정 보 보 호 학 회 지
제27권 제2호, 2017. 4

사이버 물리 시스템 테스트베드 기술 연구 동향

최 승 오*, 김 우 년**

요 약

사이버 물리 시스템(CPS, Cyber-Physical Systems)은 높은 신뢰성, 실시간성, 자동제어 특성이 요구되는 기반시설 제조 및 생산, 교통 등 산업분야에서 널리 쓰이고 있다. 센서와 액츄에이터 등의 현장장치를 네트워크 기반으로 일정한 상태를 유지하도록 제어를 담당하는 산업제어시스템이 그 예이다. 하지만, CPS는 네트워크 기반 상호 연결이 증가함에 따라 각종 사이버 공격이 급증하고 있는 추세이다. 이에 따라, CPS 보안 기술 연구의 필요성이 대두되었고, CPS 보안 기술 연구개발에 반드시 필요한 기반 환경으로써, 사이버영영과 물리영역을 포함하는 CPS 테스트베드 기술 연구가 활발히 진행 중에 있다. 본 논문에서는 CPS 관련 테스트베드 기술 동향 분석에 앞서 표준 및 지침에 명시된 CPS 구조에 대해 분석하고, 기존에 연구된 CPS 테스트베드 기술을 CPS의 계층적 구조를 기반으로 구성요소 및 구성방법을 비교·분석한다. 또한, CPS 테스트베드와 연계한 제어프로토콜 지원 현황과 사이버공격 시나리오 특징을 분석한다.

Ⅰ. 서 론

사이버 물리 제어시스템(CPS, Cyber-Physical Systems)은 기반시설, 제조 및 생산, 교통, 빌딩 등의 분야에서 높은 신뢰성이 요구되거나 폐쇄적인 환경에서 사용되고 있다. 그러나, 최근에도 CPS인 산업제어시스템을 대상으로 한 사이버 공격이 급증하면서, 산업제어시스템에 특화된 보안 기술 연구의 필요성이 대두되고 있다. 하지만, 무중단으로 운영되어야 하는 산업제어시스템의 특성 상 보안기술 연구 및 시험을 위한 환경 마련을 위해 테스트베드 구축이 선행되어야 한다.

CPS 테스트베드는 산업제어시스템 시험환경을 제공함으로써 보안 기술 연구 뿐 만 아니라 취약점 점검 및 분석, 사이버공격 영향성 분석, 신규 보안기술 및 보안장비 검증, 제어시스템 보안 관련 훈련 및 교육 등 다양한 용도로 활용이 가능하다.

시험환경 확보의 필요성과 확보 후 폭넓은 활용이 가능하기 때문에 세계적으로 CPS 테스트베드 구축이 활발하게 이루어지고 있다. 미국의 경우, 에너지부(DoE, Dept. of Energy) 주도로 NSTB 프로그램을 통해 국립연구소가 테스트베드를 구축해서 취약점 평가 및 검증에 활용하고 있다. 또한, NIST 주도로 산업제어시스템 성능시험 테스트베드를 구축하여 가용성이 가장 중요한 산업제어시스템에서 보안기술이 성능에 미치는 영향을 분석하기 위한 목적으로 활용하고 있다. 그 밖에, 유럽의 경우 SCADA Lab 테스트베드를 구축하여 취약점 분석 연구를 수행하고 있으며, 일본도 취약점 분석, 제어시스템 보안 인증 시험환경, 제어시스템 보안 관련 훈련 및 교육용으로 7개 분야의 테스트베드를 구축하여 운영하고 있다.

본 논문에서는 CPS 구조 및 참조 모델을 통해 CPS 테스트베드 설계와 구축에 고려해야 할 구성 및 구조를 살펴보고 국외 CPS 테스트베드 구축 분야 및 목적을 분석한다. 또한, 국외 CPS 테스트베드 기술 연구 동향을 분석하여 해당 표준 및 지침에서 제시한 CPS 테스트베드 계층별 구성과 각 구성요소를 설명한다. 보안 기술연구를 위한 CPS 테스트베드 구성방법과 공격 시나리오 도출 사항을 비교하여 제시한다.

본 논문은 총 5장으로 구성되어 있다. Ⅱ장에서는 표준 및 지침을 기준으로 CPS 구조 및 참조모델에 대한 정의와 계층 분류에 따른 구성요소를 설명한다. Ⅲ장에서는 국외 CPS 테스트베드 구축 현황에 대해 설명한다. Ⅳ장에서는 국외 CPS 테스트베드 기술 연구 동향을 구축 분야 및 목적, 계층별 구성 요소 및 구축 방법에 따른 분

* ETRI 부설연구소 (sochoi@nsr.re.kr)
** ETRI 부설연구소 (wnkim@nsr.re.kr)

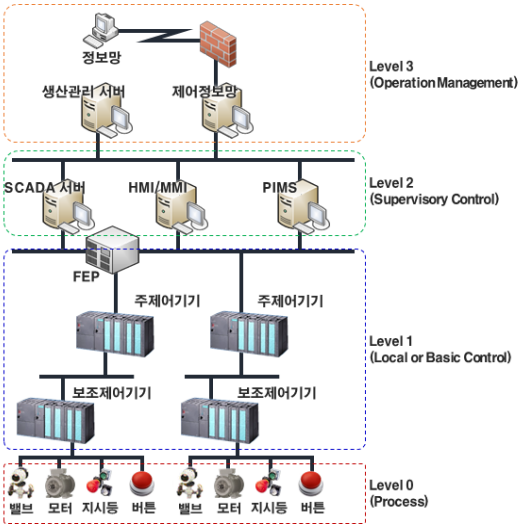
류와 사이버공격 시나리오 분석하여 비교한 결과를 제시한다. 마지막으로 V장에서 본 논문의 결론을 맺는다.

Ⅱ. CPS 구조 및 참조모델

본 장에서는 국외 CPS 테스트베드 설계 및 구축 시 고려할 사항을 관련 표준 및 지침 등에서 제시된 산업제어시스템의 구성, 구조, 참조모델 등을 기반으로 설명한다.

2.1. ISA/IEC-62443

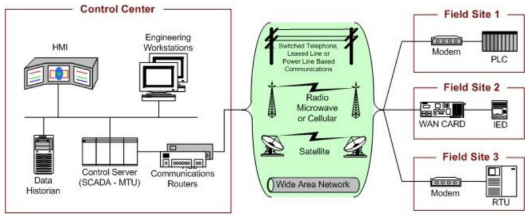
ISA/IEC-62443의 참조모델은 [그림 1]과 같이 총 4개의 레벨로 구성되어 있다. 레벨 0는 밸브, 모터, 센서 등의 현장장치로 구성되며 실제적인 물리 프로세스를 수행한다. 레벨 1은 기본제어를 수행하는 제어기기로 구성되며 레벨 0의 현장장치의 상태를 계측하여 물리 프로세스를 조작/제어하는 역할을 담당한다. 또한, 장애 발생 시 안전한 상태로 복구를 수행하는 안전 및 보호 시스템의 경우에도 이 레벨에 속한다. 레벨 2는 물리 프로세스 일체를 모니터링하고 제어하는 기능을 제공한다. 레벨 3는 운영관리를 위해 구체적인 장비 스케줄링, 신뢰성 보장 등을 포함하는 작업의 흐름을 관리를 수행한다.



〔그림 1〕 ISA-62443 산업제어시스템 참조 모델

2.2. NIST SP 800-82

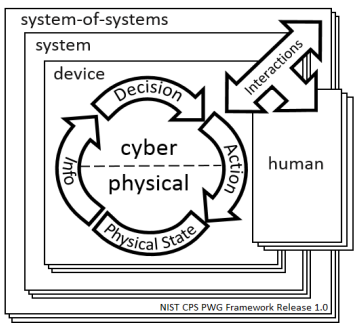
NIST Special Publication 800-82 'Guide to Industrial Control System Security'는 SCADA (Supervisory Control And Data Acquisition), DCS(Distributed Control System), PLC(Programmable Logic Controller), RTU(Remote Terminal Unit) 등 산업제어시스템의 구조와 구축 시 고려해야 할 보안 요구사항 및 통제지침을 포함하고 있다. [그림 2]는 SCADA 제어시스템의 일반적인 구조를 나타낸다. 본 지침은 산업제어시스템의 구성을 운영에 필요한 상태정보를 감시하고 제어할 수 있는 제어센터와 제어의 대상이 되는 컨트롤러 및 현장장치로 구성된 현장영역, 제어센터와 현장영역을 연결하는 네트워크 통신환경으로 구분하였다.



〔그림 2〕 NIST SP 800-82 제어시스템 구조

2.3. NIST CPS Framework

NIST 사이버 물리시스템 프레임워크(CPS Framework) 1.0을 공개했다. 본 문서는 CPS 구조를 사이버와 물리 계층 간 상호 정의된 프로세스를 수행하는 하나 또는 다수의 장치와 그 장치들이 모여 구성된 시스템, 시스템의 집합인 복합시스템(System of systems)으



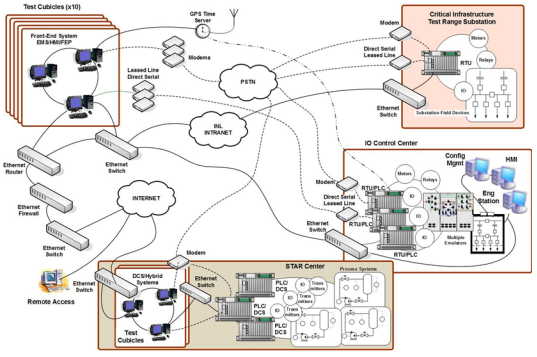
〔그림 3〕 NIST CPS Framework

로 구분했다. 각 구성요소는 상호간 연계동작과 의사 결정에 관여하는 사람간의 상호 작용도 포함된다. 특히, 장치는 물리적 상태를 제어하는 물리 영역과 제어 결정을 내리는 사이버 영역으로 구분된다. 물리 영역의 물리적 상태는 사이버 영역으로부터 전달받은 제어를 수행 후 상태 정보(예: 온도, 압력 등의 계측 정보)를 전달하여 사이버 영역 내에서 후속 제어 수행의 입력 값으로 사용하게 된다.

Ⅲ. 국외 테스트베드 구축 현황

3.1. 미국 NSTB(National SCADA Testbed)

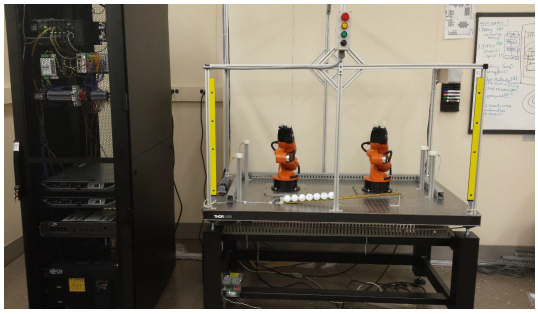
미국 국가 제어시스템 테스트베드(NSTB, National SCADA Testbed) 프로그램은 에너지부(DoE, Dept. of Energy) 주도로 전력, 에너지, 가스 분야에 도입 및 운영되는 제어시스템의 보안 강화를 목적으로 2003년부터 추진되었다. 2005년부터 2006년까지 17개 설비로 구성된 테스트베드를 구축했으며, 미국 내 6개 국립연구소(INL, SNL, PNNL, ORNL, ANL, LANL)를 중심으로 다양한 제어시스템에 대한 보안기술 연구 및 취약점 분석 업무 수행에 활용하고 있다. 특히, 아이다호 국립연구소(INL, Idaho National Laboratory)는 [그림 4]와 같이 테스트베드를 구성하여 제어시스템 취약점 점검 및 분석 수행에 테스트베드를 활용하였다.



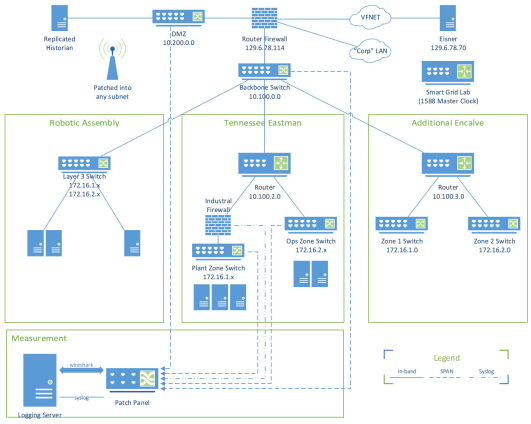
〔그림 4〕 아이다호 국립연구소(INL) 테스트베드 구성도

3.2. 미국 NIST ICS Cybersecurity Performance Testbed

산업제어시스템 사이버보안 성능 테스트베드(Industrial Control System Cybersecurity Performance Testbed)는 국제 표준 및 지침(예: ISA/IEC-62443, NIST Special Publication 800-82)에 규정된 요구사항에 대해 사이버보안 측면에서 산업제어시스템의 성능을 평가하기 위해 구축되었다. 본 테스트베드의 구축 방향은 [그림 5]와 같이 전체 플랜트 또는 시스템을 구축하지 않지만 실제 환경과 최대한 유사하게 구축하기 위해 에뮬레이션을 통해 산업제어시스템을 모사했다. 또한, 테스트베드를 활용한 산업제어시스템의 성능 평가를 위해서 개방 루프로 잘 알려진 테네시-이스트만 제어공정, 다수의 로봇 간 협업제어를 통한 조립공정, 광역네트워크(WAN) 환경에서의 배관 제어공정을 포함한 시나리오를 도출하였으며, [그림 6]과 같이 각 시나리오를 구분하여 네트워크를 구성했다. 특히, 테네시-이스트만 제어공정의 경우 산업제어시스템 성능시험을 위한 HIL(Hardware In the Loop) 방식의 시뮬레이터를 이용하여 제어프로토콜인 DeviceNet과 EtherNet/IP(CIP)를 이용하여 시뮬레이션을 수행할 수 있도록 구성했다.



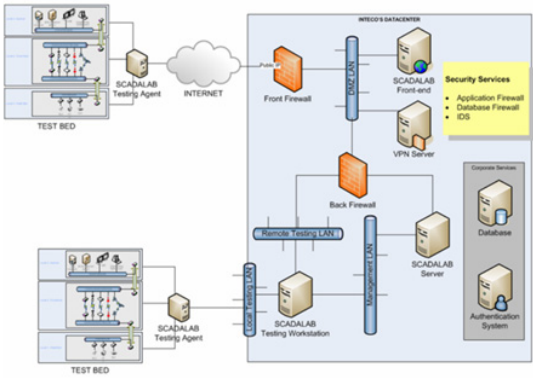
〔그림 5〕 로봇 간 협업제어 조립공정용 테스트베드 실사



〔그림 6〕 성능시험 테스트베드 네트워크 구성도

3.3. 유럽 SCADA Lab 테스트베드

유럽에서는 SCADA Lab 컨소시엄(헝가리, 이탈리아, 영국, 스페인 등 4개국 9개 기관)을 구성하여 제어시스템 테스트베드를 구축하였다. 구축된 테스트베드를 활용하여 에너지 분야 운영 환경 상의 보안 기술을 시험하였고, 취약점 분석을 목적으로 테스트베드부와 취약점 분석부를 별도로 구축하였다. [그림 7]은 SCADA Lab 테스트베드 구성도를 나타낸 것으로, 취약점 분석이 목적이므로 컨소시엄 참여기관이 원격 네트워크 접속이 가능한 환경을 제공하고 있다.

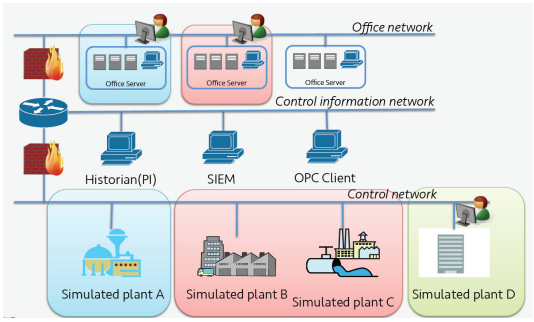


〔그림 7〕 SCADA LAB 테스트베드 구성도

3.4. 일본 CSSC

일본 제어시스템보안센터(CSSC, Control System Security Center)는 2013년 5월에 제어시스템 테스트베드를 갖춘 CSS-Base6를 개소했다. 일본 제어시스템보

〔그림 8〕 CSS-Base6 테스트베드



〔그림 9〕 CSS-Base6 테스트베드 구성도

안센터는 분야별 제어시스템 운영환경(컨트롤러 종류, 네트워크, 소프트웨어 등)이 상이한 점을 고려하여 분야별 제어시스템 테스트베드를 구축하였다. 이에 따라, [그림 8]와 같이 총 7개 분야(오폐수 처리, 빌딩제어, 조립공장, 화력발전소, 가스플랜트, 스마트시티, 석유화학공장)에 대해 제어시스템 테스트베드를 구축했다. CSS-Base6 구성은 [그림 9]와 같이 분야별 컨트롤러 및 현장장치와 운영 및 관리시스템이 별도로 구축하여 운영하고 있다.

Ⅳ. 국외 테스트베드 기술 연구 동향

본 장에서는 국외 CPS 관련 테스트베드의 구축 분야, 목적을 기준으로 관련 연구를 식별하고 해당 연구들에서 제안하고 구축한 테스트베드의 구성과 사이버보안 연구에 대해 분류 및 설명하고자 한다.

4.1. 테스트베드 구축 분야 및 목적

[표 1]과 같이 국외 CPS 테스트베드 구축 분야는 주로 산업제어시스템이 도입 및 운영 중인 에너지, 발전, 전력 분야에 집중적으로 진행되어 왔다. 특히, 전력 분야(Smart-grid, 송변전 등)를 대상으로 지속적으로 연구가 수행되었다. 최근 연구에서는 CPS 테스트베드 구축 분야가 다변화되어 빌딩제어분야(HVAC, Heating/Ventilation/Air Conditioning), 항공분야(무인항공), 산업제어분야(로보틱스) 등 그 범위가 점차 다양해지고 있다.

국외 CPS 테스트베드 구축 목적은 주로 사이버보안 이슈와 맞물려서 취약점 점검 및 분석, 사이버보안 기술이 CPS 환경에 미치는 영향, 산업제어시스템 담당자 훈련용, 학계의 교육용 등 매우 다양한 목적을 갖고 구축

〔표 1〕 국외 CPS 테스트베드 구축 분석 대상 관련연구

관련연구	게재년도	구축분야	목적
[1]	2008	수처리, 가스공급, 전력	취약점 점검, 보안장비 검증
[2]	2009	발전	연구용(테스트베드 통합 목적)
[3]	2011	발전	취약점 점검 및 분석, 사이버공격 시험환경
[4]	2011	화학제조, 가스공급, 전력(송변전), 공장자동화, 제철, 공기조화(HVAC)	사이버보안 취약점 분석 및 방안 연구, 교육용
[5]	2012	발전(보일러), 화학	사이버공격 연구 및 분석
[6]	2012	Smart-grid	사이버공격 연구 및 분석
[7]	2013	CPS 전 분야	CPS 연구 및 개발 환경
[8]	2013	발전, Smart-grid	사이버공격 연구 및 분석
[9]	2013	발전, 철도	사이버 공격 연구 및 분석
[10]	2012	CPS, WCPS	시험환경
[11]	2013	Smart-grid	연구용
[12]	2013	발전(보일러)	취약점 점검 및 분석, 제어프로토콜 및 장치 연구, 교육, 사이버공격
[13]	2014	전력(송변전)	사이버 공격 연구 및 영향성 분석
[14]	2014	전력(송변전)	취약점 점검 및 분석, 보완대책 연구, 교육 및 훈련
[15]	2015	전력(송변전)	NIDS 시험환경용, 시각화
[16]	2015	발전, 전력, 가스, 빌딩제어 등	사이버보안 교육 및 훈련
[17]	2016	항공(무인항공)	CPS 어플리케이션 시뮬레이션, 시험 및 분석
[18]	2015	발전	사이버 공격 연구 및 영향성 분석
[19]	2016	플랜트 설비	시험 환경 제공
[20]	2015	전력(송변전)	연구용
[21]	2016	전력(송변전)	사이버보안 연구, 데이터 셋 제공
[22]	2016	수처리	사이버보안 평가 및 취약점 분석
[23]	2016	발전	발전시스템 및 IEC61850 사이버보안 연구
[24]	2016	송변전	신규 기술 및 장비 시험
[25]	2016	자동제어 및 로보틱스	교육용
[26]	2016	수처리	연구용
[27]	2016	N/A	연구용
[28]	2016	발전	사이버 공격 연구 및 분석
[29]	2017	수처리	사이버 공격 연구 및 분석
[30]	2017	전력(송변전)	취약점 점검 및 분석, 교육 및 훈련

〔표 2〕 국외 CPS 테스트베드 구성

관련연구	운영 계층	제어 계층	물리 계층
[1]	Emulab	Simulink/Stateflow, DoD'sHigh-LevelArchitecture(HLA)	N/A
[2]	N/A	PowerWorld	VPST-R-local
[3]	실제 장치 및 시스템	EMS(Siemens), RTU(Siemens SiCAM), IED(Siemens SIPROTEC), 가상 RTU(DIgSILENT)	RTDS
[4]	HMI(GE/Fanuc iFix)	SCADAPack LP PLC.	모사장치, RTDS
[5]	Emulation(Emulab NS)	N/A	RT simulator(Simulink)
[6]	Windows based SCADA S/W	N/A	IED simulator
[7]	개방형 프레임워크	N/A	N/A
[8]	SCADA, HMI	S/W based RTU, IED 등	DIgSILENT, RTDS
[9]	HMI(ABB)	ABB PLC	Simulink
[10]	COOJA(Netwrok)	N/A	Simulink
[11]	N/A	N/A	RTDS
[12]	Emulab	DCS, PLC, RTU	Simulink
[13]	MATLAB/RSCAD	N/A	RTDS
[14]	OPNET	N/A	RTDS, RSCAD
[15]	N/A	PLC(Siemens S7-1200) 등	Simulink
[17]	N/A	Orbiter Space Flight Simulator, Kerbal Space Program	Beaglebone Black Boards
[18]	AGC Algorithm S/W	N/A	RTDS
[19]	HMI(RockwellAutomation Rsview32)	Embedded soft PLC (ES-PLC, KWSoftware GmbH.)	가상 플랜트 시스템
[20]	OPNET	N/A	RTDS
[21]	N/A	PMU(SEL-421, GE D60-1/D60-2, GE N60-1/N60-2, GE N60-3/N60-4)	RTDS
[22]	Emulator(CORE) 가상장치(MTU, HMI)	가상장치(RTU)	Python(Process) 가상장치(Sensor, Pump)
[23]	실제 장치 및 시스템	실제 장치 및 시스템	STM32-based I/O Simulation
[24]	LabView	N/A	실제 현장장치
[25]	N/A	Arduino	Simulink, Simscape
[26]	N/A	PLC(AB)	실제 현장장치
[27]	실제 장치 및 시스템	실제 장치 및 시스템	실제 현장장치
[28]	S/W(AGC Algorithm)	N/A	RTDS
[29]	HMI(iFIX5)	PLC(Schneider Modicon M340)	실제 현장장치
[30]	IED(SEL 351S)	N/A	OPAL-RT

이 되었다. 비록, 그 목적은 다를지라도 제안 기술이나 연구 검증, 보안 시험 및 평가하기 위한 CPS 시험환경이 필요한 것은 공통적인 특징이다.

4.2. 테스트베드 구성

2장에서 기술한 CPS의 구조 및 참조모델을 기반으로 CPS 테스트베드 구성 항목을 운영 계층, 제어 계층, 물리 계층으로 구분하였으며, 각 계통별 테스트베드 구성을 분석하여 [표 2]에 제시하였다.

4.2.1. 운영 계층

운영계층은 제어 계층간의 통신을 담당하는 장치 및 시스템과 제어 계층으로부터 전달받는 각종 정보(계측값, 제어상태, 이벤트 등)를 수집하고 표시하는 역할과 제어 계층으로 명령을 전달하여 물리 계층 내 구성요소로의 동작 상태를 변경할 수 있도록 [표 3]과 같이 제어 프로토콜을 지원하고 있다. 이러한 기능을 수행하기 위해 실제 장치 및 시스템을 사용하는 방식으로 구성한 연구보다 시뮬레이션 또는 에뮬레이션 소프트웨어를 이용하여 구성한 연구가 다수를 차지하였다. 시뮬레이션/에뮬레이션 도구는 Emulab, NS, OPNET, MATLAB, LabView 등의 소프트웨어를 사용하였다. 실제 장치 및 시스템으로 구성할 경우, 테스트베드의 실제 환경구성이 가능하지만 타 계층 간의 호환성을 고려해야하므로 구성의 유연성 저해와 구축 비용 증가될 수 있다. 반면, 시뮬레이션 또는 에뮬레이션을 이용할 경우, 환경 구성이 용이하고 비용 측면에서 유리하나 실제 환경을 충분히 반영하지 못하기 때문에, 연구 분야 및 목적을 고려하여 구축방안을 선택할 필요가 있다.

4.2.2. 제어 계층

제어계층은 물리 계층을 구성하는 장치의 감시, 계측, 제어 등의 역할을 수행하고 운영 계층으로 관련 정보를 전달한다. 제어 계층은 운영 계층과는 달리 실제 장치 및 시스템을 사용하여 테스트베드를 구성한 연구가 다수였다. 실제 장치로 구성한 경우, 주로 PLC, RTU와 같은 제어장치를 이용하여 구성하였으며 Siemens와 Allen-Bradley 등 다양한 제조사의 제품이 테스트베드 구축에 활용됨을 확인할 수 있다. 일부 연구에서는 Aduino나 소프트웨어를 통해 PLC나 RTU를 모사하는 방식을 사용하였다.

〔표 3〕 국외 CPS 테스트베드 제어프로토콜 지원 현황

관련연구	제어프로토콜 지원
〔1〕	Modbus/RTU, Modbus/ASCII, Modbus/TCP
〔3〕	IEC-61850 GOOSE, DNP3
〔4〕	Modbus/ASCII, Modbus/RTU, DNP3
〔5〕	Modbus/TCP, RPC/TCP
〔6〕	IEC-60870-5-103
〔7〕	IEEE 802.11, IEEE 802.15.4
〔8〕	DNP3, IEC-61850 GOOSE/MMS
〔9〕	Modbus, DNP3, RPC
〔10〕	IEEE 802.15.4, RPL(IETF, Routing Protocol for low power networks), CTP(Collection Tree Protocol)
〔13〕	IEEE 9 C37.118, Modbus
〔14〕	IEC-61850(GSE, SV, DNP)
〔15〕	Modbus/TCP
〔18〕	DNP3, IEEE 9
〔19〕	Modbus, OPC
〔20〕	Modbus/TCP
〔21〕	Modbus, DNP3, IEC-61850,IEEE C37.118
〔22〕	Modbus/TCP
〔23〕	IEC-61850 GOOSE
〔26〕	EtherNet/IP(CIP)
〔27〕	DNP3, Modbus/TCP, Profibus, Prfinet, WirelessHART, OPC
〔28〕	DNP3, IEEE 9
〔29〕	Modbus/TCP
〔30〕	SEL-C662, DNP3

4.2.3. 물리 계층

물리 계층은 센서, 액츄에이터 등의 현장장치와 현장장치 내 물리상태를 모두 포함한다. 물리 계층은 제어

〔표 4〕 국외 CPS 테스트베드를 활용한 사이버공격 시나리오

관련연구	CPS 공격 범위			공격 시나리오
	운영 계층	제어 계층	물리 계층	
[1]		●	●	DoS on sensors, Integrity attack, Phishing attack
[3]	●	●	●	Large scale DoS, Routing path failure/redundancies, Man-in-the-middle attack, Distributed/Coordinated attack, Malware propagation/infection
[5]		●	●	Min/Max value in short time period
[6]		●	●	Vulnerability scan, Man-in-the-middle attack
[8]	●	●	●	Malicious breaker trip, SCADA observability DoS, Remedial action scheme DoS
[9]		●	●	Packet forging attack, Control code rewriting attack, DDoS on the operation of the electrical grid and railway transportation
[13]	●	●	●	Shunt faults, Load variation, Load loss and recovery, Generator loss and recovery, Transmission line loss or recovery, Command injection attack, HMI/UI attack, Man-in-the-middle attack, Physical attack, Denial of service
[14]		●	●	Man-in-the-middle attack
[15]			●	Packet sequence & Packet cycle time gap changing the status of the circuit breakers
[18]		●	●	Measurement attack, Control attack
[20]		●	●	Man-in-the-middle attack, TCP SYN Flood DoS attack
[21]	●	●	●	Command injection attack, HMI/UI attack, Man-in-the-middle attack, Physical attack, DoS
[22]		●	●	DDoS, False data injection attack
[23]		●	●	False data injection, Spoofing GOOSE attack
[25]			●	Guidance control, Arm positioning control
[28]			●	Scaling attack, Ramp attack
[29]	●	●	●	Ping flooding, Modbus flooding, Actuators state modification, Sensor measurements modification, Fake exception response
[30]	●	●	●	Coordinated attack

계층으로부터 전달받은 명령을 수행하고 그 결과나 계측, 감시 정보를 제어 계층으로 전달한다. 물리 계층의 구성 방법은 주로 RTDS(Real Time Digital Simulation)를 이용한 실시간 기반 시뮬레이션과 Simulink를 이용한 물리 모델을 구현하여 현장장치를 대체하는 방법이 주로 사용되었다. 특히, 전력(송변전)분야에서는 현장장치 입/출력 신호를 생성하기 위해 RTDS를 대부분 활용했다. 이와 달리 수처리 분야의 경우 탱크, 펌프, 센서 등으로 구성된 실제 현장장치를 구축하여 물리 계층을 구성하였다.

4.3 테스트베드를 활용한 사이버공격 관련 연구

국외 CPS 테스트베드 기술 연구에서 테스트베드를 활용한 사이버공격 시나리오는 크게 무결성 공격과 가용성 공격으로 구성되어 있다. 대부분의 CPS 테스트베

드 관련 연구에서 제어 계층 및 물리 계층에서 발생 가능한 사이버공격 시나리오를 도출하였으며, DoS와 DDoS의 경우 기존 IT시스템의 사이버공격 대상과 달리 센서, 운영시스템, 제어 프로토콜을 대상으로 했다. 중간자 공격, 데이터 변조 공격의 경우, 제어 계층과 물리 계층 사이에서 송·수신하는 제어 명령, 계측 정보, 제어 프로토콜 내 정보가 변조의 대상이었다. 물리 계층 내 센서의 현재 상태정보와 다른 정보를 제어 계층으로 보냄으로써 정보 불일치로 인해 잘못된 명령이 제어 계층에서 물리 계층으로 전달되게 하거나 그 반대의 상황을 재현하여 공격하는 시나리오가 그 예이다.

Ⅴ. 결 론

본 논문에서는 CPS 구조 및 참조모델을 기준으로 국외 CPS 테스트베드 기술 연구 동향에 대해 살펴봤다. CPS 테스트베드의 구축 분야 및 목적, 계층별 테스트베드 구성 요소 및 방식, 사이버공격 관련 연구현황을 분석하였다. CPS 테스트베드는 연구 대상과 분야 및 구축 목적에 따라 서로 다른 구성 요소 및 방식을 가지고 있는 것을 확인하였다.

본 논문을 통해 제시한 CPS 테스트베드 기술 연구분류 기준으로 분야별 목적에 맞는 테스트베드 구축을 위해 사용 가능한 방법을 분석하여 향후 기술개발 시 객관적인 지표로써 활용될 수 있을 것이라 기대한다.

참 고 문 헌

[1] A. Giani, G. Karsai, T. Roosta, A. Shah, B. Sinopoli, and J. Wiley, “A testbed for secure and robust SCADA systems,” *ACM SIGBED Rev.*, vol. 5, no. 2, pp. 1-4, 2008.

[2] D. C. Bergman, D. Jin, D. M. Nicol, and T. Yardley, “The virtual power system testbed and inter-testbed integration,” *Proc. 2nd Conf. Cyber Secur. Exp. test*, no. August, p. 5, 2009.

[3] A. Ashok, A. Hahn, and M. Govindarasu, “A Cyber-Physical Security testbed for Smart Grid : System Architecture and Studies,” *Proc. Seventh Annu. Work. Cyber Secur. Inf. Intell. Res. ACM*, 2011., p. 20, 2011.

[4] T. Morris, R. Vaughn, and Y. S. Dandass, “A testbed for SCADA control system cybersecurity research and pedagogy,” *Proc. Seventh Annu. Work. Cyber Secur. Inf. Intell. Res. - CSIIRW ’11*, no. February, p. 1, 2011.

[5] B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera, “A cyber-physical experimentation environment for the security analysis of networked industrial control systems,” *Comput. Electr. Eng.*, vol. 38, no. 5, pp. 1146-1161, 2012.

[6] Y. Yang et al., “Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems,” *Sustain. Power Gener. Supply (SUPERGEN 2012), Int. Conf.*, no. July, pp. 1-8, 2012.

[7] M. Szczodrak, Y. Yang, D. Cavalcanti, and L. P. Carloni, “An Open Framework to Deploy Heterogeneous Wireless Testbed for Cyber-Physical Systems,” *Proc. IEEE SIES Symp., no. Sies*, pp. 215-224, 2013.

[8] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, “Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid,” *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847-855, 2013.

[9] C. Siaterlis, B. Genge, and M. Hohenadel, “EPIC: A testbed for scientifically rigorous cyber-physical security experimentation,” *IEEE Trans. Emerg. Top. Comput.*, vol. 1, no. 2, pp. 319-330, 2013.

[10] B. Aminian, “GISOO : A Virtual Testbed for Wireless Networked Control Systems,” *39th Annu. Conf. IEEE Ind. Electron. Soc.*, no. August, pp. 5588-5593, 2012.

[11] T. Yardley, R. Berthier, D. Nicol, and W. H. Sanders, “Smart Grid Protocol Testing Through Cyber-Physical Testbeds,” *2013 IEEE PES Innov. Smart Grid Technol. Conf.*, pp. 1-6, 2013.

[12] H. Gao, Y. Peng, K. Jia, Z. Dai, and T. Wang, “The design of ICS testbed based on emulation, physical, and simulation (EPS-ICS Testbed),” *Proc. - 2013 9th Int. Conf. Intell. Inf. Hiding*

Multimed. Signal Process. IIH-MSP 2013, pp. 420-423, 2013.

[13] U. Adhikari, T. H. Morris, and S. Pan, "A cyber-physical power system test bed for intrusion detection systems," *2014 IEEE PES Gen. Meet. | Conf. Expo.*, pp. 1-5, 2014.

[14] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," *2014 North Am. Power Symp. NAPS 2014*, pp. 1-6, 2014.

[15] G. Koutsandria, R. Gentz, M. Jamei, A. Scaglione, S. Peisert, and C. McParland, "A Real-Time Testbed Environment for Cyber-Physical Security on the Power Grid," *Proc. First ACM Work. Cyber-Physical Syst. and/or Priv.*, pp. 67-78, 2015.

[16] S. Shin, "A S tatus of Control System Security in Japan," *2015 10th Asian Control Conf.*, pp. 1-4, 2015.

[17] P. S. Kumar, W. Emfinger, and G. Karsai, "A testbed to simulate and analyze resilient cyber-physical systems," *Proc. - IEEE Int. Symp. Rapid Syst. Prototyping, RSP*, vol. 2016-Febru, pp. 97-103, 2016.

[18] A. Ashok, P. Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber attacks on Automatic Generation Control using a CPS Security Testbed," *IEEE Power Energy Soc. Gen. Meet.*, vol. 2015-Septe, 2015.

[19] W. Dai, P. Zhou, D. Zhao, S. Lu, and T. Chai, "Hardware-in-the-loop simulation platform for supervisory control of mineral grinding process," *Powder Technol.*, vol. 288, pp. 422-434, 2016.

[20] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed," *Proc. - CQR 2015 2015 IEEE Int. Work. Tech. Comm. Commun. Qual. Reliab.*, 2015.

[21] U. Adhikari, T. MORRIS, and S. Pan, "WAMS Cyber-Physical Test Bed for Power System, Cybersecurity Study, and Data Mining," *IEEE Trans. Smart Grid*, vol. 3053, no. c, pp. 1-1, 2016.

[22] A. Tesfahun and D. L. Bhaskari, "A SCADA Testbed for Investigating Cyber Security Vulnerabilities in Critical Infrastructures," *Autom. Control Comput. Sci.*, vol. 50, no. 1, pp. 54-62, 2016.

[23] M. Kabir-Querrec, S. Mocanu, J. M. Thiriet, and E. Savary, "A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks," *IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA*, vol. 2016-Novem, pp. 1-4, 2016.

[24] S. Adhikari, "Application of LabView as real time SCADA in power system transmission line," *Int. J. Appl. Eng. Res.*, vol. 11, no. 7, pp. 5028-5031, 2016.

[25] I. Tejado, J. Serrano, E. P??rez, D. Torres, and B. M. Vinagre, "Low-cost Hardware-in-the-loop Testbed of a Mobile Robot to Support Learning in Automatic Control and Robotics," *IFAC-PapersOnLine*, vol. 49, no. 6, pp. 242-247, 2016.

[26] 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.

[27] B. Green, D. Hutchison, S. A. F. Frey, and A. Rashid, "Testbed diversity as a fundamental principle for effective ICS security research," *SERECIN*, 2016.

[28] A. Ashok, S. Sridhar, A. D. McKinnon, P. Wang, and M. Govindarasu, "Testbed-based performance evaluation of attack resilient control for AGC," *Proc. - 2016 Resil. Week, RWS 2016*, pp. 125-129, 2016.

[29] G. Bernieri, E. Etchevés Miciolino, F. Pascucci, and R. Setola, "Monitoring system reaction in cyber-physical testbed under cyber-attacks," *Comput. Electr. Eng.*, vol. 0, pp. 1-13, 2017.

[30] S. Poudel, Z. Ni, and N. Malla, “Real-time cyber physical system testbed for power system security and control,” *Int. J. Electr. Power Energy Syst.*, vol. 90, pp. 124-133, 2017.

〈저 자 소 개〉

사 진

최 승 오 (Seungoh Choi)
비회원

2012년 2월 : 아주대학교 정보및컴퓨터공학과 졸업
2014년 2월 : 아주대학교 컴퓨터공학과 공학석사
2013년 12월~현재 : ETRI 부설연구소 연구원
관심분야 : SCADA 보안, 제어시스템 보안, 제어 프로토콜 퍼징, 네트워크 보안

사 진

김 우 년 (Woo-Nyon Kim)
정회원

1996년 2월 : 안동대학교 컴퓨터공학과 졸업
1998년 2월 : 경북대학교 컴퓨터과학과 이학석사
2000년 2월 : 경북대학교 컴퓨터과학과 박사수료
2000년 3월~2003년 12월 : ㈜니츠 선임연구원
2003년 12월~현재 : ETRI 부설연구소 책임연구원/실장
관심분야 : 기반시설보안, SCADA 보안, 제어시스템 보안, 취약점 분석, 네트워크 보안