Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.3, Jun. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.3.645

제어시스템 사이버 보안 교육훈련 방안 연구

김 경 호,[1†] 맹 영 재,[1] 장 문 수,[1] 류 재 철[2‡]
[1]ETRI 부설연구소, [2]충남대학교

A Study on Control System Cyber Security Education & Training Method

Kyeong-Ho Kim,[1†] YounJae Maeng,[1] MoonSu Jang,[1] Jae-Cheol Ryou[2‡]
[1]The Affiliated Institute of ETRI, [2]Chungnam National University

요 약

제어시스템에 대한 사이버 위협 사례가 증가함에 따라 제어시스템 사이버 보안에 대한 필요성이 증가하고 있다. 현재 국내외에서 다양한 사이버 보안 관련 교육과 제어시스템 관련 교육이 수행되고 있다. 그러나 제어시스템의 특성과 참가자의 특성을 온전히 반영하기에 아쉬움이 있다.

본 논문에서는 제어시스템의 특성을 반영하기 위하여 다양한 제어시스템을 분석하였다. 분석 내용과 IEC62443에서 제시된 제어시스템 모델을 이용하여 제어시스템 훈련 환경을 제안한다. 그리고 참가자의 학습 성과를 향상하기 위해 참가자 특성을 분석하고, 교육 분야의 ARCS 학습 모델을 활용한 융합소통 훈련 기법을 제안하였다. 그리고 제안한 훈련환경과 훈련기법을 이용한 교육훈련 시나리오를 제시하였다. 제안한 내용을 통해 보안전문가와 제어시스템 전문가의 상호 이해를 바탕으로 한 협업 모델을 실무에 적용하여 최종적으로 제어시스템 사이버 보안 능력을 향상시킬 수 있을 것이라고 기대한다.

ABSTRACT

As the number of cyber threats to control systems increases, the need for control system cyber security is also increasing. Currently, various cyber security related education and control system education are being conducted. However, it does not fully reflect the characteristics of the control system and the characteristics of the participants.

In this paper, we propose a training system and technique to enhance the control system cyber security capability. To this end, we analyze the limitations of existing security education. Based on the results, we develop a control system training environment model based on the IEC62443 Standard and develop an ARCH based training method.

Keywords: Industrial Security, ICS Security, SCADA Security, Training, Education, ICS Training

I. 서 론

사이버 물리시스템(Cyber-Physical System, CPS)은 다양한 통신 매체를 통해 네트워크를 형성하고 여러 IT(Information Technology) 시스템과 연산체계를 통합함으로써 물리 프로세스와 상호작용 할 수 있는 컴퓨팅 시스템을 통칭하는 단어이다[1-2].

제어시스템은 포괄적인 범위의 CPS라는 용어에 앞서 산업제어시스템 이라는 명칭으로 조금 더 협소한 분야를 지칭하는 용어이다. 일반적으로 ICS (Industrial Control System) 또는 SCADA (Supervisory Control And Data Acquisition)로 쓰인다. 이러한 제어시스템은 전력, 화학, 교통, 수자원, 항공, 항만 등 다양한 기반시설과 산업 시설에 활용되고 있다. 최근 제어시스템을 대상으로 한 사이버

Received(04. 16. 2019), Modified(05. 20. 2019), Accepted(05. 23. 2019)
† 주저자, lovekgh@nsr.re.kr
‡ 교신저자, jcryou@home.cnu.ac.kr(Corresponding author)

공격과 보안에 대한 관심이 급증하면서 이러한 위협에 대한 대응 방안의 수립 필요성이 증가하고 있다.

대응 방안으로는 제어시스템 환경 하에서 사이버 보안 능력을 향상 시킬 수 있는 보안기술의 연구 개발, 상용 보안 시스템 도입, 보안 컨설팅 등을 생각해볼 수 있다. 하지만 비용, 시간, 인력 등 현실적인 제약으로 인해 쉽게 시도하기 힘들다. 또한 이 방법들은 근본적인 해결책이 아니다. 보안 기술, 장비를 도입하고 정책을 수립해도 이를 운용하는 인적 자원에 따라 만족할만한 성과를 얻을 수 없을 가능성이 있기 때문에 인적 자원의 능력 계발이 필요하다.

인적 능력을 강화하는 가장 기본적인 방법은 외부 보안 전문가를 수급하는 방법이다. 하지만 제어시스템의 특수성으로 인해 어려움이 있다. 제어시스템은 앞서 언급한 바와 같이 다양하고 특수한 물리 장비들을 제어하는 시스템이다. 이런 환경에서 기존의 보안 전문가는 다양한 상황으로 인해 본인의 역량을 모두 펼치기 힘들다. 반대로 제어시스템 전문가를 수급하면 제어시스템에 대한 역량은 강하지만 사이버 보안 관련 역량을 보유하고 있는 경우를 찾기 힘들다. 결국 사이버 보안과 제어시스템 전반에 관한 역량을 동시에 갖춘 인력을 양성하거나 상호 협력할 수 있도록 하는 방안이 필요하다.

본 논문은 사이버 보안과 제어시스템 모두의 역량을 갖춘 인력을 양성하기 위한 훈련 방안을 제시한다. 이를 위하여 현재 알려진 사이버 보안 관련 교육과 제어시스템 관련 교육을 분석한다. 이 분석을 통해 기존 보안 교육으로 제어시스템 분야에서 사이버 보안 전문 인력을 양성하기 힘든 원인을 도출하고, 원인을 해결하기 위하여 제어시스템의 구조와 보안 위협 요소, 동향을 분석한다. 이를 통해 훈련 시스템을 설계·구축하고, 인력 양성을 위한 훈련 기법을 제시한다.

본 논문은 총 6장으로 구성되어 있으며 2장에서는 제어시스템의 특징과 제어시스템을 대상으로 하는 보안위협의 동향을 분석한다. 3장과 4장에서는 제어시스템 보안 교육 동향 및 기존 보안교육의 한계점을 제시한다. 5장에서는 제어시스템 사이버 보안 훈련 방안을 제시하고 마지막 6장에서 결론을 맺는다.

II. 제어시스템 특징 및 보안위협 동향

2.1 제어시스템 개요

제어시스템은 서로 다른 유형의 상호 연결된 장치와 기본적인 물리적 프로세스를 포함하는 복잡한 자동화 시스템이다. 제어시스템 공정의 형태는 크게 연속 제조 공정(Continuous Manufacturing Process)와 일괄 제조 공정(Batch Manufacturing Process)이 있다. 연속 제조 공정은 전력 플랜트, 화학 플랜트 등이 있다. 일괄 제조 공정은 연속성이 필요 없는 제조 공정을 말한다.

제어시스템은 공정의 형태에 따라, 설치시기에 따라, 제조사에 따라 매우 다양한 형태의 시스템과 구성이 사용된다. NIST(National Institute of Standards and Technology) Special Publication 800-82 'Guide to Industrial Control System Security'[3]에서는 사이버 보안 관점에서 공통 요소를 뽑아 제어시스템의 형태를 Fig.1.과 같이 제시하였다.

기본적으로 제어시스템은 제어를 위한 컨트롤 센터와 현장인 사이트로 구성된다. 컨트롤 센터는 각 사이트의 상태를 모니터링하고 제어하여 제어시스템이 안전하게 운영될 수 있도록 한다. 사이트는 각종 필드장치와 제어기기로 구성된다. 그리고 제어기기는 다양한 통신 매체를 이용하여 컨트롤 센터로 수집된 데이터를 전송하고, 수신된 명령을 수행한다.

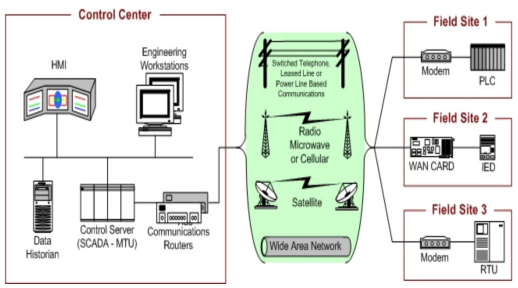

Fig. 1. SCADA System General Layout[3]

2.2 제어시스템 특징

제어시스템은 2.1에서처럼 일반 IT시스템과 형태와 구성에서부터 차이가 있다. 대표적으로 Table 1. 과 같은 차이가 있다.

Table 1. Features of Control System

System / Feature	Control System	IT System
Non-stop Service	Must	Optional
H/W, S/W	Dedicated	Universal
Performance	Strong Real-time	Throughput
Operating Cycle	Long-term	Relative Short-term
Damage Effect	Physical	Economic

대부분의 제어시스템은 24시간 365일 무중단 운영이 필수이다. IT시스템의 경우에도 무중단 운영이 필요하지만, 상황에 따라 잠시 운영의 중단이 허용된다. 무중단 운영이라는 특징으로 인해 제어시스템은 보안 업데이트 등의 조치가 어렵다. 또한 IT시스템은 대부분 범용 H/W와 S/W를 사용하는 반면에 제어시스템은 그 용도에 맞는 행위를 위하여 전용 장치와 임베디드 OS를 사용하는 경우가 많다. 이는 강한 실시간성을 요구하기 때문이기도 하다. 그리고 제어시스템은 특정 상황에 맞는 사이클(Cycle)이라고 표현하는 제어 처리 주기에 대한 강한 요구사항이 있다. 반면 IT시스템은 전체 성능에 초점을 맞춘다. 따라서 특정 부분에서 처리속도의 지연은 감수할 수 있다. 또한 제어시스템은 한번 설치되면 10~30년 이상 운용하게 된다. 이는 장비의 노후화, 소프트웨어의 노후화로 이어져 시간의 흐름에 따라 강화되는 보안 요구사항을 만족하기 어려운 상황이 발생한다. 가장 결정적인 차이점으로 IT시스템은 사고 발생 시 경제적 피해와 사용자의 불편을 야기 할 수 있지만, 제어시스템은 그 특성에 따라 물질적· 인적 피해로 이어지기 쉽다.

2.3 보안위협 동향

제어시스템 보안 위협의 증가 추세는 미국 국토안보부 산하의 ICS-CERT(Industrial Control System - Cyber Emergency Response Team)에서 발표되는 통계에서 확인할 수 있다. 제어시스템 사이버사고 건수는 2010년 39건에서 2016년 290건으로 가파른 증가 추세를 보인다.

Table 2. NCCIC/ICS-CERT FY Metrics

Report / Year	ICS Incident Reports	ICS Related Vulnerability Reports
2010	39	18
2011	140	139
2012	197	137
2013	257	187
2014	245	159
2015	295	189
2016	290	187

또한 보안 취약점 발견 건수 역시 2010년 18건에서 2016년 187건, 2017년 322건, 2018년 415건으로 증가하였다[4,12].

제어시스템에 대한 사이버 위협은 2010년 이란의 원심분리기를 파괴하던 Stuxnet을 시작으로 2011년 정보유출을 위한 Night Dragon, Nitro Attacks, 2012년 Flame, Mahdi 등 꾸준히 보고되고 있다. 그리고 2015년에는 우크라이나에서 사이버 공격으로 인한 대규모 정전사태인 Black Energy가 발생하였다. 2016년 러시아 해커가 열차 통제시스템 공격 및 제어 방법을 공개하였으며, 2019년인 현재까지 제어시스템에 대한 공격 시도, 취약점은 꾸준히 보고되고 있다. 이외에도 정보 수집을 위한 악성코드의 활동이 활발하게 탐지되었으며, 국내 역시 이와 관련된 위협이 계속 보고되고 있다.

이러한 정보 수집 형태의 공격은 우크라이나 정전사태와 같은 대규모 제어시스템의 물리적 피해를 야기하는 것을 최종 목적으로 하는 것을 고려해볼 때, 이러한 위협에 대한 보고가 증가하는 것을 예의주시해야 한다.

III. 제어시스템 사이버 보안 교육 동향

제어시스템에 대한 사이버 보안 위협이 증가함에 따라 인력양성에 대한 필요성이 대두되었다. 이에 따라 제어시스템 사이버 보안을 목적으로 하는 교육이 이루어지고 있다.

3.1 국외

INL(Idaho National Laboratory)은 1949년

에 미국 에너지부서의 임무(원자력 및 에너지 분야 등)를 지원하기 위해 설립된 국립 연구소이다. 2001년 이후 사이버위협이 고조됨에 따라 ICS 보안 관련 프로그램을 연구하고 있다. NSTB(National SCADA Test Bed) 프로그램과 더불어 제어시스템 보안 모의침투 방어 교육 훈련을 실시하고 있다. 제어시스템에 대한 환경을 구축하여 놓고, 공격팀과 방어팀을 구성하여 모의침투 방어교육을 실시하고 있다. 이 과정은 1주일 과정으로 진행되고, 참가자를 자국민으로 제한한다[13].

CSSC(Control System Security Center)는 제어시스템 관련 보안평가 기술, 시험도구를 개발하고 평가를 수행하기 위한 목적으로 설립되었다. 제어시스템 보안과 관련된 다양한 연구를 수행하며 2014년 METI(상업 정보 정책국 정보 보안 정책실) 주관 전력·가스·빌딩·화학 분야의 사이버 보안 훈련을 실시하였다. 또한 각 분야의 사업자와 산업 단체 들을 대상으로 2018년 2월과 3월에도 실시하였다[14].

제어시스템 보안 기초에서부터 위협 평가, 침투테스트, 평가 인증 등 다양한 제어시스템 보안 교육을 제공한다. 해당 교육은 5일 과정으로 진행되며 제어시스템 테스트베드를 활용하거나 별도의 교육용 장치를 이용하여 교육한다.

iTrust는 SUTD(Singapore University of Technology and Design)의 사이버 보안 분야 연구실이다. 2015년 수처리 제어시스템을 대상으로 만들어진 제어시스템 테스트 베드를 구축하였다[5].

Fig. 2. Example of INL Training

Fig. 3. Testbed of CSSC(Water Treatment, Chemical factory)

iTrust에서는 제어시스템 사이버보안 교육을 진행하고 있으며 상기 테스트베드 또는 별도의 교육용 시스템을 이용하여 교육을 수행하고 있다. 또한 제어시스템에 대한 관심 유도와 참여자의 흥미를 유발하기 위하여 2016년부터 2017년까지 2회에 걸쳐 S3(SUTD Security Showdown)라는 CTF (Capture The Flag) 이벤트를 진행하였다[6,15]. 그리고 이와 관련된 데이터를 홈페이지에 공유하고 있다.

SANS 연구소는 1989년 연구 및 교육기관으로 설립된 이래 전 세계적으로 보안 전문가 대상 교육을 하는 회사이다. 보안 정책부터 기술적인 요소까지 전반적인 분야에 걸쳐 교육한다. 제어시스템 보안이 이슈됨에 따라 현재 관련 교육이 점차 증가하고 있는 추세이다. 2019년 4월 현재 약 3개의 과정이 각 5일 내외로 운영되고 있으며, 기존 IT 보안 전문가의 관점에서의 제어시스템 보안에 대한 내용으로 구성되어 있다[16]. 제어시스템 보안에 관련된 과정의 일례로 Fig.5의 가상 도시를 구성하는 제어시스템 요소에 대한 위협과 방어 기법을 교육 받는다.

Fig. 4. Testbed of iTrust(SWaT)[8-9,14]

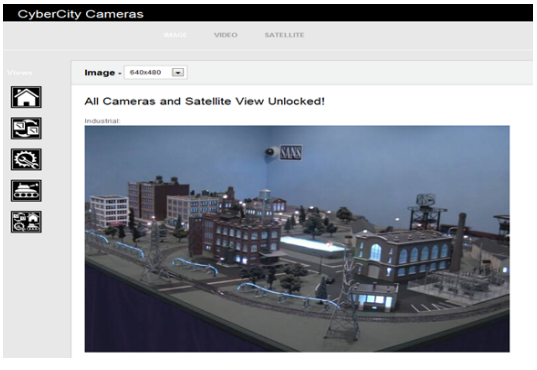

Fig. 5. CyberCity of SANS

3.2 국내

국가보안기술연구소 사이버안전훈련센터는 2014년에 개소하여 국가·공공기관의 사이버 위협 대응 능력 향상을 위하여 교육·훈련을 진행하고 있다. 운영중인 훈련 중에 기반시설 제어시스템 보안에 대한 내용을 다루어지고 있다. 센터에서 수행하는 훈련은 하나의 기관을 상정하고 대상자에게 IT 시스템에서부터 제어시스템까지의 환경과 각 시나리오에 따른 훈련 콘텐츠가 제공된다. 훈련은 제어시스템에 대한 사이버 위협 단계에 따라 대응 절차를 습득하는 것을 목표로 한다. 다만, 참여 대상이 제한되어 일반인은 참여가 어렵다.

한국인터넷진흥원의 KISA 사이버보안인재센터는 2009년에 개소하여 일반인의 정보보호 인식 제고에서부터 보안전문가를 육성하기 위하여 전반적인 보안 관련 교육을 진행하고 있다. 많은 분야를 다루고 있고 그 중 민간 기반시설 정보보호 담당자 교육 과정을 운영하고 있다. 2019년 현재 관리 분야인 정보통신 기반시설 정보보호 업무실무 과정에서부터 기술 분야인 기반시설 네트워크 보안 과정이 운영되고 있으며 현재 무료로 운영되고 있다.

또한 민간 보안 교육 업체에서 기존에 운영되던 IT시스템 보안 교육을 각색하여 제어시스템 분야의 보안 교육 과정을 준비하거나 개설하여 운영하고 있다.

IV. 기존 교육의 한계

본 논문에서 대상으로 하는 제어시스템 사이버 보안은 크게 IT시스템의 사이버 보안과 제어시스템 보안으로 나누어 볼 수 있다. 일반적으로 보안 교육은 IT시스템에 대한 사이버 보안을 말한다. 따라서 대부분의 사이버 보안 관련 교육·훈련은 IT시스템 위주로 구성되어 있다.

최근 제어시스템 영역에서의 보안 교육 필요성이 대두됨에 따라, 제어시스템을 대상으로 하는 다양한 교육이 개설되고 운영되고 있다. 하지만 IT시스템에 익숙한 보안 전문가가 과정을 구성하고 강의를 함에 따라 제어시스템의 특성에 대한 고려가 부족하며, 교육 대상 또한 IT영역에서의 보안 전문가 수준으로 맞추어져 있는 형편이다. 3장에서 언급한 제어시스템 사이버 보안 교육도 IT 분야의 보안 전문가의 제어시스템 분야 능력 강화에 초점이 맞추어져 있다.

IT영역에서 보안은 해킹, 악성코드 등 사이버 보안 (Security) 으로 통용된다. 하지만 제어시스템 분야에서 보안은 안전(Safety) 또는 물리 보안을 말한다.

2.2에서 언급한 IT시스템과 제어시스템의 차이도 매우 중요한 요소로 작용한다. 대표적으로 IT 시스템은 약간의 지연 정도보다는 전체 성능을 중요시하지만, 제어시스템은 1ms의 지연도 사고와 이어질 수 있다. 그리고 사고는 물리적 피해와도 연동 된다. 이러한 특수성에 기인해 기본적으로 제어시스템관련 종사자는 안전과 가용성을 가장 중요시 하는 환경에서 근무하고 있다. 자연스럽게 보안 신기술, 기존 환경에 영향을(성능 등) 끼치는 새로운 요소 도입에 대하여 매우 보수적으로 접근한다.

그리고 제어시스템 관련 분야의 종사자 중 다수는 전기, 토목, 건설, 화학 등 다양한 전공을 가지고 있다. 컴퓨터 시스템에 대한 지식수준이 업무 수행과 큰 연관이 없어 보안 교육을 받기에 부족한 경우가 적지 않다. 마찬가지로 IT시스템 관련 종사자는 제어시스템의 특성에 대한 이해와 지식이 부족한 경우도 적지 않다.

이런 원인으로 제어시스템 분야에서 사이버 보안의 중요성이 강조되고 있지만, 그 역량을 강화하기가 매우 힘든 실정이다.

V. 제어시스템 사이버 보안 훈련 방안

5.1 해결하고자 하는 내용

우리는 앞서 기존의 교육훈련 동향을 조사하고 한계점을 분석하였다. 이 논문에서 해결하고자 하는 바는 다음과 같다.

- IT 전문가와 제어시스템 전문가 인식 괴리 해소
- 제어시스템의 특징이 반영된 훈련 환경 모델
- 훈련 효과 향상을 위한 기법 개발

5.2 제어시스템 사이버 보안 훈련 시스템

제어시스템 훈련 환경 모델

본 논문에서는 제어시스템의 형태·사이트·구축 시기 등에 따라 다른 구성을 가지는 제어시스템의 공통 요소를 포함하는 훈련 환경 모델을 개발하기 위하여, 제어시스템 분야에서 범용적인 표준으로 사용되는 IEC62443[7,17]에서 제시되는 참조 모델을 기반으로 하였다. 이를 바탕으로 현재 제어시스템에서 실 사용되는 요소를 도출하여 훈련을

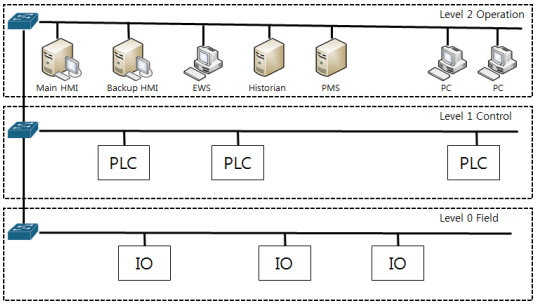

Fig. 6. Control System Training Model

위한 '제어시스템 훈련 환경 모델'을 개발하였다.

제어시스템을 구성하는 요소 중 Level2 Operation 영역에 속하는 시스템으로는 HMI(Human Machine Interface), EWS(Engineering Workstation), Historian DB(Database), PMS(Patch Management System), PC(Personal Computer)가 있다. 이 구성은 일반적인 제어시스템 환경의 구성요소를 선별한 것이므로, 훈련의 목적과 상황에 따라 추가하거나 제외할 수 있다.

각 구성요소의 역할은 다음과 같다. HMI는 제어시스템의 가동 상황을 모니터링하고 필요시, 적절한 제어를 수행하기 위한 시스템이다. EWS는 PLC(Programmable Logic Controller)의 로직 상태를 점검하고 업그레이드 등 유지보수를 위한 시스템이다. Historian DB는 제어시스템의 각종 센싱 값, 운영 상태 등의 기록을 위한 DB이다. PMS는 제어시스템에 존재하는 장치들의 패치를 관리하는 시스템이다. 마지막으로 PC는 운영자의 보고서 작성 등과 같은 일반 사무 업무를 위한 시스템이다.

Level1 Control 영역에 속하는 시스템으로는 PLC가 있다. 연결된 IO의 값을 모니터링하고 지정된 로직에 따라 판단하여 동작하는 제어 장치이다. 이 장치는 오퍼레이션 영역의 시스템의 제어 명령에 따라 물리적으로 동작하는 필드 장치를 제어하는 역할도 병행한다. 물론 이 영역에 속하는 장치 PLC 이외에도 DCS(Distributed Control System) 등 다양한 요소가 있지만 본 논문의 훈련을 위한 모델에는 포함하지 않는다.

Level0 Field 영역은 대부분 실제 물리 장치로 구성된다. 각종 센싱을 위한 센서 장치, 버튼, 그리고 동작을 위한 액추에이터가 그 범위에 속한다. 액추에이터는 대표적으로 Relay, Motor, Pump, Valve 등이 있다. 대부분의 제어시스템은 동작을 위한 액추에이터를 사용하지만 동작의 형태나 원리는 상기 예시로 든 장치와 유사하다.

제안하는 훈련시스템 구현

제어시스템 사이버 보안 훈련 시스템은 CPS의 기본 정의와 같이 가상 훈련환경과 물리장치의 연계로 구성된다. 그리고 이를 위한 인프라 부분이 있다. 개념도는 Fig. 7.과 같다.

제안하는 훈련 시스템은 훈련 운영의 효율성을 위하여 가상화하여 설계하였다. 가상환경 제공 장치는 가상 네트워크 환경(L3, L2 스위치 등)과 가상 시스템 환경(서버, PC 등)을 훈련 요구사항에 맞게 재구성하여 제공한다. 가상 시스템은 제시하는 제어시스템 모델의 Level2를 구현하며, 가상 네트워크는 모든 레이어에서 사용되는 인프라를 구성해 Level0-2를 구현한다. 물리장치는 제어시스템의 특성을 반영하기 위한 구성요소로 IO 장치가 설치된 Level0와 제어장치가 설치된 Level1의 영역을 구현한다.

가상환경은 일반적인 보안 교육 환경의 개인 차원의 교육 환경에서 기관 차원의 전산망 환경으로 확장된 훈련 환경을 제공 한다. 이를 통해 대외 서비스(Web 등)에 대한 위협에서부터 일반 사무환경의 보안 위협에 이르는 콘텐츠를 구현할 수 있다.

물리 환경은 제어시스템의 특성을 반영하기 위한 요소로, IT시스템에서의 보안 위협으로 인해 발생하는 제어시스템 피해에 대한 상황을 직관적으로 확인 할 수 있도록 할 수 있다.

훈련 환경은 시스템의 구성 요소도 중요하지만 그 내부를 구성하는 훈련 상황에 따른 서비스, 구성

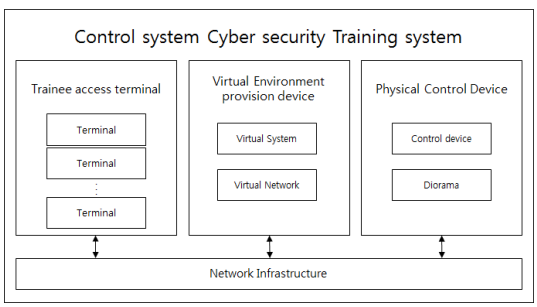

Fig. 7. Training System Concept

등이 중요하다. 본 논문에서는 실제와 같은 훈련을 수행하기 위하여 많은 분야의 실제 제어시스템을 분석하였고, 이를 바탕으로 각 분야에 맞는 서비스를 선별하였다. 또한 선별된 서비스와 분야에 맞는 제어 프로세스와, PLC 제어로직을 개발하고 액추에이터의 동작 형태를 설계하고 개발하였다.

구축한 환경의 일례로 Fig. 8.과 Fig. 9.의 정수처리 제어시스템이 있다. 정수처리 제어시스템은 연속 제조 공정의 부류에 속한다. 수원으로부터 원수를 채취하여 정수장에서 각종 여과공정을 거쳐 정수된 물을 생산하고, 각 가정에 공급한다. 정수를 위하여 다양한 공정이 있지만, 본 논문에서는 주요 제어 요소로 약품(염소) 투입 공정을 대상으로 하였다.

제어시스템은 지정된 조건에 따라 공정이 자동으로 운행되게 PLC 로직이 개발되었으며, 이와 연계되는 HMI에서 정수 상태의 모니터링과 각종 제어 행위를 실제와 같이 할 수 있도록 환경을 구축하였다. 또한 연계되는 물리 장치는 PLC와 최종 상태를 대상자가 명확히 인지 가능한 형태로 구축하였다.

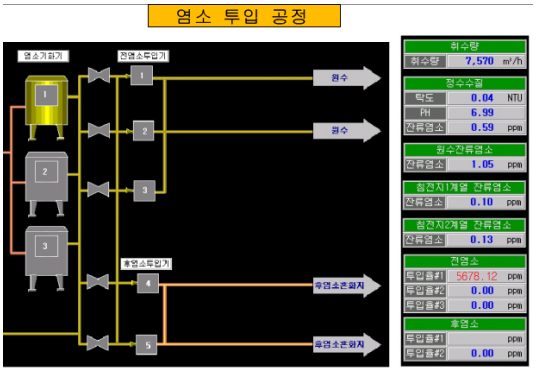

Fig. 8. HMI Chlorine Input Process

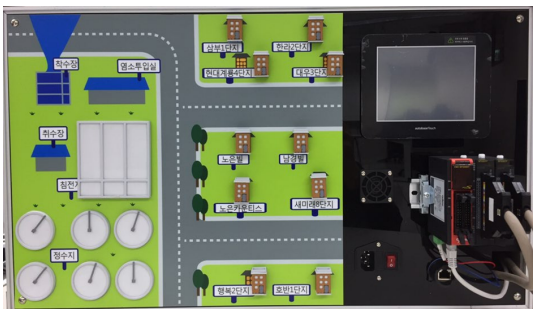

Fig. 9. Example of Physical Device

Table 3. Features of Suggested Training System

System / Feature	Traditional	Suggested
Physical Control Device	△	○
ICS Protocol	△	○
ICS Damage Effect	-	○

실제 제어시스템과 같은, 그리고 대상자가 훈련 상황 인지가 용이한 형태의 시스템을 구축하였다. 구성된 제어시스템 훈련 환경 하에서 사이버 보안 역량을 향상하기 위하여 본 논문에서는 제어시스템을 대상으로 벌어지고 있는 사이버 위협 사례들을 분석하여 위기 상황을 구현하였다.

구현 결과 Table 3.와 같이, 제안하는 시스템은 기존의 훈련 환경보다 제어시스템의 특성을 반영하였다. 제어시스템에서 사용되는 장비를 설치하여 기존에는 만족하기 어려웠던 제어시스템의 특성을 만족할 수 있도록 하였다. 이와 더불어 제어시스템에서 활용되는 프로토콜을 적용하여 현실성을 강화하였다. 마지막으로 제어시스템에서의 피해를 표현하여 대상자의 상황 인지와 몰입 효과를 강화하였다.

5.3 융합소통 훈련 기법

앞서 Ⅲ.제어시스템 사이버 보안 교육 동향에서는 사이버 보안 관련 교육 중 제어시스템과 관련된 내용을 언급하였다. 하지만 제어시스템이라는 특수한 환경에서의 사이버 보안 역량 강화라는 목적을 달성하기에는 어려움이 적지 않다. 이러한 어려움을 보완하기 위하여 본 논문에서는 기존 교육의 한계 요인을 분석하였고, 도출된 요인을 고려한 융합소통 훈련 기법을 제시한다.

교육학적 관점에서 톄이거루스와 메릴은 교수 변인을 교수 조건, 교수방법, 교수 결과의 세가지 범주로 분류하였다. 교수 조건은 교과 내용의 특성, 교수 목적, 제한점, 학습자의 특성이 있다. 교수방법에는 조직 전략과 전달 전략 그리고 관리 전략이 있다. 교수 결과는 수업의 효과성 수업의 효율성, 수업의 매력성이 있다. 이런 상호 관계를 고려하여 교수 모델을 형성하여야 한다[11].

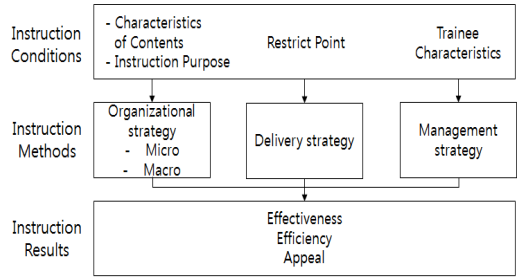

Fig. 10. Correlation between teaching conditions, methods, and outcome variables

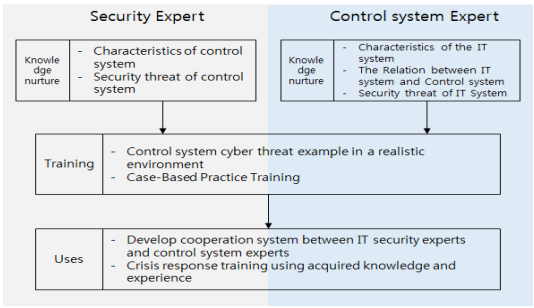

Fig. 11. Suggested Training Model

간략하게 예를 들면 교수 조건의 특성 또는 목적은 제어시스템 보안 역량의 강화를 위함이고, 제한점과 학습자의 특성은 대상자의 지식수준, 교육내용의 특수성을 들 수 있다. 상관관계 모델을 고려하여 다양한 교수 모델을 개발할 수 있다. 본 논문에서는 캘러 교수의 ARCS 모형을 바탕으로 한다. ARCS는 학습자의 학습 능력은 학습자의 특성과 교수 뿐 아니라 학습자의 동기와 밀접한 관계가 있다는 전제에서 개발된 모형이다. ARCS는 Attention(주의 집중), Relevance(관련성), Confidence(자신감), Satisfaction(만족감)의 첫 글자를 딴 모형이다[9-10]. 이 이론의 가장 중요한 요소는 학습자의 동기를 호기심, 그리고 자신감을 가지게 하는 것이라고 볼 수 있다.

융합소통 훈련기법은 교수-학습의 일반적인 상황에서 IT분야 보안전문가와 제어시스템 전문가의 협업 상황을 상정하고 있다.

기존의 교육훈련에서 대상자인 IT분야 전문가와 제어시스템 전문가가 제어시스템 보안 관련 교육에서 자신감과 흥미를 잃어버리는 가장 주요한 요소는 상호 분야에 대한 인식과 지식의 부족이 큰 부분을 차지한다. 인식과 지식의 부족으로 인해 훈련 내용에 대한 성취가 감소하고, 이는 다시 자신감의 감소, 흥미 감소라는 악순환의 고리를 형성한다.

따라서 대상자에게 자신감과 흥미를 유지하기 위해서는 충분한 기본 지식 제공해야 한다. 기본 지식을 바탕으로 보다 전문적인 지식에 대한 교육이 이루어질 때 자신감을 가지고 학습에 임할 수 있기 때문이다. 관련성은 훈련에 참가하는 행위로서 이미 만족 되었다고 판단할 수 있다. 현업과 연계되거나, 제어시스템 보안 분야에 관심이 있다고 추론할 수 있기 때문이다. 이러한 조건을 바탕으로 교육분야에서 검증되고 사용되고 있는 캘러 교수의 ARCS 모형을 융합소통 훈련 기법에 적용하였다.

융합소통 훈련 기법은 크게 세 단계로 구성되어 있다. 1단계는 지식 배양, 2단계는 제어시스템의 실제적인 위협 사례를 활용한 훈련, 3단계는 IT 분야 전문가와 보안전문가의 협업으로 위협 상황을 해결하는 활용단계이다.

1단계 지식 배양 단계는 상호 분야에 대한 기본적인 지식을 습득하는 것이다. 이 단계는 각 전문가들의 협업은 오히려 악영향을 유발할 우려가 있기 때문에 별개로 진행한다. 따라서 현장 강의도 가능하고 사전에 인터넷 강의나 도서의 형태로 진행할 수 있다.

지식 배양 단계가 끝나면 2단계인 훈련 단계에 진입한다. 훈련 단계에서는 1단계에서 습득한 지식을 바탕으로 상호 분야의 특성과 지식이 현장에서 어떻게 적용되고 있는지 확인한다. 또한 현업에서 자신의 업무보다 큰 개념의 관점을 획득하게 된다. 그리고 실제 사례에 기반 한 제어시스템 보안 위협 상황을 바탕으로 상호 소통을 통한 협력 방법을 습득한다. 이 과정을 통해 제어시스템 사이버 보안에 대한 자신감을 습득하고, 흥미를 유발한다.

3단계 활용 단계는 각 분야의 전문가들이 기존에 보유하고 있던 지식과 경험, 그리고 과정 중 습득한 지식과 경험을 조합하여 위기상황을 해결해 나가는 단계이다. 제시된 상황에 대한 IT 분야 보안 전문가와 제어시스템 전문가는 앞선 과정을 통해 조성된 상호 이해를 바탕으로 적절한 대응 방안을 모색한다. 이 과정을 통해 상호간의 괴리를 완화 할 수 있으며, 상대의 관점을 이해할 수 있다. 그리고 과정에서 습득한 지식과 상대방의 노하우를 체득할 수 있다.

5.4 교육훈련 시나리오

5.1에서 훈련 환경에 대한 소개와, 5.2에서 융합소통 훈련 기법에 대해 소개하였다. 여기서는 제안한 내용을 바탕으로 한 교육훈련 시나리오를 제시한다.

0단계 준비 단계

융합소통 훈련 기법을 적용하기 위하여 보안 전문가 군과 제어시스템 전문가 군을 분리한다. 군의 분류 기준은 참가자의 소속 기관, 담당 업무, 자신의 판단을 참고하여 1차 분류를 수행한다.

이후 1차 분류된 인원들에 대한 심층 문항을 통한 자가수준 진단을 통하여 각 분류의 적절성을 판단하며, 파악된 수준을 바탕으로 훈련을 위한 2차 분류를 수행한다. 효과적인 훈련을 위하여 2차 분류를 바탕으로 한 팀을 구성한다.

1단계 지식 배양 단계

지식 배양 단계에서는 준비 단계에서 분류된 결과를 바탕으로 보안 전문가 군과 제어시스템 전문가 군을 분리하여 교육을 실시한다. 이때 교육되는 내용은 각 군에 따른 특화된 내용과 2차 분류 시 파악된 참가자의 수준을 바탕으로 한다.

2단계 훈련 단계

훈련 단계에서는 지식 배양 단계를 통해 확보된 상호 분야에 대한 지식을 바탕으로 현장 상황을 상상하고, 서로 소통에 문제가 없도록 한다. 훈련 단계는 매우 많은 세부 시나리오가 존재하지만 간략하게만 제시하도록 한다.

- 무대 설정 : 훈련을 수행하는 훈련 환경에 대한 몰입감을 높이기 위하여, 대상 제어시스템에 대한 스토리를 부여한다. 그리고 참가자 간 역할을 할당하고 이에 따른 업무를 부여한다.
- 위협 설정 : 시나리오에 따른 담당 제어시스템의 위협 요소와 사례를 제시한다. 제시된 위협 요소가 발생했을 때, 각 참가자의 역할에 따른 대응 방법을 토의하고 모색한다.
- 대 응 : 주어진 훈련 환경에서 실제 위협이 발생하였을 때 보안 전문가와 제어시스템 전문가로 구성된 팀이 각자의 역할을 수행하고, 협동하여 위협을 대응하고, 침해 방지를 위해 훈련한다.
- 반 복 : 상기 훈련상황과 유사한 다른 위협에 대해 반복 훈련하여 대응 방법을 체득한다.

3단계 활용 단계

활용 단계에서는 상기 단계에서 습득한 내용을 바탕으로 주어진 상황에 대하여 대응할 수 있는 방법과 체계를 제시할 수 있도록 토론을 수행한다. 토론을 통하여 실무와 교육훈련 상황 간의 차이점을 논의해보고 실제적인 보안 방법에 대한 의견을 교류한다.

5.5 실험결과

우리는 논문에서 제시한 제어시스템 훈련환경을 2017년부터 적용하였으며, 훈련 기법은 2018년부터 적용하였다. 여기서는 그 운용 결과를 제시한다. 결과의 확인은 설문을 통해 이루어졌으며, 국가·공공기관 기반시설 제어시스템 관련 종사자를 대상으로 하였다. 다만, 참가자는 IT분야 종사자와 제어시스템 실제 운영자가 혼재되어 있다. 제시 결과는 2017년 7회 91명, 2018년 5회 54명 설문 응답 결과이다. 제시된 항목은 설문 중 결과를 추론해볼 수 있는 난이도, 만족도, 활용도이다. 난이도와 만족도를 통하여 참가자의 분야 간 인식 괴리의 해결 정도와 제시한 훈련 기법에 따른 학습 효과를 추론해볼 수 있다. 그리고 활용도 항목으로 학습의 효과와 실제 제어시스템 특성의 반영 정도를 추론할 수 있다.

각 항목은 상, 중, 하 3단계로 구성되어 있으며,

Table 4. Result of Survey

Item \ Year		2017	2018	Difference
Difficulty	H	14%	6%	-8%
	M	86%	93%	7%
	L	0%	1%	1%
Satisfaction	H	75%	85%	10%
	M	24%	15%	-9%
	L	1%	0%	-1%
Utilization	H	53%	65%	12%
	M	40%	30%	-10%
	L	8%	6%	-2%

결과를 통해 참여자가 체감하는 난이도가 전년 대비 적절한 것을 볼 수 있다. 만족도 역시 상승하였으며, 활용도는 비슷한 수준을 유지하고 있다.

결과를 분석해 보면 2017년도 대비 2018년도 난이도는 어렵다 8% 감소, 적절하다 7%로 증가, 쉽다 1% 증가하였다. 이 결과를 보면 2017년도 대비 참가자가 체감하는 난이도가 적절해진 것을 나타낸다. 이는 융합소통 훈련 기법을 적용하여 지식배양 단계를 각 분야의 전문가에 맞추어 진행한 것이 그 원인으로 판단된다.

만족도는 상 10% 증가, 중 9% 감소, 하 1% 감소하였다. 이 결과를 보면 2017년도 대비 참가자의 만족도는 전체적으로 향상된 것을 볼 수 있다. 이는 2018년도에 적용된 훈련 기법에서 지식배양을 통해 각 분야의 전문가들의 상호 이해를 이끌어내고, 이를 통해 흥미와 자신감을 강화한 결과 결과적으로 참가자의 훈련 만족도가 향상한 것으로 판단할 수 있다.

활용도는 훈련 시 습득한 내용의 현업 활용성에 대한 문항이다. 상 12% 증가, 중 10% 감소, 하 2% 감소하였다. 2017년과 2018년도에는 제어시스템의 특성이 반영된 훈련환경을 동일하게 제공하여 같은 조건이다. 그럼에도 활용도가 전체적으로 향상된 이유는 훈련 기법 적용을 통해 참가자의 이해도와 학습 효율이 증가하여, 현업의 환경에 적용할 수 있을 수준으로 지식이 배양된 결과라고 볼 수 있다.

상기 제시된 결과를 보면 제어시스템의 특성을 반영한 훈련 환경을 제공함으로써, 참여자의 흥미와 학습 효율을 향상시킬 수 있다. 하지만 2017년과 2018년의 비교에서 볼 수 있듯, 단순히 훌륭한 환경을 제공하는 것에 더하여, 훈련 기법도 중요하다는 결과를 확인할 수 있다.

Ⅵ. 결 론

본 논문에서는 기존의 IT분야 관점의 보안 교육을 활용한 '제어시스템의 사이버 보안 교육'의 어려움에 대해 원인을 분석해 보았다. 그리고 이 어려움을 완화하기 위하여 제어시스템 기반 사이버 보안 훈련 방안을 제시하였다. 실제 제어시스템 환경과 유사한 환경을 구축할 수 있는 제어시스템 사이버 보안 훈련 환경 모델과 시스템을 제시하고 구축하였다. 또한 IT 분야 전문가와 제어시스템 분야 전문가의 효율적인 협업을 위한 융합소통 훈련 기법을 제시하였다. 그리고 제안하는 훈련 환경과 기법을 활용하여 2017년부터 2018년까지 적용하여 비교한 결과, 제안하는 방법을 통해 각 분야의 전문가는 상호 분야에 대한 이해를 바탕으로 상호 협력하여 실제적인 제어시스템 사이버 보안을 강화할 수 있는 역량이 강화되었음을 추론할 수 있었다.

다만 연구를 수행하면서 일반 논문과 달리 교육훈련 분야의 특성에 따른 어려움으로 분석자료가 현장 강의 교수와 참가자의 의견, 설문 결과 등의 주관적인 내용이 주를 이루어, 객관화하여 제시하기 곤란한 면이 있었다. 같은 맥락으로 제시한 방법의 비교분석을 위한 수치화 가능 요소의 도출에 대한 어려움이 있었다. 향후에는 융합소통 훈련 기법과 훈련 시스템을 현장에 적용하여 대상자의 학습 성취도의 변화, 과정 진행의 효율성, 흥미 유발 등 학습 요소에 미치는 영향을 분석하고, 이를 보다 객관적으로 표현할 수 있는 방법에 대한 연구를 진행할 예정이다.

References

[1] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: a new frontier," in Proc. NSF Workshop on Cyber-Physical Systems, pp. 1-9, Oct. 2006.

[2] R. Poovendran, "Cyber-physical systems: close encounters between two parallel worlds," in Proc. IEEE, vol. 98, no. 8, pp. 1363-1366, Aug. 2010.

[3] Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST SP.800-82 Rev2, May 2015.

[4] "ICS-CERT Annual Assessment Report FY2016," ICS-CERT, 2016.

[5] A. P. Mathur and N. O. Tippenhauer, "SWaT : A Water Treatment Testbed for Research and Training on ICS Security," 2016 Int. Work. Cyber-physical Syst. Smart Water Networks, pp. 31-36, 2016.

[6] Daniele Antonioli, Hamid Reza Ghaeini, Sridhar Adequ, Martin Ochoa and Nils Ole Tippenhauer,

"Gamifying Education and Research on ICS Security: Design, Implementation and Results of S3," CPS'17, pp.93-102, Nov. 2017

〔7〕 Tyson Macaulay and Bryan Singer, "Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS," CRC Press, Nov. 2011.

〔8〕 Reigeluth, C. M., Merrill, M. D. "Classes of Instructional Variables," Educational Technology, pp.5-24, 1979.

〔9〕 John M. Keller, "Motivational Design for Learning and Performance: The ARCS Model Approach," Springer, Nov. 2009.

〔10〕 John M. Keller, "Development and use of ARCS model of instructional design," Journal of instructional development 10, pp.2-10. 1987.

〔11〕 Sook Hee Park and Myung Sook Yeom. "Educational Technology," Hakjisa, 2001.

〔12〕 ICS-CERT(NCCIC) https://ics-cert.us-cert.gov/Assessments

〔13〕 INL(Idaho National Laboratory) https://inl.gov

〔14〕 Control System Security Center http://www.css-center.or.jp

〔15〕 iTrust SUTD https://itrust.sutd.edu.sg/itrust-labs-home/itrust-labs_swat/

〔16〕 SANS https://www.sans.org

〔17〕 ISA https://www.isa.org/pdfs/autowest/phinneydone/

〈저자소개〉

김 경 호 (Kyeong-Ho Kim) 정회원
2010년 2월: 조선대학교 컴퓨터공학과 졸업
2012년 2월: 조선대학교 컴퓨터공학과 석사
2011년 12월~현재: ETRI 부설연구소 선임연구원
2019년 3월~현재: 충남대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 제어시스템 보안, 교육 훈련

맹 영 재 (YoungJae Maeng) 정회원
2006년 8월: 인하대학교 컴퓨터공학과 졸업
2008년 8월: 인하대학교 정보통신대학원 석사
2017년 2월: 인하대학교 컴퓨터정보공학과 박사
2012년 4월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 정보보호, 취약점 분석

장 문 수 (MoonSu Jang) 정회원
2002년 2월: 경성대학교 컴퓨터공학과 졸업
2005년 2월: 포항공과대학교 정보통신학과 석사
2015년 8월~현재: KAIST 전산학부 박사과정
〈관심분야〉 정보보호, 제어시스템, 취약점 분석

류 재 철 (Jae-Cheol Ryou) 종신회원
1985년 2월: 한양대학교 산업공학과 졸업
1988년 5월: Iowa State University 전산학 석사
1990년 12월: Northwestern University 전산학 박사
1991년 2월~현재: 충남대학교 컴퓨터공학과 교수
〈관심분야〉 정보보호, 인터넷보안, 암호학, 보안프로토콜