Journal of The Korea Institute of Information Security & Cryptology
VOL.26, NO.5, Oct. 2016
ISSN 1598-3986(Print)
ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1335

스마트공장 정보보호 인식교육을 위한 커리큘럼 개발*

전 인 석,[1†] 이 병 권,[2] 김 동 원,[1] 최 진 영[1‡]
[1]고려대학교 정보보호대학원, [2]전남대학교

Curriculum Development for Smart Factory Information Security Awareness Training*

In-seok Jeon,[1†] Byung-gueon Yi,[2] Dong-won Kim,[1] Jin-yung Choi[1‡]
[1]Graduate School of Information Security, Korea University
[2]Chonnam University

요 약

세계적으로 제조업분야의 스마트공장은 매우 빠르게 확산이 되고 있다. 국내에서는 KOSF(Korea Smart Factory Foundation)을 중심으로 스마트공장을 추진하고 있다. 제조업을 중심으로 발전한 스마트공장은 정보보호에 대한 인식이나 투자가 매우 부족한 상황이고, 그 여력이 충분하지 않다. 그로 인해 스마트공장이 직면하게 되는 새로운 유형의 위협에 효과적으로 대응할 수 없고, 보안사고가 발생할 수 있다. 새로운 위협을 식별하고 정보보호현황을 조사해본 결과, 스마트공장이 안전하게 확산되기 위해 가장 효과적이고 효율적인 방법은 추가적인 예산투입 없이 정보보호 인식을 교육하는 것이다. 따라서 본 연구에서는 NCS(National Competency Standards)를 기반으로 국제표준, 산업의 요구사항, 교육기관의 커리큘럼을 참조하여 스마트공장 정보보호 인식교육 커리큘럼을 개발하였다. 이를 전문가 집단을 통한 타당성 검증을 진행하였으며, 이를 통하여 보다 안전하게 스마트공장이 확산될 수 있도록 하였다.

ABSTRACT

Smart factory of Manufacturing sector is rapidly spreading, globally. In case of domestic, it is on going based on KOSF. It is neither lack of invest nor security of information due to it has been spread from manufacturing sector. Hence, that's very difficult to efficiency prevent from new type of intimidation and security accident happened sometimes from this situation. According to research information security condition with recognized new menace, there is a most efficient way is provide education of information security without any extra budget to safely spread smart factory. Thus, this study of research has developed security awareness training curriculum from international standard, requirement of the industry, and curriculum of educational institution based on NCS (National Competency Standard). It is be very helpful to spread smart factory safely due to expert group has been test of validity.

Keywords: smart factory security, smart manufacture security

I. 서 론

스마트공장은 제품의 기획,설계.생산,유통,판매 등 전 생산 과정에 ICT 기술을 접목하여 최소비용과 시간으로 고객맞춤형 제품을 생산하는 진화된 형태의 공장의 의미한다.[3] 한국제조업의 패러다임은 경공업 중심의 수입대체형 전략(제조업혁신 1.0)으로 시작하여 조립,장치사업 추격형 전략(제조업 혁신 2.0)

Received(09. 12. 2016), Accepted(09. 26. 2016)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2016-H8501161012000100 2)
† 주저자, wilcois@ahnlab.com
‡ 교신저자, choi@formal.korea.ac.kr(Corresponding author)

을 지나 융합 신산업 선도형 전략(제조업혁신 3.0)으로 나아가고 있다.〔4〕 이는 ICT기술의 발전으로 공장 설비간의 통신이 가능해지고 고비용 생산구조에서 효율적인 생산구조로 전환을 위하여 전자화(Electrification)·자동화(Automation)·디지털화(Digitalization)가 진행되고 있다. 국외는 산업계 중심의 Industry 4.0을 독일에서 발족하였으며, 미국은 셰일가스와 IT·SW를 바탕으로 한 Reshoring 및 첨단제조기술을 지원하고 있다.〔5〕 제조업과 ICT기술의 융합은 매우 긍정적이지만, 모든 산업에서 네트워크와 연결이 되면서 그전에 없었던 새로운 위협으로 인한 위험이 증가하게 된다. 따라서 전통적인 공장에서는 고려하지 않았던 보안적 요소가 스마트공장에서 대응을 하지 않았을 경우 정보유출이나 비정상동작으로 인한 피해가 발생할 수 있다. 하지만 제조업의 특성상 최소의 단가로 고품질의 제품을 생산하는 것이 공장의 경쟁력이기 때문에 보안솔루션을 도입하거나 보안예산을 투입하기가 쉽지 않다. 실제로 매출액에 비례하여 정보보호예산을 투자하고 있고 전통적인 공장에서 스마트공장으로 전환한 공장의 경우는 정보보호 예산에 대한 투자가 전무한 경우도 있다. 또한 제조업 중심으로 성장한 공장의 경우는 대표가 정보보호의 필요성이나 위험성에 대하여 인지하지 못하는 경우가 많아, 정보보호에 대한 투자를 전혀 하지 않다가 보안사고로 이어질 수 있다. 스마트공장이 안전하게 확산되어 정착되기 위해서는 적은 비용으로 효율적이고 효과적으로 정보보호 수준을 향상시킬 수 있는 방안이 필요한 것이다.

II. 국내 스마트공장 현황

2.1 스마트공장의 정보보호 관련 동향

스마트공장 추진단에 의해 지원을 한 1,240EA 공장에 보급된 솔루션은 Fig. 1과 같다. 대부분의 공장에서 MES(Manufacturing Execution System)를 도입하고 있다. MES, ERP등의 솔루션은 삼성SDS, LG CNS, SK C&C와 같은 국내 SI업체들의 활동으로 글로벌 기업과의 경쟁에서 다른 요소기술에 비해 많이 뒤처지지 않는 수준이지만, GE, Rockwell, SIEMENS, Applied Materials등의 해외 기업들이 다양한 산업 분야에 강세를 보이고 있다.〔15〕

제조실행시스템 MES는 제조기업 생산성의 가용성

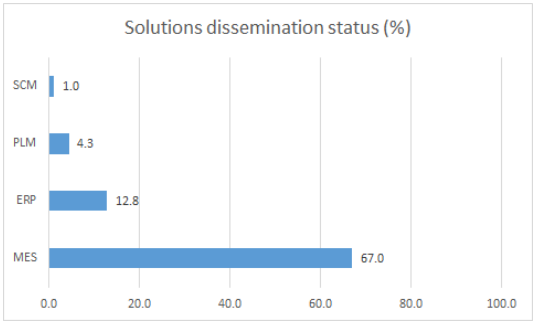

Fig. 1. Solutions dissemination status〔2〕

및 효율성을 향상시키기 위하여 생산라인의 프로세스(생산계획, 작업지시, 자재소요, 생산추적, 설비관리, 생산성과분석, 등)를 자동으로 분석하고 온라인으로 공유하는 시스템이다.〔1〕

2.1.1 IEC 61508 - Functional Safety requirement

IEC 61508 Functional Safety requirement는 전기·전자·프로그램 가능한 전자 안전관리 시스템(E/E/PE)의 기능안전(Functional Safety) 표준이며, 모든 종류의 산업에 적용 가능한 기본적인 기능 안전 표준이 될 의도로 작성되었다.

IEC 61508 Functional Safety requirement는 시스템, 하드웨어 또는 소프트웨어의 잘못된 명세, 안전 요구사항 명세에서 누락, 하드웨어 우발 고장 메커니즘, 소프트웨어 오류, 공통 원인 고장, 인적 오류, 환경적인 영향, 공급 시스템 전압 불안정 등 위험 측정 오류에 대한 기능 안전을 확보하기 위한 방법을 제공하고 있다.

2.1.2 IEC 62443 - Security requirement

IEC 62443, "Industrial communication networks - Network and system security"는 일반적인 산업의 네트워크 및 시스템을 대상으로 보안시스템의 개념, 운영, 시스템 통합, 컴포넌트 벤더 등에 대한 내용을 기술하고 있다.

데이터의 기밀성과 무결성을 강조하는 기존의 사이버 보안과는 다르게 IEC 62443는 기능안전과 같이 가용성과 안전성을 최우선시 하며, 공격 대상에 따라 작은 취약점 노출로도 전 시스템이 치명적인 피해를 받을 수 있기 때문에 전체적인 관점에서 시스템을 보호해야 한다.

2.1.3 IEC SG8

IEC의 SMB(표준화 관리 이사회)는 전세계 상호 호환성이 확보된 스마트공장 기술의 발전을 위한 국제표준화 전략을 마련하기 위해 2014년 6월에 SG(전략그룹) 8 : 인더스트리 4.0 - Smart Manufacturing을 구성하였다. IEC 내부의 TC(기술위원회) 구성을 위하여 2014년 11월부터 2015년 3월까지 미국, 독일, 스웨덴, 일본, 중국, 프랑스, 영국, 브라질, 한국 등의 9개국이 참여하여 3차례 회의를 진행하였으며, 현재 10개국 총 19명으로 구성되어 있고, 독일의 SIEMENS와 미국의 Rockwell이 공동의장으로 활동하고 있다.

2.1.4 IEEE P2413

2014년 6월에 P2413 프로젝트를 공식적으로 개시함으로써 IoT 아키텍처 구축을 통해 더욱 다양한 산업과 기술 영역으로의 확장하였다. Cisco Systems, Huawei, GE, Oracle, Qualcomm, ZigBee Alliance 등 23사의 개발업체 및 조직 참여중 이며, 홈 자동화 및 산업 시스템 등 향후 IoT가 적용될 것으로 기대되는 부문의 커넥티드 기기와 어플리케이션들 간의 상호운용성을 담보하는 프레임워크를 구성하는 것이 목표이다.

2.2 스마트공장 위협

스마트공장은 과거 오프라인으로 관리되던 공장 프로세스가 네트워크에 연결됨으로써 과거에 비해 많은 긍정적인 효과가 있지만, 보안적으로 위협에 노출될 수 있기 때문에 보호되고 관리 되어야 한다. 일반적인 IT환경에서의 위협요소와 스마트공장의 산업제어시스템은 많은 요소에서 차이가 있다. 특히 위험관리의 요구사항 중 IT환경에서는 기밀성, 무결성, 가용성이 중요하고 사업의 중단이 발생하지 않는 범위에서 일시적 정지는 감수할 수 있지만, 산업제어시스템에서는 인간의 안전이 제일 중요하며, 에러에 대한 내성은 본질적이고 일시적 정지도 불가능 하다.[7] 운영시스템 역시 IT환경에서는 다수의 사용자를 대상으로 개발되고 자동으로 업그레이드가 이루어지지만 산업제어시스템은 개별적인 운영시스템이 개발되고 소프트웨어 업그레이드는 매우 주의 깊게 이루어져야 한다.

산업시스템을 대상으로 하는 공격은 계속해서 진화하고 있다. 스턱스넷은 2010년 6월 벨라루스에서 처음 발견된 웜 바이러스(worm virus)로, 이란 핵시설을 마비시키기 위해 미국이나 이스라엘이 퍼뜨린 사이버 무기인 것으로 추정되고 있으며, 산업시설을 감시하고 파괴하는 최초의 악성 소프트웨어이다.[16] 독일 제강공장은 2014년 12월 악성코드의 공격을 받았다고 2014년 연차보고서에서 발표하였으며, 공격자는 스피어 피싱 이메일을 사용하여 회사 네트워크의 접속권한을 획득하여 공장 네트워크로 들어갈 수 있었다.[17] 한국수력원자력도 2014년 12월 15일부터 2015년 3월 12일까지 총 6회에 걸쳐 고리와 월성 등 국내 주요 원자력발전소의 원전중단을 협박하며 해킹 한 제어시스템 설계도를 웹에 공개한 사건이 발생하였다.[18]

SW관련 취약점은 CVE취약점 신고/추적 시스템을 관리하는 비영리기관 'MITRE'에서 16개 카테고리로 공격매커니즘을 분류하여 관리하고 있다. 또한 IEC 62443을 기반으로 스마트공장에서 발생할 수 있는 추가적인 보안위협은 Table 1 과 같다.

III. 스마트공장 정보보호 인식교육 커리큘럼 개발

3.1 연구 방법

스마트공장 정보보호 인식교육 커리큘럼 개발을 위하여 ISO/IEC 27001, IEC61508, IEC62443을 참고하여 점검리스트를 통해 실태조사를 실시하였다. 실태조사는 설문과 인터뷰를 진행하였으며, 스마트공장에서 도입하는 솔루션의 기능과 역할에 대하여 중점적으로 확인하였다. 인터뷰를 통해 보호해야 하는 자산과 정보를 식별하고 보호수준을 측정하였다. 이를 기반으로 정보보호 인식교육이 가장 효과적인 대상을 식별하였다.

스마트공장 정보보호 인식교육을 위한 커리큘럼은 "국가직무능력표준(NCS, National Competency Standards)"을 기반으로 국제표준, 산업의 요구사항, 교육기관의 커리큘럼을 참조하여 작성하였다. 효율적인 커리큘럼 개발을 위하여 NIST 800-16, 800-50에서 정의하고 있는 정보보호 교육 프레임워크를 반영하였다. 효과적인 스마트공장의 수준 및 교육자의 수준에 따른 교육을 진행할 수 있도록 4단계로 레벨을 구분하였고, 스마트공장의 고도화 수준에 따라 각 교육을 배치하여 불필요한 중복교육을 방지

Table 1. CAPEC VIEW: Mechanisms of Attack & IEC62443 [6][8]

Categories	Threat type	rationale
Gather Information	Social Information Gathering Attacks	CAPEC, IEC 62443
	Information Elicitation via Social Engineering	CAPEC, IEC 62443
	Flooding	CAPEC, IEC 62443
	Excessive Allocation	CAPEC, IEC 62443
	Resource Leak Exposure	CAPEC, IEC 62443
	Amplification	CAPEC, IEC 62443
Injection	Parameter Injection	CAPEC, IEC 62443
	Resource Injection	CAPEC, IEC 62443
	Command Injection	CAPEC, IEC 62443
	Fault Injection	CAPEC, IEC 62443
Deceptive Interactions	Action Spoofing	CAPEC, IEC 62443
	Software Integrity Attack	CAPEC, IEC 62443
	Hardware Integrity Attack	CAPEC, IEC 62443
Manipulate Timing and State	Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions	CAPEC, IEC 62443
Manipulate Timing and State	Manipulating User State	CAPEC, IEC 62443
Abuse of Functionality	API Manipulation	CAPEC
	Functionality Misuse	CAPEC, IEC 62443
	Communication Channel Manipulation	CAPEC
Probabilistic Techniques	Brute Force	CAPEC
	Screen Temporary Files for Sensitive Information	CAPEC
	Fuzzing	CAPEC
Exploitation of Authentication	Authentication Abuse	CAPEC, IEC 62443
	Authentication Bypass	CAPEC, IEC 62443
	Privilege Abuse	CAPEC
	Exploiting Trust in Client	CAPEC
	Privilege Escalation	CAPEC
	Hijacking a privileged process	CAPEC
	Catching exception throw/signal from privileged block	CAPEC
	Hijacking a Privileged Thread of Execution	CAPEC
	Subvert Code-signing Facilities	CAPEC
	Target Programs with Elevated Privileges	CAPEC
Manipulate Data Structures	Buffer Manipulation	CAPEC, IEC 62443
	Attack through Shared Data	CAPEC, IEC 62443
	Integer Attacks	CAPEC, IEC 62443
Manipulate Resources	Input Data Manipulation	CAPEC
	Infrastructure Manipulation	CAPEC
	Variable Manipulation	CAPEC
	Abuse of Transaction Data Structure	CAPEC
	Protocol Manipulation	CAPEC
	Contaminate Resource	CAPEC
	Modify Shared File	CAPEC
Analyze Target	Reverse Engineering	CAPEC
	Protocol Analysis	CAPEC
Alter System Components	Malicious Logic Insertion	CAPEC
Manipulate System Users	Target Influence via Social Engineering	CAPEC, IEC 62443

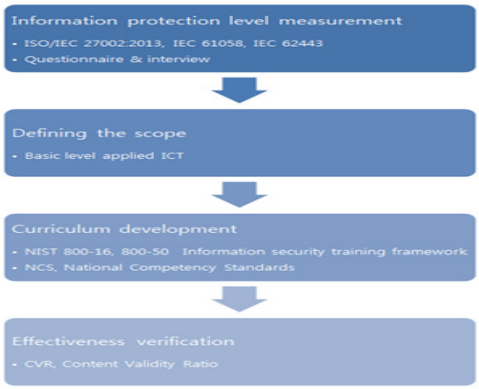

Fig. 2. Smart factory information protection awareness curriculum development

하고 효과성을 극대화 하고자 하였다.

최종적으로 작성된 커리큘럼의 타당성을 확인하기 위하여 현업에 종사하는 정보보호 전문가 및 산업체 전문가에게 타당도 비율(Content Validity Ratio, CVR)을 산정하여, 기준에 미달하는 항목에 대해서는 수정과 삭제를 진행하였다.

3.2 정보보호 수준 측정

스마트공장 정보보호 실태조사를 위한 기준은 ISO/IEC 27002:2013, "Code of practice for information security contorls"를 준용 하여, 정보보호관리체계의 통제분야인 "정보보안 정책(2)", "정보보안 조직(7)", "인적자원 보안(6)", "자산관리(10)". "접근통제(14)", "암호통제(2)", "물리적 및 환경적 보안(15)", "운영보안(14)", "통신보안(7)", "정보시스템 취득 개발 및 유지보수(13)", "공급자 관계(5)", "정보보안 사고관리(7)", "업무연속성 관리(4)", "준수(8)" 114개 통제항목을 기준으로 전기·전자·프로그램 가능한 전자 안전관리 시스템(E/E/PE)의 기능안전(Functional Safety) 표준인 IEC 61508과 산업분야의 보안 표준인 IEC 62443 (Industrial network and system security)의 안전 및 정보보호(Safety & Security) 요구사항을 맵핑하여 1차 필터링 과정을 통해 스마트공장에 필요한 정보보호 통제항목을 도출 하였다.

스마트공장의 실태조사를 위한 점검항목 개발은 ISO/IEC 27002:2013을 기반으로 1차 필터링(기능안전 및 산업보안 요구사항)과 2차 필터링(스마트공장 수준)을 통해 점검항목을 도출하였으며, 업체

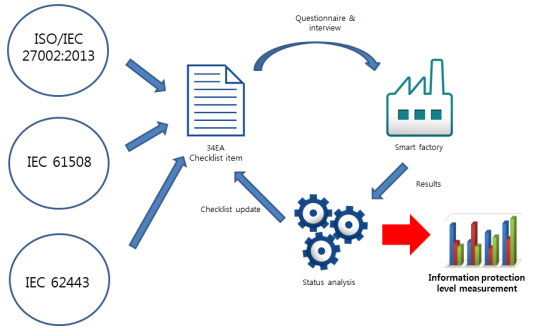

Fig. 3. Smart factory security level survey

일반현황(6)", "시설·설비·장비 및 매체보안 (4)", "시스템 접근권한 관리 (7)", "시스템 운영 보안 (6)", "암호통제 (2)", "시스템 개발 보안 (5)", "정보보호 침해사고 관리 (1)", "개인정보 생명주기 관리 (3)"로 총 34개의 통제항목을 도출하여 스마트공장 정보보호 수준측정에 활용 하였다.[15]

이를 기반으로 실태조사는 스마트공장을 추진함에 있어 준수해야 하는 정보보호 요건을 도출하고 수준을 측정하여 교육커리큘럼에 활용하기 위하여 진행하였다. 분석 방법은 설문지를 작성하여 스마트공장 방문 전 담당자에게 배포하였으며, 현장 방문 시 인터뷰 내용을 사전에 인지하도록 하였다. 스마트공장 담당자 인터뷰는 설문지 기반으로 하여 문서검토, 공장 실사, 인터뷰, 등을 진행하였으며 추가로 도입된 솔루션의 기능 및 역할에 대하여 중점적으로 확인하였다.

스마트공장의 안전한 보호를 위한 정보보호체계 구축 기반 마련을 위하여 스마트공장 정보보호체계 구축 지원사업을 받은 스마트공장(총 1,240개 중 구축완료 875개, 구축 중 365개) 중 기계/전자 부품조립 공장 3개 제약공장 1개 대하여 스마트공장 실태조사 실시 하였다.

업체마다 매출액의 격차가 존재하여 보안에 투자할

Fig. 4. Smart factory information protection status

수 있는 예산의 차이가 있었으며, 대다수 스마트공장은 ERP와 MES를 도입하여 운영 중인 것으로 확인되었다. MES 운영정보가 모바일기기 및 신뢰할 수 없는 경로를 통한 접근을 제어해야 하며, MES 도입에 대한 위험평가 실시의 필요성 있었다.

조사한 스마트공장의 매출액과 정보보호 현황은 정비례한 것으로 확인 되었다. 공장의 규모 및 매출에 따라서 정보보호에 투자할 수 있는 예산의 차이가 크기 때문에 기업규모별로 정보보호에 수준이 다를 수 밖에 없다. 정보보호 전문조직 및 전담인력을 보유한 스마트공장과 겸업을 하고 있는 스마트공장 간의 보안수준의 차이가 발생하고 있었으며, 스마트공장의 안전성을 확보하기 위해서는 정보보호 전담조직 및 인력에 대한 확보, 적절한 예산, 정보보호에 대한 인식이 매우 중요한 것으로 확인되었다.

특히, 정보보호 인식교육의 경우 추가예산의 확보 없이 정보보호 수준을 올릴 수 있으므로, 가장 시급한 부분은 정보보호 인식 향상을 위한 교육임을 확인할 수 있다.

3.3 개발 범위

스마트공장은 기초, 중간(1,2), 고도화로 총 4가지 단계로 구분되어 있다. 기초수준은 공정물류 중심의 생산실적 관리를 하며, 바코드, RFID 등을 활용하여 기초데이터를 수집하는 수준이다. 중간수준은 설비, 생산정보를 활용한 품질분석 및 실시간 생산관리를 하며 센서, PLC, 등을 활용한 실시간 생산정보를 자동으로 수집하고 설비제어를 하는 수준이다. 고도화 수준은 기획, 생산, 유통, 물류 시스템을 통합으로 제조의 모든 단계에서 실시간 연동되는 수준으로 정의되어 있다. [13] 대기업의 스마트공장은 설비 투자에 대한 예산확보가 용이하고 정보보호 관련 인증을 받기 때문에 정보보호에 대한 체계적인 교육이 이미 도입되어 있다. 하지만 기존의 전통적인 공장형태에서 ICT 솔루션을 도입하여 스마트공장이 된 공장은 정보보호에 대한 어떠한 교육이나 관리체계가 매우 미흡한 것을 실태조사를 통해 확인하였다.

따라서, 정보보호인식 교육이 가장 필요하고 효과적인 대상은 이제 솔루션을 도입하여 과거에 없던 위협에 노출되어 있는 기초 수준의 스마트공장이다. 실제 인터뷰에서 정보보호의 필요성은 인지하고 있으나, 너무 막연하기 때문에 어떤 부분을 어떤 방법으로 개선해야 하는지 모르고 있었고, 그 가이드의 필요성이 산업현장에 요구사항으로 존재 하였다.

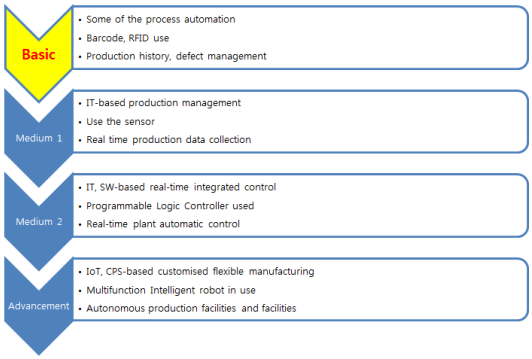

Fig. 5. Smart factory level

미국은 효율적인 인식제고 프로세스 및 프레임워크를 구성하기 위해 인식, 훈련 및 교육에 대한 명확한 정의를 내리고 있다. 특히 정보보호 교육에 대한 프레임워크는 "NIST 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model"의 프레임워크가 가장 잘 구성되었다고 알려져 있다. 정보보호 교육은 인식, 훈련, 교육 3단계로 나눌 수 있으며, 교육 대상에 따라 구성이 달라지며, 전 직원에게는 "정보보호인식교육"이 필요하다. IT시스템에 관련된 모든 직원들에게는 "보안의 기초" 교육이 필요하며, IT시스템과의 생명주기와 관련된 각각의 역할을 담당하는 직원에게는 각 단계별 구체적인 보안 훈련이 필요하며, 또한 보안전문가들에게는 "교육과 경험"이 필요하다. [14]

"NIST 800-50 Building an Information Technology Security Awareness and Training Program"에서 인식, 훈련, 교육을 다음과 같이 정의하고 있다.

① 인식 : 인식(awareness)은 훈련이 아니며 인식제고의 목적은 단순히 보안에 대한 주의를 집중시키는 것이고 개인들로 하여금 보안에 대한 염려를 인지시키는 것이며, 이에 따라 대응할 수 있도록 하려는 것임. 이를 통해 조직의 구성원들이 IT보안에 대해 알고 발생할 수 있는 문제들에 대응할 수 있게 되며, 인식제고를 위한 프로그램이 마련되면 이를 뒷받침해줄 수 있는 기본적인 사항들과 관련 문서들이 필요하게 됨.

② 훈련 : 훈련은 구성원들이 인식제고 프로그램을 통해 생산된 문서들을 올바르게 이해하고 보안능력을

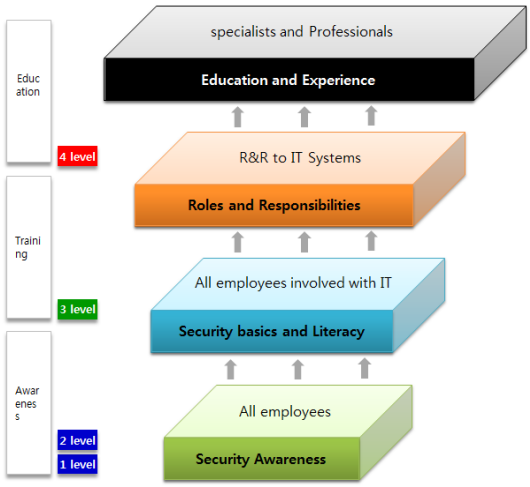

Fig. 6. Define education, training, awareness [10][11]

키우며 실천할 수 있도록 해줌. 훈련은 업무와 관련된 기술을 가르쳐 개인의 원활한 업무 수행을 지원할 수 있도록 한다는 점에서 인식제고와 다르다고 볼 수 있음. "훈련"은 정보보호전문가가 아닌 기능적인 전문분야의 참석자로 하여금 필요한 보안스킬과 능력을 제공하는 것으로, 사람들로 하여금 특정기능을 수행하는 스킬을 가르치는 것. 반면에 인식은 어떠한 이슈에 대해 개인적인 주의를 끄는 것이 초점임.

③ 교육 : 교육은 조직의 모든 기능 업무들에서 이루어질 수 있는 보안능력, 경쟁력 등을 하나의 지식으로 집약시켜 전문가를 양성하는데 초점을 맞추고 있음.

스마트공장의 안전한 확산을 위해서 필요한 여러 가지 요소 중에서 기초수준의 스마트공장을 대상으로 정보보호 인식향상을 위한 교육이 필요하고 효과적이고 효율적인 교육을 위해서 커리큘럼 개발이 필요하다.

3.4 커리큘럼 개발

교육커리큘럼은 국가직무능력표준(NCS)의 능력단위 "보안운영관리", 분야 "기계" 를 기반으로 하였으며, ISO 27001, IEC 62443 및 관련 교육기관의 교육과목을 참고하여 개발 하였다.

각각의 영역에서 선정된 교육단위는 NCS의 "보안엔지니어링", "제조" 직무에서 요구하는 기본 교과목과, 타 교육기관 및 협회(KISA 아카데미, 한국생산성본부 등), 정보보호 전문가 커리큘럼을 참조하여

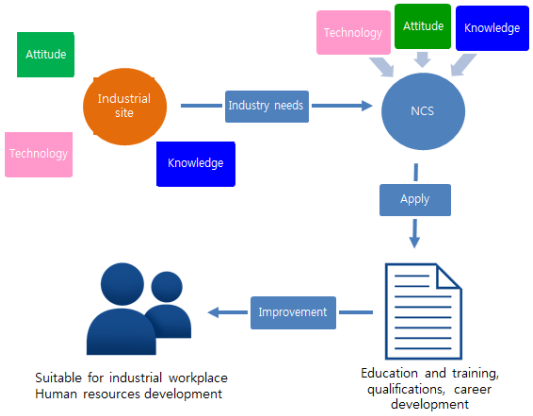

Fig. 7. National Competency Standards concepts [9]

인식교육에 필요한 기초(Basic)를 중심으로 구성되었으며, 이는 지속적인 연구를 통해 체계적인 커리큘럼 확보가 필요하다. 교육단위에 따라 요구하는 지식·기술·태도는 교육의 목적, 방향, 내용 등에 따라 상이할 수 있으며, 최소 요구사항이 반영되어야 효과적인 교육이 이루어 질 수 있다. 이는 NCS에서 기본적으로 요구하는 교육대상자 요구사항으로 본 연구에서는 이를 적극적으로 반영하여 커리큘럼 구성에 활용하였으며, Table 2.와 같이 교육에서 필요한 지식·기술·태도 기준을 정의하였다. 이를 통해 각 교과목 별로 교육대상자에게 필요한 기술적, 지식적, 태도적인 기준을 제시함으로써 효과적인 교육을 기대할 수 있다.

Table 2. Smart factory information security base[14]

	Main contents
Knowledge	• Smart factory laws and policies related information protection and security • Smart factory privacy policy / task guideline • Key information handling outsourcing related law/regulations/procedures • Managing access authority of key information • Classification standard of information asset • Strategic planning for the development of methods of information protection services

	• Smart factory information systems proctection, security program and safety facilities • Smart factory classification, listing and security management of assets • Security rating method for major asset • Handling key information assets • Management method of media contained key information • Physical disposal / destruction method of key information contained in media and industrial, electronic equipment • Subjects and sort of training needed or performed in interior and exterior facility • Key information management regulations • Key information writing guide, required entry and standard of content for key information creater • Key information writing, keeping, disposal, system buildup for general staff • How to protect key information and manage security • Designing, development, utilization and management of key information protection training program • Key information educational material development methods and training techiques • Knowledge about cause of major information accident and trends • Guideline knowledge about major information accident
Technology	• Smart factory laws and policies related information protection and security • Key information handling outsourcing related law/regulations/procedures • Managing access authority of key information • Classification standard of information asset • Smart factory information systems proctection, security program and safety facilities • Smart factory classification, listing and security management of assets • Smart factory classification, listing and security management of assets • Security rating method for major asset • Handling key information assets • Management method of media contained key information • Physical disposal / destruction method of key information contained in media and industrial, electronic equipment • Subjects and sort of training needed or performed in interior and exterior facility • Key information writing guide, required entry and standard of content for key information creater • Reward and punishment regulations and methods established by commission for key information writing • Key information writing, keeping, disposal, system buildup for general staff • How to protect key information and manage security • Designing, development, utilization and management of key information protection training program • Key information educational material development methods and training techiques • Knowledge about cause of major information accident and trends
Attitude	• Law-abiding spirit for legal requirements / regulations about information security • Law-abiding spirit for legal requirements / regulations about technical security for key information • Responsible and fair attitude to key information security • Dilligent attitude to activity for medical information proctection /

	security • Responsible attitude as key information manager • Elaborate attitude to finding key information's vulnerability and preventing • Active and propulsive attitude to keeping information security • Cooperation for keeping friendly relationship with other departments for information security • Law-abiding spirit to follow fixed law / rules / regulations for information security • Resonsible attitude to keep information security • Diligent attitude to repetitive tasks for information security • Logical and creative attitude to developing curriculum and teaching materials for various educatee • Responsible attitude to careful planning for maximizing efficiency • Continued research and research will for efficiency advancement of information security education management system • Effort to apply information security guideline to work

최종적으로 도출한 스마트공장 정보보호 커리큘럼은 산업보안(5), 스마트공장 동향(2), 위험관리(8), 보안감사(2), 보안이론(1), 보안기술(5), 솔루션 이해(1), 보안동향(2)로 개발 되었다. 이는 주기적으로 산업현장의 요구사항과 보안기술 동향을 파악하여 지속적으로 개발되고 개선되어야 할 것이다.

스마트공장이 확산되고 있는 현시점에서는 레벨 1-2의 인식단계에 대한 교육 컨텐츠를 먼저 개발하여 산업현장에서 바로 적용할 수 있도록 하였을 경우 그 효과가 매우 크다고 볼 수 있다.

3.5 타당성 분석

각 과정마다 내용이 타당한지 판정하기 위해서 내용 타당도 비율(Content Validity Ratio, CVR)을 구하였다. CVR을 구하는 공식은 CVR = (ne - N/2)/(N/2) (N: 응답 수, ne: Likert 4-'타당함' 또는 Likert 5-'매우 타당함')로 구하였다.[12]

Table 4. The minimum value of the relevant percentage[12]

Personnel	7	8	9	10	15	20	25	30	35
CVR minimum	0.99	0.75	0.78	0.62	0.49	0.42	0.37	0.33	0.31

현업에 종사하는 정보보호 및 산업보안 전문가 20인을 대상으로 커리큘럼 개발의 방법론과 결과에 대하여 리뷰를 진행하였으며, 각 항목에 대해서 타당성을 검증하였다. CVR 최소값을 충족하지 못하는 항목은 없었으나 일부 의견을 반영하였다. 교육단위요소에 대해서는 타당하다는 의견이 절대적이었으며, 일부 레벨에 대하여 타당하지 않다는 의견이 있었다. 해당 전문가의 의견을 반영하여 완성된 것인 Table 3 이다.

최종적인 커리큘럼에 대한 전문가의 타당도 비율값(CVR)은 Table 5와 같이 나왔으며, 0.42보다 높은 값으로 전체적으로 타당하다는 결론을 도출 하였다.

$$CVR = \frac{Ne - \frac{N}{2}}{\frac{N}{2}}$$

Fig. 8. CVR formula

IV. 결 론

스마트공장은 매우 빠른속도로 확산되고 있다. 수많은 업종이 ICT기술과 접목하면서 발전하고 활성화되고 있으며 특히 IOT산업의 발전으로 인하여 스마트공장은 그 확산속도가 매우 빠르다. 제조업 특성상 단가경쟁이 심하고 더 적은 예산을 투입하여 고품질의 제품을 생산해 내는 것이 해당 공장의 경쟁력이며 매우 중요한 요소이다. 보안은 예산투자를 필요로 하기 때문에 보안에 대한 투자는 단가의 상승으로 이어질 수 있다. 특히 중소규모의 스마트공장인 경우는 단가에 더 민감할 수 밖에 없다. 따라서 추가 예산의 투자가 적으면서 가장 효과적으로 보안성을 높일 수 있는 방안이 안전하게 스마트공장을 확산하는 방법이라 할 수 있다.

Table 3. Smart factory information security curriculum

Educational distinction	Education	Type	Level	Educational units element
Industry security	Industry convergence security	Education	4	Industry convergence security
	Factory infrastructure security	awareness	3	Factory infrastructure security
	Industrial terrorism and infrastructure security	awareness	2	Industrial terrorism and infrastructure security
	Computing platform	Education	1	Computing platform
	Supply chain security	Education	4	Supply chain security
Smart factory Trends	Smart factory standard trend	awareness	2	IEC 62443 understanding
	The smart factory trends	awareness	1	Domestic and international trends in the smart factory
Risk management	Security planning	Training	4	Factory environmental analysis
		Training	4	To set the security range
		Education	4	Security goals
	Security risk assessment	awareness	2	Asset identification
		Training	4	Asset analysis
		Training	4	Risk analysis
		Training	4	Risk assessment
	Define security requirements	Training	4	Eliciting security requirements
		Training	4	Security requirements analysis
		Training	4	Security requirements specification
		Training	4	Verification of the security requirements
	Administrative security building	Education	4	Information protection policy
		Training	4	Protect organizational information
		Training	4	Establishing human security measures
	The physical security of the building	Training	3	Physical control of the protected areas
		Training	3	System protection
		awareness	1	Office building security
	Technical security provisioning	Training	3	Build the application security
		Training	3	Server security building
		Training	3	Network security building
		Training	3	Build a database (DB) security
	Security system management	Training	4	Establishment of operational security
		Training	4	Infringement incident response

Educational distinction	Education	Type	Level	Educational units element
		Education	4	IT established a disaster recovery system
		Training	4	Information security training
	Security threat management control	Training	4	Security threat detection
		Training	4	Security threat analysis
		Training	4	In response to security threats
		Training	4	Post processing
Security audit	Security audit	Training	4	Security audit plan
		Training	4	Performs security audits
		Training	4	Security audit follow-up
	Security certificate management	Training	4	Security certification preparation
		Training	4	Security certification application
		Training	4	Security certification audit
		Training	4	Security authentication measures nonconformance
		Training	4	Security certification follow-up
Security theory	Introduction to information protection	awareness	1	Introduction to information protection
Security technologies	Network hacking and vulnerability analysis	Training	3	Network hacking and vulnerability analysis
	Web hacking and vulnerability analysis	Training	3	Web hacking and vulnerability analysis
	An analysis on the system hacks and weakness	Training	3	An analysis on the system hacks and weakness
	Secure coding and development security	Training	4	Secure coding and development security
	Database security	Training	3	Database security
Understand the solution	Understanding the smart factory solutions	awareness	2	Understanding the smart factory solutions
Security trends	The latest trends in information security technology	awareness	1	The latest trends in information security technology
	Information security accident case	awareness	1	Information security accident case

Table 5. Educational units element CVR

Educational distinction	Educational units element	CVR
Industry security	Industry convergence security	1
	Factory infrastructure security	1
	Industrial terrorism and infrastructure security	1
	Computing platform	1
	Supply chain security	1
Smart factory Trends	IEC 62443 understanding	0.8
	Domestic and international trends in the smart factory	0.8
Risk managemen t	Factory environmental analysis	0.9
	To set the security range	0.9
	Security goals	0.8
	Asset identification	0.9
	Asset analysis	0.9
	Risk analysis	0.9
	Risk assessment	1
	Eliciting security requirements	0.8
	Security requirements analysis	0.9
	Security requirements specification	0.9
	Verification of the security requirements	1
	Information protection policy	0.9
	Protect organizational information	0.9
	Establishing human security measures	1
	Physical control of the protected areas	0.9
	System protection	1
	Office building security	0.9
	Build the application security	0.8
	Server security building	1
	Network security building	1
	Build a database (DB) security	1
	Establishment of operational security	1
	Infringement incident response	0.9
	IT established a disaster recovery system	1
	Information security training	1
	Security threat detection	0.9
	Security threat analysis	0.9
	In response to security threats	0.9
	Post processing	0.9
Security audit	Security audit plan	0.8
	Performs security audits	1
	Security audit follow-up	1
	Security certification preparation	0.9
	Security certification application	0.8
	Security certification audit	0.9
	Security authentication measures nonconformance	1
	Security certification follow-up	1
Security theory	Introduction to information protection	0.6
Security technologies	Network hacking and vulnerability analysis	0.8
	Web hacking and vulnerability analysis	0.7
	An analysis on the system hacks and weakness	0.8
	Secure coding and development security	0.7
	Database security	0.9
Understand the solution	Understanding the smart factory solutions	0.9
Security trends	The latest trends in information security technology	0.9
	Information security accident case	1

본 연구에서는 기초수준 스마트공장의 보안성을 향상시키기 위한 스마트공장 정보보호 인식교육 커리큘럼을 개발하여 제안하였다. 이를 통해 다음과 같은 부분에서 보안성을 향상할 수 있다.

- 패스워드 복잡성 유지 및 주기적인 패스워드 변경
- 보호구역 설정의 필요성 및 관리방법
- 업무/비업무의 무선AP 분리 및 암호화 설정
- 업무용 무선AP의 기기인증

- 주요 시스템에 대한 로그검토
- 시큐어 코딩 가이드를 통한 개발방법 공유
- 침해사고 발생 시 비상연락망 공유
- 전반적인 정보보호의 필요성 및 개선활동

안전하게 스마트공장이 확산되고 정착이 되기 위해서는 주기적으로 산업현장의 요구사항과 보안기술 동향을 파악하여 지속적으로 개발되고 개선되어야 할 것이다.

References

〔1〕 wikipedia, https://ko.wikipedia.org/wiki/%EC%83%9D%EC%82%B0_%EA%B4%80%EB%A6%AC_%EC%8B%9C%EC%8A%A4%ED%85%9C

〔2〕 Korea Smart Factory Foundation, http://www.smart-factory.kr/dext5editordata/2016/06/20160602_102324259_38328.jpg

〔3〕 Korea Smart Factory Foundation, 2015 smart factory support companies participating in monthly House of excellence, pp. 5, 2015

〔4〕 Ministry of Commerce Industry and Energy, http://www.motie.go.kr/motie/py/brf/motiebriefing/motiebriefing11.do?brf_code_v=11#header

〔5〕 Ministry of Commerce Industry and Energy, creative economy implementations for manufacturing innovation 3.0 strategy, pp. 3. 2014

〔6〕 mitre, hhttp://capec.mitre.org/data/definitions/1000.html

〔7〕 NIST, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY (FINAL PUBLIC DRAFT),pp. 20-21, 2008

〔8〕 IEC 62443-3-3, "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels"

〔9〕 NCS, http://www.ncs.go.kr/ncs/page.do?sk=P1A1_PG01_001

〔10〕 NIST 800-16 "Information Technology Security Training Requirements:A Role- and Performance-Based Model"

〔11〕 NIST 800-50 "Building an Information Technology Security Awareness and Training Program"

〔12〕 C. H. LAWSHE, A QUANTITATIVE APPROACH TO CONTENT VALIDITY, Personnel Psychology, Volume 28, Issue 4, pp. 563 - 575, Dec, 1975

〔13〕 Korea Evaluation Institute Of Industrial Technology, PD ISSUE REPORT, VOL 15-11, pp. 14, 2015

〔14〕 KHIDI, Health and medical information and medical information for Exchange-based activation, 2015

〔15〕 KOSF, The Foundation for the spread of the smart plant study on spontaneous composition, 2016

〔16〕 wikipedia, https://ko.wikipedia.org/wiki/%EC%8A%A4%ED%84%B1%EC%8A%A4%EB%84%B7

〔17〕 dailysecu, http://www.dailysecu.com/news/articleView.html?idxno=12372

〔18〕 boannews, http://www.boannews.com/media/view.asp?idx=44738

〈저자소개〉

전 인 석 (In-Seok Jeon) 종신회원
2009년 8월: 건국대학교 정보통신대학원 정보보호학과 석사
2016년 8월: 고려대학교 정보보호대학원 정보보호학과 박사 수료
2009년 9월~현재: Ahnlab CERT팀 선임 연구원
〈관심분야〉 네트워크보안, 정보보호관리체계, 정형기법, DevOps, 소프트웨어 보안 등

이 병 권 (Byung-Gueon YI) 정회원
1989년 2월: 전북대학교 컴퓨터공학과 졸업
1992년 2월: 포항공대 대학원 전산과 석사 수료
2005년 2월: 전남대학교 대학원 정보보호협동과정 박사 수료
2001년 1월~2008년 11월:한국정보보호진흥원 팀장
2009년 6월~2012년 5월: (주)안랩 팀장
2012년 6월~현재: 현대오토에버 정보보안실장
〈관심분야〉 정보보호, SCADA보안, 스마트팩토리 보안, IoT보안 등

김 동 원 (Dong-Won Kim) 종신회원
2009년 2월: 서울과학기술대학교 컴퓨터공학과 졸업
2012년 2월: 건국대학교 정보통신대학원 정보보호학과 석사
2014년 2월: 고려대학교 정보보호대학원 정보보호학과 박사 수료
2014년 3월~현재: 서울호서전문학교 사이버해킹보안과 전임교수
〈관심분야〉 시큐어코딩, 정보보호, 모바일 보안, 지능형 차량 보안, SSCA, 정형기법 등

최 진 영 (Jin-Young Choi) 종신회원
1982년 서울대학교 컴퓨터공학과 (학사)
1993년 미국 Univ. of Pennsylvania, Dept. of Computer and Information Science (박사)
1986년 미국 Drexel University, Dept. of Mathematics and Computer Science (석사)
1996년~현재 고려대학교 컴퓨터-전파통신공학부 교수
〈관심분야〉 정형기법, 임베디드 실시간시스템, 프로그래밍언어, 프로세스 대수, 소프트웨어 공학