한 구성요소 및 유형들로 이루어져 있다.

기존의 산업제어시스템들은 제어용 컴퓨터 내장기기와 독자적인 통신프로토콜이 적용되며 외부에서 분리된 구성으로 구축 및 운영 되어 왔지만, 최근에는 ICS 업무 효율화와 다양한 분야 적용을 위해 일반 업무용 시스템 망과 연계하게 되었고 IT 및 인터넷 기술을 이용하게 되었으며, 이로 인해 ICS에도 범용 표준기술이 적용되고 개방화가 진행되고 있다.[1,11]

이와 대비해 국내·외 산업제어시스템 피해사례는 꾸준히 늘고 있는데 기존의 전력, 수자원, 원자력, 교통, 방송 등 다양한 분야에 걸쳐 발생하여 인명 피해 또는 경제적인 손실을 야기하고 있다. 대표적인 해외 제어시스템 피해 사례인 '스턱스넷 사건'은 이란의 원자력 발전소 제어시스템 내에 바이러스가 침투하여 원자력 일부 기능을 마비시킨 사건이다. 국내의 경우, 2013년 방송 전산망에 악성코드가 침투하여 시스템을 파괴하고 장애가 발생하는 등 PC 및 시스템을 포함한 약 4만9천여 대 피해를 발생시켰다.[3]

본 논문에서는 산업제어시스템 보안 표준을 위험관리 측면에서 분석하고자 하며 2장에서는 산업제어시스템과 관련된 보안 표준 ISA 62443과 NIST SP 800-82에 대해 분석하고, 3장에서는 국내 제어시스템 관련 현황을 파악한다. 4장에서는 국내·외 보안 표준 현황을 비교 분석하였으며, 결론에서는 향후 산업제어시스템을 보호하기 위해 나아가야 할 개선방향을 논하고자 한다.

## Ⅱ. 해외 보안 표준 동향

ICS는 기존 IT시스템과 다른 특성을 가지고 있기 때문에 기존에 적용한 정보보호 방법론을 그대로 적용하기가 어렵다. 즉, ICS 환경에 적합한 형태의 새로운 보안 표준이 필요하게 되었다. 특히, 미국을 중심으로 ICS에 대한 정보보호 대책을 수립하고 구현하기 위한 ICS의 위험 평가 및 관리 방법에 대한 개발이 활발하게 진행되고 있다.[10]

미국을 중심으로 한 자동화표준 단체인 ISA (International Society of Automation)는 ICS를 구성하

* 고려대학교 정보보호대학원 (annapark@korea.ac.kr)
** 고려대학교 정보보호대학원 (sky4uni@korea.ac.kr)
*** 고려대학교 정보보호대학원 (kevinlee@korea.ac.kr, 교신저자)

는 제품 및 시스템의 보안요구사항을 정의하고 표준화하고 있다. 또한 ICS의 위협과 취약성을 분석해 위험도를 낮추고 안정성을 확보하기 위한 인증 제도를 개발하고 있다. 이에 해당되는 문서가 ISA 62443 시리즈이다.[1,13]미국의 또 다른 기관인 NIST(National Institute of Standards and Technology)는 국립표준기술연구소로, 표준 및 기술을 진보시키는 것이 공식적인 임무이다. ICS에 대한 정보보호 평가과정이나 위험 통제관리 등에 대한 자세한 가이드라인을 각 문서에 제시하고 공개하고 있다.[15]

본 장에서는 ICS 관련 보안 표준 및 가이드라인의 위험관리 방법에 대해 알아보고 비교해보고자 한다.

### 2.1. ISA 62443

IT시스템과 달리 ICS의 보안목표는 제어 시스템의 가용성, 현장설비 및 장치 보호, 실시간 대응 등이다. IT는 물리적 자산보다는 정보자산 보호에 중점을 두고 있으나 ICS는 현장 설비 등 물리적 자산 보호를 포함한 정보보호에 중점을 두고 있다.[1] IT와 ICS의 차이 중 하나는 자산에 대해 기밀성・무결성・가용성의 중요도 우선순위를 다르게 보는데 있다. ISA 62443-1-1에 따르면 IT는 기밀성-무결성-가용성 순으로 중요도를 책정하고 이와 대조로 ICS는 실시간성을 보장해야하기 때문에 가용성-무결성-기밀성 순으로 중요도를 책정한다. 하지만 시스템의 특정 동작이나 환경에 있어 CIA 우선순위는 달라질 수 있다.[4] ICS는 산업 내・외부간 네트워크로 상호연결이 되어있고 상업용 운영체제나 보안되지 않은 프로토콜 등 보안성이 고려되지 않은 기존 구성을 사용하기 때문에 더 큰 위협에 노출되어 있다. 무엇보다도 내부 인식부족 및 관리미흡으로 인한 문제가 야기될 수 있다. 이러한 ICS와 IT시스템과의 차이점 및 위협요소는 보안목적으로 이어져 이를 만족시키기 위한 정보보호 대책 및 보안요구사항 정의를 ICS 환경에 맞게 변경할 필요성이 생겼다. 이에 ISA는 ICS 정보보호를 위한 표준인 ISA 62443을 개발하였다.

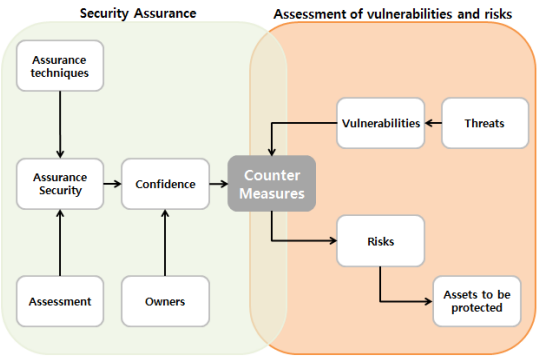
ISA-62443은 크게 4개의 영역으로 구성되어 있으며 각 영역은 세부 주제의 문서로 ICS 운영과정에 대한 규격을 정의하고 있다. 좀더 상세히 살펴보면, ISA 62443-1은 ISA 62443에 대한 요약과 용어 정의와 같이 전체적인 문서에 대한 일반적인 내용이다. ISA 62443-2 는 조직 및 정책적인 측면에 관한 내용으로


〔그림 1〕 ISA 62443 시리즈 구성

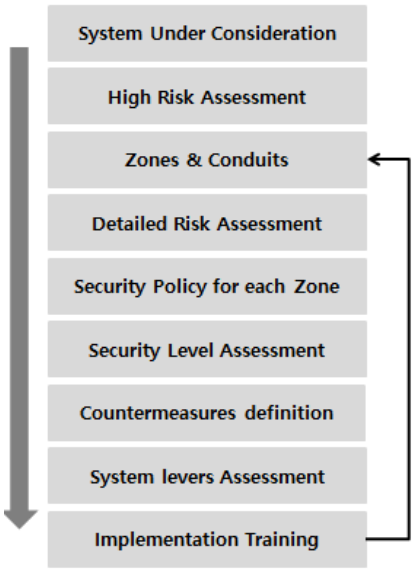
ICS 보안구성, 운영, 관리, 인증에 대해 각 세부주제로 구분되어 있다. ISA 62443-3은 ICS 시스템에 관련된 문서로 보안기술 정의와 ICS에 대한 인증 및 보안요구사항에 따른 등급에 대해 기술하고 있다. ISA 62443-4는 ICS 구성요소, 시스템 제공자들이 제품 또는 시스템 개발생명주기에서 준수해야 할 사항에 대해 정의하고 있다.

ISA 62443의 접근방식은 [그림 3]과 같이 보안 보증과 취약성 및 위험 측정을 동시에 수행하는 방식을 취하고 있다. 보안 보증은 의도적인 보안 문제뿐만 아니라 환경적인 측면 등 일어날 수 있는 모든 확률적인 사건을 통제하고, 취약성 및 위험 측정은 누군가에 의해 의도되어진 보안 문제를 다루기 때문에 ISA 62443은 상호접근 방식으로 내외부의 모든 위험을 통제할 수 있다.[7]

ISA 62443의 주요 원리는 Defense in depth로 공격자가 ICS의 특정 부분까지 접근할 수 없게 Security Zone으로 분할하여 하나의 시스템에 계층별 보안을 제공하거나 외부 공격속도를 늦추는 방법이다. 이 원리를 적용하는 과정에서 Security Zone과 Consuit라는 용어




〔그림 2〕 Context 모델




〔그림 3〕 ISA 62443 주요단계

〔표 1〕 NIST SP 800-82 주요 개정내용

| 구분 | 주요 내용 |
|---|---|
| 1 | ICS 위협 및 취약점 업데이트 |
| 2 | ICS 위험 관리, 구조 업데이트 |
| 3 | ICS 보안의 현재 활동에 대한 업데이트 |
| 4 | ICS 보안 능력 및 도구에 대한 업데이트 |
| 5 | 다른 ICS 보안 표준 및 가이드라인 추가 정렬 |
| 6 | overlay 도입 포함, NIST SP 800-53 개정 4판 보안 통제에 대한 새로운 안내 |
| 7 | ICS에 대한 낮은, 적정한, 높은 영향에 대한 보안 통제 기준을 제공하는 NIST SP 800-53 개정 4판에 대한 ICS overlay |

가 정의되는데, Security Zone은 일반적인 보안 요구사항을 분할하여 자산을 묶은 영역을 말한다. Consuit는 Zone이라는 단위를 연결해주는 역할을 한다. Consuit의 보안목적은 Zone 간의 접근통제, 네트워크 트래픽 무결성 보장이다.

주요 원리인 Defense in depth에 따라 작은 단위의 Zone에서 위험을 측정하고, Zone과 Zone이 결합되었을 때의 위험을 측정한다. 이를 통해 작은 범위에서 큰 범위로 위험을 측정하고 보안등급을 산정한다. 이러한 위험 측정은 Zone이 결합되어 완전한 하나의 시스템을 이룰 때까지 반복된다. 이는 각 항목에 대한 보안뿐만 아니라 결합되었을 때의 보안을 고려한다는 점이 기존 IT시스템 위험평가를 하는 방식과 조금 다르다. ISA 62443은 이러한 점층적인 방식의 위험평가를 통해 ICS의 보안 취약점 노출을 줄이게 된다. 그리고 각 위험 평가는 위협과 취약성, 예상되는 결과의 가능성을 고려해 산정된다.[4-6]

## 2.2. NIST SP 800-82

NIST SP 800-82는 SCADA 및 ICS 보안에 대한 공식적인 안내서로 NIST에서 2006년에 최초 발행하였으며, 이후 2015년 5월에 최신 버전으로 개정되었다. 최신 버전에서의 주요 개정내용은 다음과 같다.

ICS는 다양한 종류의 잠재적 위험과 피해가 다양한 수준으로 존재하기 때문에, NIST SP 800-82에서는 다양한 대응 방법과 ICS를 보호하기 위한 기술들의 목록을 제공한다.

이 문서는 주로 공통 시스템 토폴로지, 위협 및 취약성과 대응책을 제시하였으며, 관리적・운영적・기술적 보안제어 등 포괄적으로 보안 측면을 다루고 있다. 하지만 이 문서는 특정 시스템을 보호하기 위한 체크리스트로 그대로 사용할 수 없다. 자신의 시스템에 위험 기반 평가를 수행하고 특정 보안, 비즈니스 및 운영 요구 사항을 충족하기 위해 권장 지침 및 솔루션을 조정해야 한다.

〔표 2〕 ICS 발생가능 위협

| 순서 | ICS에 발생가능한 위협 |
|---|---|
| 1 | ICS에 장애가 되는 네트워크를 통한 정보의 차단과 지연 |
| 2 | 정상적 업무환경에 지장을 주거나 인명피해를 발생시킬 수 있는 지시 또는 알람 임계값의 무단변경 |
| 3 | 시스템 관리자로부터 위장하거나, 부적절한 행동을 하게 유도하는 정보를 전송 |
| 4 | ICS 소프트웨어의 설정 값이 변경되거나 악영향을 끼칠 수 있는 악성코드에 감염 |
| 5 | 인간의 생명을 위험에 빠뜨릴 수 있는 안전 시스템의 작동에 간섭 |

〔표 3〕 ICS 대응방안

| 순서 | ICS 보안위협에 대한 대응방안 |
|---|---|
| 1 | ICS 네트워크의 동작에 대한 논리적 접근을 제한 |
| 2 | ICS 네트워크 및 장치에 대한 물리적 접근 제한 |
| 3 | ICS 구성 요소에 대한 해킹으로부터 보안적용 |
| 4 | 정상적인 동작이 어려운 환경에서도 기능 유지 |
| 5 | 사고 이후 신속한 시스템 복원 |

ICS에서 발생가능 한 위협의 종류와 대응방안은 다음과 같다.

ICS의 보안 문제를 해결하기 위해, 사이버 보안 팀의 위험의 평가 및 부서 간 다양한 영역의 지식과 경험을 공유는 필수적이다. 사이버 보안 팀은 조직의 IT 직원의 구성원, 제어 엔지니어, 제어 시스템 운영자, 네트워크 및 시스템 보안 전문가, 관리 직원의 멤버, 그리고 최소한의 물리적 보안 부서의 구성원으로 구성해야 한다. 연속성과 완성도를 위해, 사이버 보안 팀은 제어 시스템 공급 업체 및 시스템 통합 업체와 상의해야 한다. 사이버 보안 팀은 직접 현장을 관리하거나 ICS의 사이버 보안에 대한 완전한 책임과 사후관리가 가능한 회사의 CIO 및 CSO에 직접 보고해야 한다. ICS에 대한 효과적인 사이버 보안 프로그램은 '심층방어(Defense in depth)'로 알려진 전략을 적용한다. 심층방어는 어느 하나의 고장의 영향을 최소화하는 레이어로 이루어진 보안 메커니즘이다.

일반적인 ICS에서 심층방어 전략은 다음을 포함한다.

- 아키텍처를 설계 할 때 ICS의 라이프 사이클 전반에 걸쳐 보안을 적용
- 중요한 통신이 안전하고 안정적인 층에서 발생하도록 여러 층을 갖는 ICS 네트워크 토폴로지를 구현
- 중요한 구성에 대해서는 이중화하거나 이중화된 네트워크로 구성
- 중요 시스템의 경우, 치명적인 연쇄 사고을 방지할 수 있도록 설계
- ICS 동작에 영향을 주지 않도록 사용하지 않은 포트와 ICS 장치를 비활성화
- ICS 네트워크 및 장치에 대한 물리적 접근 제한
- 작업을 수행하는 데 필요한 ICS 사용자 권한을 개인별로 제한
- 침입탐지 소프트웨어 등 기술적으로 ICS에서 예방, 방지 탐지 및 노출을 완화하고, 악성소프트웨어의 전파를 차단할 수 있는 보안 통제을 적용
- ICS 데이터 저장 및 통신에 적절한 암호화 및 암호해시와 같은 보안기술을 적용
- ICS의 중요한 영역에 추적 및 모니터링 감사단계를 적용

NIST는 보안 컨트롤에 대한 구체적인 지침을 개발하기 위해 공공 및 민간 부문의 ICS 보안 프로젝트를 만들었다. 그 지침은 NIST SP800-53(연방 정보 시스템과 ICS 조직에 대한 권장 보안 컨트롤)이다. NIST SP 800-53의 부록 F: Security Control Catalog 에 있는 대부분의 통제들이 ICS에 적용 할 수 있도록 되어 있지만, ICS 특성에 따라 재해석하는 등 유연성을 필요로 한다.[8,9]

## Ⅲ. 국내 제어시스템 관련 현황

국내 제어시스템 보안 관련 현황은 정보통신기반보호법에 근거하여 주요정보통신기반시설을 지정 및 관리하고 있으며 취약점 분석·평가 기준을 제시하고 있다. 또한 국가사이버안전센터에서 실시하는 정보보안 관리실태 평가를 통해 정부·공공기관에 대해서 보안진단을 하고 진단결과는 정보보호정책 및 계획 수립의 기초자료로 활용하고 있다.

### 3.1. 주요정보통신기반시설 취약점 분석、평가

2001년 제정된 정보통신기반보호법에서는 "정보통신기반시설이란 국가안전보장·국방·금융·운송·에너지 등의 업무와 관련된 전자적 제어관리시스템 및 정보통신망을 말한다" 라고 규정한다. 동법에서는 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을「주요정보통신기반시설」로 지정 할 수 있도록 규정하였다. 주요정보통신기반시설로 지정되기 위한 요건으로는 정보통신기반시설을 이용한 업무의 국가사회적 중요성, 정보통신기반시설에 대한 의존도, 다른 정보통신기반시설과의 상호연계성, 침해 사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위, 침해사고의 발생가능

성 또는 그 복구의용이성 등을 고려하여 지정하고 있다. 2014년 12월 기준으로 정보통신 및 미디어, 금융, 교통, 의료 등 17개 관계중앙행정기관과 188개의 관리기관 그리고 292개의 주요정보통신기반시설이 지정, 관리되고 있다.[3]

정보통신기반보호법 제 9조에 따라 주요정보통신기반시설 취약점 분석·평가 기준을 준수해야하는데, 여기서 취약점 분석·평가는 사이버 위협에 대한 주요 정보통신기반시설의 취약점을 종합적으로 분석 및 평가하는 일련의 과정을 말한다. 수행주체는 주요정보통신기반시설의 관리기관이 직접 수행하거나 외부 전문기관에 위탁으로 이루어진다. 취약점 분석·평가의 범위는 정보시스템 자산에 관여하는 물리적·관리적·기술적 분야를 포함하고 연계된 타 시스템이 있을 경우 연계 시스템이 기반시설에 미치는 영향을 포함한다. 분석결과에 따라 위험등급 상·중·하 3단계로 표시하고 기밀성·무결성·가용성을 고려하여 정의한 기준에 맞춰 개선방향을 수립한다. 즉, 취약점 분석·평가 기본 체크리스트가 존재하여 각 기관은 체크리스트의 기준에 따라 상중하로 평가하고 평가결과에 따라 정량적인 종합점수가 산출되는 방식을 사용하고 있다.[12]

### 3.2. 정보보안 관리실태 평가

각급기관이 체계적으로 정보보안 업무를 수행토록 지원하고 국가·공공기관 종사자의 보안의식을 함양함으로써 각급 기관 정보보안 수준 제고 및 국가 사이버 안전 확보를 목적으로 하는 정보보안 관리실태 평가가 있다. 정보보안 관리실태 평가는 2004년 정보보안 관리수준 평가제도가 도입되고, 2006년 시범평가가 실시된 이후 매년 진행되고 있다. 정보보안 관리실태 평가는 기관의 자체평가와 국가사이버안전센터의 현장실사로 구성되며, 평가 단계는 다음과 같다.

정보보안 관리실태 평가는 정보보안 정책, 정보자산 보안관리, 인적 보안, 사이버위기 관리, 전자정보 보안, 정보시스템 보안 등 다섯 가지 분야를 중점으로 진행되며, 최종 합산된 평가점수에 따라 우수(90점 이상), 양호(80점 이상), 보통(70점 이상), 미흡(60점 이상), 불량(60점 미만)의 5단계로 각급기관의 정보보안 관리수준에 대한 평가결과를 산출한다.[14]

〔표 4〕 정보보안 관리실태 평가 단계

| 순서 | 평가 단계 | 주체 |
|---|---|---|
| 1 | 기관별 자체평가 | 각급기관 |
| 2 | 현장실사 | 국가사이버안전센터 |
| 3 | 결과분석 및 점수산출 | 국가사이버안전센터 |
| 4 | 평가결과 심의·의결 | 평가위원회 |
| 5 | 최종 평가결과 통보 | 국가사이버안전센터 |

## Ⅳ. 국내、외 보안 표준 분석

해외 산업제어시스템 보안 표준 ISA 62443-2-1과 NIST SP 800-82, 국내에 해당하는 주요정보통신기반시설 취약점 분석·평가와 정보보안 관리실태 평가를 살펴보았다. 아래에서는 NIST SP 800-82를 중심으로 점검 항목이, ISA 62443을 중심으로 접근 방법을 분석하고자 한다.

### 4.1. 점검 항목

국내에서 시행 중인 주요정보통신기반시설 취약점 분석·평가 기준에 따르면 평가의 범위를 물리적·관리적·기술적 분야로 설정하고 있다. 한편, [표 5]에 나타나듯이 기술적 분야 점검항목 313개 중 산업제어시스템에 적용 가능한 항목은 약 7%에 해당하는 22개로 나타났다. 또한 주요정보통신기반시설 취약점 분석·평가는 산업제어시스템을 포함한 정보시스템을 평가의 대상으로 설정하고 있다. 점검 항목이 산업제어시스템에 특화되어 있지 않음에도 불구하고 전체 항목 수가 162개인 반면, [표 6]을 참고하면 산업제어시스템에 특화된 NIST SP 800-82의 전체 항목 수는 이보다 많은 193개로 나타났다. 즉, 산업제어시스템을 보호하기 위해서는 산업제어시스템에 특화된 보다 세부적인 평가가 이루어질 수 있도록 점검 항목의 개선이 필요하다.

〔표 5〕 주요정보통신기반시설 취약점 분석·평가(ICS중점)

| 분야 | | 항목 |
|---|---|---|
| 관리적 분야 (114개) | 정보보호 정책 | 8 |

| | | |
|---|---|---|
| | 정보보호 조직 | 4 |
| | 인적 보안 | 6 |
| | 외부자 보안 | 5 |
| | 자산분류 | 5 |
| | 매체 관리 | 5 |
| | 교육 및 훈련 | 5 |
| | 접근 통제 | 21 |
| | 운영 관리 | 33 |
| | 업무 연속성 | 4 |
| | 사고 대응 | 13 |
| | 감사 | 5 |
| 물리적 분야 (26개) | 접근 통제 | 3 |
| | 감시 통제 | 8 |
| | 전력 보호 | 4 |
| | 환경 통제 | 11 |
| 기술적 분야 (22개) | 계정관리 | 3 |
| | 패치관리 | 1 |
| | 접근 통제 | 5 |
| | 보안관리 | 13 |
| 계 | | 162 |

〔표 6〕 NIST 800-82 평가

| 분야 | 항목 |
|---|---|
| 접근 통제 | 18 |
| 교육 및 훈련 | 4 |
| 감사 및 책임 | 12 |
| 보안 평가 및 권한 부여 | 8 |
| 구성 관리 | 11 |
| 비상 계획 | 10 |
| 식별 및 인증 | 8 |
| 사고 대응 | 8 |
| 유지 | 6 |
| 미디어 보호 | 7 |
| 물리 및 환경 보호 | 17 |
| 계획 | 5 |
| 인적 보안 | 8 |
| 위험 평가 | 4 |
| 시스템 및 서비스 획득 | 13 |
| 시스템 및 통신 보호 | 22 |
| 시스템 및 정보 무결성 | 16 |
| 프로그램 관리 | 16 |
| 계 | 193 |

### 4.2. 접근 방법

국내 정보보안 관리실태 평가의 경우 취약점 분석 및 평가 계획 수립, 취약점 분석 및 평가 대상 선별, 취약점 분석 수행, 취약점 평가 수행 4단계로 구성된 절차를 수행한다. 2단계의 취약점 분석 및 평가 대상 선별에서 기반시설의 IT, 산업제어시스템 등 자산을 식별하고 유형을 그룹화하여 목록을 작성한다. 작성된 자산에 대해 취약점 분석을 실시하고 관리적·물리적·기술적 취약점 분석 결과에 따라 진단결과값을 산출한다. 산출한 진단결과값을 합산하여 해당자산의 전체 취약점 점수를 도출하고 일정 점수 이상의 결과에 도달해야하는 Security관점으로 이행한다.

반면 ISA 62443에서는 Zone 이라는 새로운 단위가 있는데, 공통된 보안요구사항을 공유하는 물리적·논리적 자산의 집합을 말한다. Zone 단위로 위험평가를 진행하고 보안에 대해 Security Level이라는 보안등급을 책정한다. Security Level은 특정 기능을 가진 장치나 시스템이 Zone 내부로의 사용을 결정하기 위한 기준을 제시한다. 이 Security Level은 Zone의 환경이 바뀌거나 새로운 장치가 추가되었을 때마다 Zone에서 요구하는 보안 조건을 충족시키는지에 대한 여부를 판단한다. Security Level 등급은 1에서 4단계로 나뉘며 높은 등급에 따라 더 많은 보안 조건을 요구한다.

즉 ISA 62443에서의 Security Level은 자산이 아닌 Zone이라는 단위에 대해 Assurance와 Risk

Assessment 관점을 적용하고 있다. 이는 국내 정보보안 관리실태 평가에서 체크리스트 기반의 자산별 취약점 분석 및 평가를 진행하는 Security관점과 차이를 나타내는 것으로 분석된다.

## Ⅴ. 결 론

국내 에너지 산업의 경우, 정기적으로 점검 및 평가를 하지만 2014년 '양호'평가를 받은 기관에서 내부자료가 유출되는 등 문제가 발생되었다.

본 논문에서는 산업제어시스템에 대하여 미국의 보안 가이드라인인 NIST SP 800-82와 표준인 ISA 62443을 알아보고 위험관리 방법에 대해 비교해 보았다. NIST SP 800-82, 53은 통제항목이 세부적으로 기술되어 있었고, ISA 62443은 최소한의 단위에서 하나의 시스템까지 점층적인 위험관리를 적용하고 있었다. 특히 통제항목에서 NIST SP 800-82의 항목들이 국내 주요정보통신기반시설 취약점 분석·평가 기준보다 제어시스템에 대해 더 특화되고 다양하다는 점을 알 수 있었다. ISA 62443에서는 궁극적으로 Security Level을 통한 Assurance 목적을 취하고 있기 때문에 의도된 공격뿐만 아니라 물리적이고 환경적인 피해나 손실까지 고려한 접근방식을 적용하고 있었다. 이러한 표준과 가이드라인은 상호보완적으로 발전해나가는 방향을 가진다.

따라서 향후 국내의 ICS의 보안위협에 대응하기 위해서는 최소한 NIST SP 800-82 통제항목을 포함하고 ISA 62443의 Security Level의 Assurance 접근방향으로의 위험관리가 필요할 것으로 판단된다.

## 참 고 문 헌


[1] 손경호, "산업제어시스템 보안성 평가·인증 동향 분석", 정보보호학회지, 24(5), pp. 15-25, 2014

[2] 차영태, 조병훈, 나중찬, KEIT PD Issue Report, 한국산업기술평가관리원, 13(6), June 2013.

[3] 국가정보원, 정보보호백서, 국가정보원, pp. 106-115, 2015.

[4] ISA, ANSI/ISA‐62443-1-1 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models, ISA, 2007

[5] ISA, ANSI/ISA‐62443-2-1 Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program, ISA, 2009

[6] ISA, ANSI/ISA‐62443-3-3 Security for industrial automation and control Systems Part 3-3: System security requirements and security levels, ISA, 2013

[7] Jean-Pierre HAUET, ISA99/IEC 62443: a solution to cyber-security issues, pp. 13-34, 2012

[8] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security, NIST, 2015

[9] NIST, NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, NIST, 2013

[10] 이철원, "국가 기반시설 사이버 보안기술 동향", 한국위기관리논지, 4(1), pp. 1-12, 2008

[11] 전용희, "산업제어시스템 정보보호: 개요", 정보보호학회지, 19(5), pp. 52-59, 2009

[12] 미래창조과학부, 주요정보통신기반시설 취약점 분석평가 기준, 미래창조과학부고시 제2013-37호, 2013

[13] 김인중, 정윤정, 고재영, 원동호, "중요핵심기반시설에 대한 보안 관리 연구", 한국통신학회논문지, 30(8C), 2005

[14] 국가사이버안전센터, "정보보안 관리실태 평가 소개", 한국정보보호학회지, 23(5), pp. 9-11, 2013

[15] https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology

[16] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST, 2014

## 〈저 자 소 개〉


**박 소 현 (Park So Hyeon)**
정회원

2015년 2월 : 광운대학교 소프트웨어학과 졸업
2015년 3월 ~ 현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 정보보호정책, 개인정보보호

**이 용 주 (Lee Yong Ju)**
정회원

2012년 2월 : 한국항공대학교 전자및 항공전자공학과 졸업
2015년 3월~현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 위험관리, 정보보호컨설팅, 개인정보보호

**이 경 호 (Lee Kyung Ho)**
정회원

1989년 8월 : 서강대학교 수학과 학사 졸업
1997년 8월 : 서강대학교 정보통신대학원 석사 졸업
2009년 8월 : 고려대학교 정보보호대학원 박사 졸업
1994년 2월~2012년 : 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재 : 고려대학교 정보보호대학원 부교수
관심분야 : 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책