情 報 保 護 學 會 誌
第22卷 第5號, 2012. 8

제어시스템용 테스트베드 구축 방안

김 지 홍*, 유 천 영**, 김 성 용***

요 약

국가기반산업분야에 사용되고 있는 제어시스템은 원자력・화학 등의 에너지산업과 수자원, 교통 신호등의 다양한 제어 분야에서 사용되고 있다. 지금까지 폐쇄적으로 운용되었던 제어시스템은 최근에는 경영시스템과의 상호연동성 및 제어시스템 간의 상호운용성등으로 인하여 점차 외부로 노출되고 있기 때문에 사이버 테러리스트의 공격 목표가 되고 있다. 실제로 사이버전쟁 발생 시에는 제일 처음의 목표가 국가기반의 산업용 제어시스템이 될 수 있으며, 해커나 공격자 등에 의한 공격으로 엄청난 재앙이 발생될 수 있다.

본 논문에서는 제어시스템에 대한 보안취약점으로 일반 IT 정보 시스템에서의 보안이슈와 함께, 제어시스템에서 사용되는 제어용 소프트웨어에 대한 보안이슈를 다루고, 이러한 보안 취약성을 분석・평가하기 위한 제어시스템용 테스트베드 구축방안을 제시하고자 한다.

Ⅰ. 서 론

제어시스템은 전력, 화학, 원자력 등 국가기반 및 대규모 산업플랜트를 운영관리하기 위하여 필수적으로 사용되는 시스템으로 센서, 제어 계통, 통신망 및 컴퓨터 등으로 구성되어 있다. 또한 IT 기술의 발달로 인하여, 기존의 폐쇄망으로 구성된 산업플랜트의 네트워크망 관리의 효율화와 제어시스템 간의 상호연동, IT 정보시스템을 이용한 효율적인 관리을 위하여 점차 개방화되고 있는 추세이다. 그러나 보안 정책이나 보안 대책을 고려하지 않고, 편의성만을 고려하여 원격제어 기능을 추가하는 것은 국가기반 제어시스템에 대한 치명적인 보안 위협을 초래할 수 있다.

실제로 국가 기간 제어시스템에 대한 보안침해 사례를 살펴보면, 2003년 1월 25일에 발생된 슬래머 웜으로 인하여 오하이오 Davis-Besse 원자력 발전소의 안전 모니터링 시스템이 5시간동안 중단되었으며, 알카에다 교육 훈련소에서 발견된 컴퓨터에 댐과 관련된 SCADA 정보가 발견되었으며, 미국의 가스 시설 내에 모니터링 및 제어가 되지 않은 가스 설비의 오작동으로 인하여 3개의 설비가 장애를 일으킴으로서 약 450억원의 피해가 발생되었다. 최근 이란에서는 스턱스넷으로 인하여 6만대 이상의 컴퓨터를 감염시키고 핵시설 등 산업 기반시설의 원격 통합 감시제어시스템까지 피해를 입혔던 사례가 있다[9].

이와 같이 제어시스템에 대한 보안침해는 재산적인 손실 뿐 아니라, 국가 산업기반이 마비되는 형태로 사회 전체에 혼란을 야기 시키는 경우도 발생할 수 있다.

본 논문은 다음과 같이 구성된다. 2장에서는 기본적인 제어시스템에 대한 개요와 제어용 통신프로토콜을 설명하고, 3장에서는 제어시스템에서의 보안이슈를 다룬다. 4장에서는 제어시스템용 테스트베드 구축방안을 다루며, 마지막으로 결론으로 마무리한다.

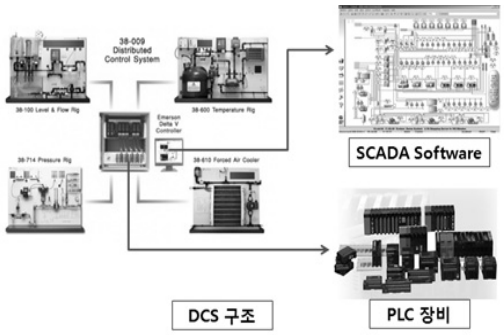
Ⅱ. 제어시스템 개요

2.1 제어시스템 구성

산업자동화(Industrial Automation)는 크게 공정자동화(Process Automation)와 공장자동화(Factory Automation)로 구분된다. 공정자동화 기기는 DCS(Distributed Control System), 공장자동화 기기는 PLC (Programmable

* 세명대학교 정보통신학부 (jhkim@semyung.ac.kr)
** 세명대학교 대학원 전산정보학과 (soliebe1@semyung.ac.kr)
*** 세명대학교 정보통신학부 (ksy4765@lycos.co.kr)

Controller)로 분류하고 있으나, 최근에는 PLC의 기능이 고도화 됨에 따라 DCS와 PLC의 구분이 거의 없다. [그림 1]은 일반적인 제어시스템의 구성을 보여준다.



〔그림 1〕 일반적인 제어시스템

2.1.1 DCS

DCS (Distributed Control System)는 분산제어시스템으로서 고성능 소프트웨어기술, 측정제어기술, 고성능데이터 전송 기술을 이용해 정보, 제어분야에서 전 세계적 추세인 소형화, 개방화를 이뤘다. 또한 사용자의 편의를 위해 HMI(Human Mach interface)를 통합하였고, 표준화를 지향하기 위해 IEC-131-3 표준 언어를 RCS에 탑재하여 로직, 루프 처리가 필요한 플랜트 제어를 보다 쉽게 처리할 수 있다.

DCS는 프로세스 정보처리 및 운전 조작, 컴퓨터들의 관리기능 등을 주 컴퓨터에 집중화시킴으로서 자료처리 및 운영관리를 원활하게 하는 특징을 가지고 있다. 주요 기능으로는 실시간 처리 및 고속의 데이터를 전송하는 System Interface, 양방향 통신 및 신뢰성과 확장성을 가지는 Process Interface, 감시하기 위한 상태표시장치 및 HMI기능을 강화시키는 Operator Interface 등이 있다.

2.1.2 PLC

PLC(Programmable Logic Controller)는 디지털 또는 아날로그 입출력 모듈을 통하여 로직, 시퀀싱, 타이밍, 카운팅, 연산과 같은 특수한 기능 등을 수행하기 위해 프로그램 가능한 메모리를 사용하여 여러 종류의 기계나 프로세서를 제어하는 디지털 동작의 전자 장치로서 안정성과 호환성이 높은 것이 특징이다. 일반적으로 RTU(Remote Terminal Unit) 이상의 기능을 가지며 사용하는 통신 매체에 따라 1:1 또는 1:N 연결이 가능하다.

2.2 SCADA

일반적으로 제어시스템을 SCADA(Supervisory Control And Data Acquisition) 시스템이라 부른다. SCADA 시스템의 구성은 PLC들로 구성된 MTU(Main Terminal Unit)와 RTU, 통신장비 및 SCADA 소프트웨어로 구성된다.

SCADA 소프트웨어는 통신 경로상의 아날로그 또는 디지털 신호를 사용하여 원격장치(RTU)의 상태정보 데이터를 수집, 수신·기록·표시하여 중앙 제어 시스템이 원격 장치를 감시 제어하는 시스템으로서 일반적으로 소프트웨어로 구성되어있다. 주요기능은 원격장치의 경보 상태에 따라 미리 규정된 동작을 실행하는 경보기능, 원격외부 장치를 선택적으로 수동 및 자동 또는 수·자동 복합적으로 동작하는 감시 제어기능, 그리고, 원격 장치의 상태 정보와 디지털 정보를 수신 및 합산하여 표시·기록하는 지시·표시 기능 등이 있다[1].

MTU는 SCADA를 이용하여 네트워크상의 하위레벨에 있는 모든 RTU를 제어 및 모니터링할 수 있다. 일반적으로 RTU는 현장 데이터 수집 및 제어용 계기로서 그 용량은 처리 가능한 포인트의 수로 표시된다. 현장의 데이터를 수집하여 전용선 또는 공중선을 통하여 MTU로 전송하는 역할을 한다.

2.3 산업용 프로토콜

Modbus는 MTU와 RTU사이의 정보 교환 및 상호운영성을 확립하기 위해 1978년 모디콘(Modicon)사에 의해 개발된 프로토콜로서 통신 매체에 따라 다른 통신방식을 사용해야 하고, MTU를 중심으로 Master/Slave 방식을 이용한 반 양방향 통신이 특징이다.

1979년 Hung Yu가 만든 MODiconBUS 프로토콜은 초기 산업용 데이터 네트워크 중의 하나인 모드버스로 Modicom PLC를 위해 고안된 반 양방향 시리얼 통신 프로토콜이며, 결정성(determinant)은 높았지만 시리얼 통신이기 때문에 속도가 매우 느리다.

DNP(Distributed Network Protocol)는 제어시스템을 위해 설계된 표준통신 프로토콜로서, RTU, IED

(Intelligent Electronic Device)와 마스터 스테이션 사이의 상호 운영성을 확립하기 위하여 개발된 개방형 프로토콜이다. DNP는 1990년 Westronic, Inc 에 의해 최초로 개발되었고, 1994년에 DNP 3.0으로 일반에 공개되었다[2].

EtherNet/IP는 Allen-Bradley 컨트롤 라인을 위해 로크웰 오토메이션이 개발한 것으로, 원래 비결정성 데이터 전송을 위해 고안된 것이지만, 표준 이더넷이나 TCP/IP 보다 훨씬 안정적이고 결정성이 있는 것으로 알려져 있다[3].

2.2.1 ModbusTCP

ModbusTCP는 전 세계적으로 PLC 등에 널리 사용되고 있는 직렬 통신 프로토콜이다. TCP/IP 네트워크상에서 수행되며, 현재 원격 디지털 입/출력 컨트롤이 가능한 제품들에 사용되고 있다. ModbusTCP는 이더넷 포트용과 직렬 포트용으로 구분되고, 사용 시 기본적으로 제품의 이더넷 포트를 이용해야 한다. 하지만 사용자에 따라 시리얼 포트를 이용해 장비들을 제어/감시하는 경우가 있어 직렬 ModbusTCP가 개발되었다.

2.2.2 DNP3

DNP는 자동제어시스템에서 구성 요소간에 사용되는 통신 프로토콜로서 Modbus와 더불어 SCADA시스템에서 많이 사용되고 있다. DNP3는 OSI 7 Layer Model을 참조하여 만들었기 때문에 확장성과 호환성이 좋고 다양한 매체에서 같은 동작이 가능하며 오류 발생시 자동 재전송 기능이 있는 것이 특징이다. 기본적으로 폴링 방식, XR방식, 브로드캐스팅 방식이 지원되기 때문에 환경에 따라 최적화된 통신을 할 수 있으며 SCADA 시스템 소프트웨어를 통하여 다양한 데이터 객체를 사용자가 손쉽게 구현 및 수정할 수 있다[2].

Ⅲ. 제어시스템에서의 보안 이슈

3.1 네트워크 보안 이슈

네트워크 보안취약점은 제어시스템 네트워크를 구성함에 있어서 고려되어야 할 보안취약점을 말한다. 일반적인 네트워크 구성 시에 고려하여야 할 보안정책과 관련하여, 네트워크 구성에 대한 이해와 보안영역을 설정하여야 한다. 또한 외부로부터 악성코드가 투입되는 것을 막기 위하여, 인가자 외에 대한 불법접근을 차단하기 위한 접근통제 정책과 방화벽 및 네트워크 침입차단 정책을 설정/구현하여야 한다[10].

또한 무선네트워크를 사용할 경우에는 무선 네트워크를 통한 불법접근을 막기 위하여 AP에 대한 인증기능이나 암호화 기능이 필요하다. 기타 물리적인 보안방안으로 네트워크의 이중화 및 물리적인 보안방안이 고려되어야 한다. 기타 제어시스템에서 주로 사용되고 있는 MTU와 RTU간의 제어 프로토콜, 제어망간의 Ethernet /Serial 통신 등의 통신방식에 대한 보완이 필요하다.

3.2 시스템 보안 이슈

제어시스템과 관련된 보안이슈는 소프트웨어 및 제품 보안취약점과 설정 및 운용상의 보안취약점으로 구분할 수 있다.

소프트웨어 및 제품 보안 취약점은 제품이 자체적으로 가지고 있는 보안취약점을 말한다. 크게 운영체제와 각종 응용프로그램의 취약성과 보안기능의 미흡으로 인한 보안 취약점으로 분류할 수 있다.

운영체제 및 각종 응용 프로그램의 취약점은 IT 정보시스템과 달리 제어시스템에서는 다양한 운영체제를 사용하고 있기 때문에 사용하고 있는 운영체제별로 입력값에 대한 검증기능, 취약한 함수/기법 사용 및 에러처리에 대한 미흡 등으로 보안취약점이 발생될 수 있다. 또한 보안기능 부분으로는 인증기능과 데이터 무결성 검사 기능, 암호/해쉬 알고리즘의 미흡함으로서 발생될 수 있다.

설정 및 운용상의 보안 취약점은 제품 설치후의 제어시스템 운용을 위하여 관리자에 의해 발생될 수 있는 보안취약점을 말한다. 크게 제어시스템 운용을 위한 설정과 관련된 보안취약점과 실제 운용상의 보안취약점으로 구분할 수 있다.

설정상의 보안취약점은 중요화일에 대한 접근제한, 인증정보 관리 및 설정, 로그기록 및 분석, 불필요한 서비스 포트를 개방함으로서 발생될 수 있으며, 기타 운용상의 보안취약점은 보안패치 및 백업, 백신소프트웨어

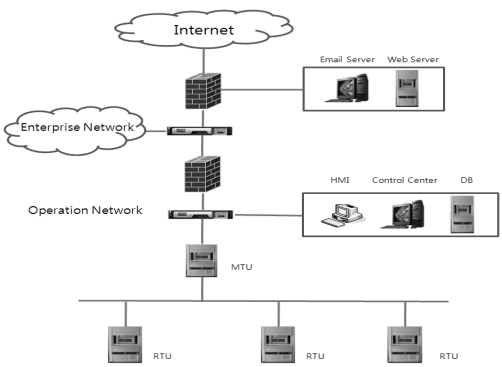
설치 및 업데이트, 보안정책에 대한 계획 및 절차, 자산관리, USB 등의 저장매체에 대한 접근통제로 인하여 발생될 수 있다[10].

Ⅳ. 제어시스템용 테스트베드 구축방안

산업용 제어시스템을 테스트하기 위한 테스트베드 구축방법으로 다음과 같은 세 가지 형태로 분류할 수 있다.

1. 통합형 테스트베드
2. 산업 유형별 테스트베드
3. 제어프로토콜 테스트베드

통합형 테스트베드의 구성은 네트워크 전반의 일반적인 보안 취약점을 고려한 제어시스템의 형태로서, 크게 인터넷, 엔터프라이즈 네트워크, 제어시스템 운영 네트워크로 구분된다. 기존에 폐쇄형으로 운영되었던 제어시스템들이 최근에는 원격관리를 위하여 엔터프라이즈 네트워크 뿐 만 아니라, 외부 인터넷과 연결하여 사용하는 경향이 높다. 그러므로 [그림 2]와 같이 기업내부의 엔터프라이즈 네트워크와 인터넷으로 연결하는 형태로 구성된다.



〔그림 2〕 일반적인 산업기반 제어시스템

외부 인터넷을 통한 기업 내의 연결은 1차 방화벽에 의하여 기업 내의 네트워크의 접근 및 제한된 서비스만이 가능하며, 중앙제어실 및 기관실 등의 중요 기관의 연결은 2차 방화벽에 의한 제한된 접근이 가능하게 구축한다.

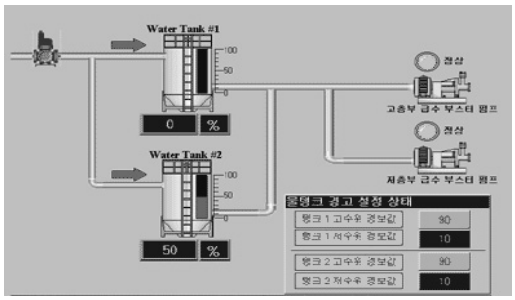
산업 유형별 테스트베드는 산업별로 다양한 기기를 효율적으로 감시 및 제어하기 위해 [표 1]과 같이 제어유형에 따라 구분하여 모델별로 테스트베드 구축할 수 있다.

〔표 1〕 산업유형 별 테스트 항목

세부 분류	테스트 항목
수조제어 시스템	물탱크, 정유탱크 관리시스템
급수탑 시스템	상수도, 급수시설 관리시스템
가스관 시스템	상하수도관, 송유관등 관로시스템
컨베이어 제어시스템	공장 및 공정자동화 시스템
감시시스템	전력제어, 설비감시제어시스템

4.1 수조제어 시스템

수조(water tank) 제어시스템은 석유화학 정제과정인 오일 저장 탱크로의 원유 전달 과정과, 오일을 정제기로 일정하게 공급하는 과정을 시뮬레이션 할 수 있는 테스트베드이다.



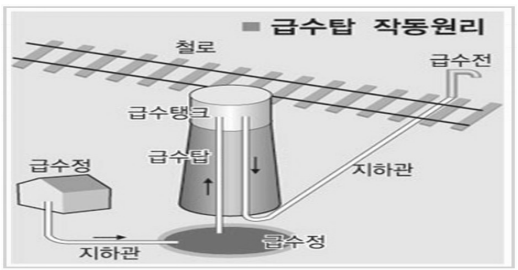
〔그림 3〕 수조 제어시스템의 예〔4〕

위의 과정을 오일 대신 물을 이용하여 모형화시킨 수조제어시스템은 두 개의 물탱크 구조와 물탱크간의 물의 흐름을 제어하기 위한 솔레노이드 밸브, 펌프 등으로 구성한다. 수조내의 물의 수위를 나타내는 수위 센서와 펌프 등의 액츄에이터를 구동하기 위한 설정값 레지스터, 그리고, 시스템 및 펌프, 수위 센서 상태 레지스터를 구분하여 확인할 수 있다.

4.2 급수탑 시스템

상수도 및 댐 관리 시스템 같은 물 분배시스템에서의 일정한 수압을 제공하기 위해 사용되는 급수탑을 모형

화한 테스트베드이다.

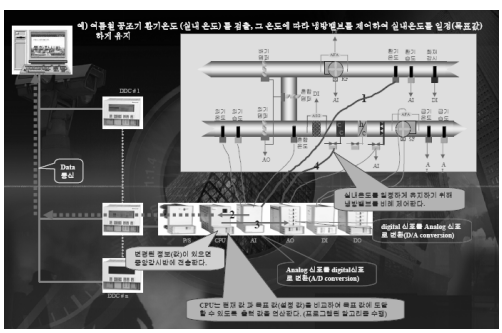


〔그림 4〕 급수탑 시스템의 예〔5〕

급수탑내의 물의 수위를 나타내는 수위 센서와 펌프, 타운하우스 전등 등을 액츄에이터를 이용하여 구동하기 위한 설정값 레지스터, 그리고, 시스템 및 펌프·수위 센서·타운하우스 상태 레지스터를 구분하여 확인할 수 있다.

4.3 가스관 시스템

가스관(gas pipeline) 제어시스템은 천연가스를 전달하기 위한 가스관 혹은 온수를 전달하기 위한 냉난방시스템 등에 사용되는 파이프라인 제어시스템을 모형화한 것이다.



〔그림 5〕 파이프라인 제어시스템의 예〔6〕

이 시스템을 제어하기 위해서는 파이프라인을 통과하는 유체의 압력, 온도 등을 나타내는 센서와 유체를 공급하기 위한 펌프, 적정량을 규제하기 위한 밸브 등을 액츄에이터를 이용하여 구동하기 위한 설정값 레지스터와 PSI내의 압력, 펌프 상태 및 Value 상태의 출력 설정 레지스터를 확인 할 수 있다.

4.4 공장컨베이어 시스템

공장 컨베이어(company conveyor) 자동 제어시스템은 크게 물류 운송 역할과 분류기를 통하여 물류를 분류하는 과정을 시뮬레이션 할 수 있는 테스트베드이다. 공장에서 생산된 제품을 컨베이어를 이용하여 다른 공정으로 전달하고, 제품을 분류하는 과정과, 제련 공정 과정에서 생산된 철강 제품을 압연공장으로 전달하는 과정 및 자동차, 반도체 등 기타 제조 공정라인에서의 컨베이어 시스템 시뮬레이션을 할 수 있다.

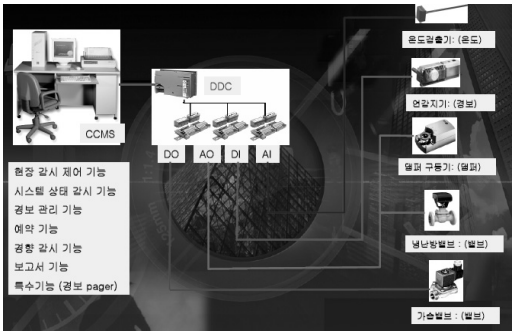
〔그림 6〕 컨베이어 제어시스템의 예〔7〕

컨베이어 시스템을 제어하기 위해서는 컨베이어 벨트위의 물체를 감지하는 센서와 컨베이어 벨트를 구동시키는 모터, 분류기 작동 등을 액츄에이터를 이용하여 구동하기 위한 설정값 레지스터와 분류기·모터·분류 센서의 상태를 나타내는 출력 레지스터를 설정 및 확인을 할 수 있다.

4.5 감시 시스템

감시 제어 시스템에서 각종 기기의 상태를 파악하고, 이에 따라 액츄에이터를 이용하여 제어하는 과정을 시뮬레이션 할 수 있는 테스트베드이다. 이 시스템으로 기반시스템의 시설, 설비의 동작을 감시하기 위해 각종 센서로 부터 읽어 들인 정보를 이용하여 기기를 동작시키는 과정과 홈 네트워크 및 공장의 자동화 공정에서 각종 센서로 부터 읽어 들인 정보를 이용하여 기기를 동작시키는 과정을 모니터링 한다.

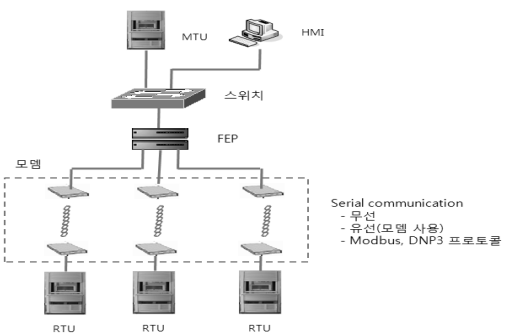
본 장에서 예시된 5가지 테스트베드 모델은 기본적으로 산업계에서 가장 많이 사용되고 있는 제어시스템의 모델로 제시하였다. 그러나 실제로는 이와 더불어 산



〔그림 7〕 감시시스템의 예[6]

업계에서 사용되고 있는 제어시스템들은 각기 복합적이고 다양한 제어방식이 존재하고 있다.

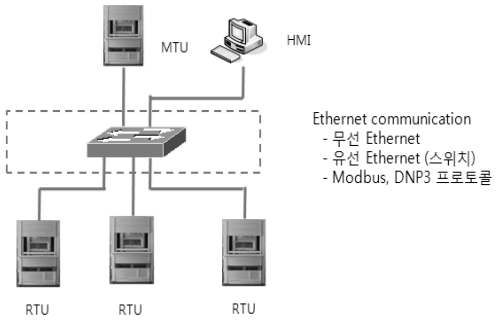
마지막으로 제어 프로토콜 테스트베드는 실제로 MTU와 RTU간의 통신과 RTU와 현장제어설비간의 제어 데이터 송수신을 위한 프로토콜로 Modbus 프로토콜과 DNP3 프로토콜을 사용하여 구축한다. 현장에서 사용되는 통신로는 유, 무선형태로 구분될 수 있으며, 대부분 Ethernet 혹은 Serial 라인으로 구성되어 있기 때문에 두 가지 환경에 대한 테스트베드로서, [그림 8]과 [그림 9]와 같이 구성한다[8].



〔그림 8〕 직렬통신 환경의 테스트베드

직렬통신 환경에서는 수조(water storage tank), 급수탑(raised water tower), 공장컨베이어벨트(factory conveyor belt), 가스관(gas pipeline), 산업배기(industrial blower)분야의 제어시스템에 주로 사용되고 있다[8].

Ethernet 환경에서는 철강 압연(steel rolling operation), 스마트그리드(smart grid) 분야의 제어시스템에 주로 사용되고 있다[8].



〔그림 9〕 Ethernet 환경의 테스트베드

〔표 2〕 테스트베드 별 적용분야

유형별 모델시스템	적용분야
수조제어 시스템	상하수도, 정수장, 석유화학, 정유 산업
급수탑 시스템	상수도, 정유·화학 산업 및 각종 급수시설
가스관 시스템	송유관, 상하수도관 및 가스관
컨베이어 제어시스템	공정 자동화, 각종 제조 분야
감시시스템	교통신호, 전력전송, 철도 및 지하철

[표 2]는 산업유형별 모델시스템의 적용분야를 나타낸다. 수조제어시스템은 상하수도, 정수장 등 석유화학 분야의 제어분야에, 급수탑 시스템은 상수도, 급수시설의 제어분야에, 가스관제어시스템은 상하수도 및 가스관의 제어분야의 테스트베드로서 적용될 수 있다. 컨베이어제어시스템은 공장의 자동화 공정 및 제조공정분야에서 적용되고 있으며, 감시시스템은 교통신호, 전력전송, 철도 및 지하철 분야의 제어시스템에 적용될 수 있다.

Ⅴ. 결 론

본 논문에서는 제어시스템 테스트베드 구축방안과 테스트베드를 이용한 제어시스템 취약점 분석방안에 대하여 살펴보았다.

현재 국가 기반산업분야에서 사용되고 있는 제어시스템은 원자력·화학 등의 에너지산업과, 수자원, 교통신호등의 다양한 제어가 사용되고 있다. 하지만, 해커나 공격자 등에 의한 사고 발생, 또는, 관리자의 USB저장장치 사용 부주위로 제어시스템이 감염되어 엄청난 재앙이 발생할 수 있다. 실제로 사이버전쟁 발생 시 제일

처음의 목표가 국가기반에 사용 중인 제어시스템이 될 수 있으며, 현재 제어시스템은 인터넷의 발달로 폐쇄된 위치에서 점점 외부로 노출되고 있어 테러리스트의 공격 목표가 되고 있다.

본 논문에서는 이러한 문제점을 시뮬레이션하기 위한 테스트베드 구축방안에 관한 논문으로서, 네트워크 분야의 보안방안으로 1차 2차적인 방화벽의 구성과 서버운용, 그리고 제어시스템 간에는 ModBus 와 DNP3 프로토콜을 이용한 RTU 간의 통신이나 MTU와 RTU의 통신 및 RTU 와 다른 제어기기 간의 통신방법을 시뮬레이션할 수 있는 테스트베드를 제안하였다.

마지막으로 산업기반 제어시스템들을 수조제어 시스템, 급수탑 시스템, 가스관 제어 시스템, 공장자동화 시스템, 감시 시스템 별로 분류하여 각 분야들에 대한 테스트베드를 구축방안을 설명하였다. 결과적으로 산업기반의 제어시스템을 전체적으로 구성하여 테스트하기에는 광범위하고, 변수가 너무 많기 때문에, 기반시스템으로 제시된 5가지의 형태를 조합하여 각각의 산업기반 제어시스템의 테스트를 위한 테스트베드를 구성할 수 있다. 이와 같은 테스트베드를 이용하여 산업기반 제어시스템에 대한 보안취약점 분석과 함께 보안방안을 검토할 수 있다. 이러한 결과는 단위공정별로 발생될 수 있는 보안 취약점을 발견할 수 있으며, 또한 이를 이용하여 거대 국가기반산업분야에서 발생될 수 있는 보안 취약점 해석에 기초가 될 것으로 사료된다.

참고문헌

[1] “Common Cybersecurity Vulnerablities in Inustrial Control System”, DHS.

[2] DNP 3.0 Overview, www.dnp.org, 1997.

[3] 산업용 시리얼 광무선 통신 프로 디바이스 http://blog.naver.com/PostView.nhn?blogId=114jhkim&logNo=20144546738.

[4] 아이뉴스24, 위즈정보기술, 자동제어시스템구축, http://news.inews24.com/php/news_view.php?g_menu=020200&g_serial=21120.

[5] 한국철도 문화협력회 (Railroad culture data research), cafe.daum.net/psg8877).

[6] 김덕주, “자동제어의 이해”, honeywell korea automation college.

[7] Automation Supplies Ltd. Modular conveyors. Alumininum profile systems. “http://www.automation-supplies.com/modular-plastic-belt-conveyors.html”

[8] Tomas Morris, Anurag Srivastavab, Bradley Reavesa, Wei Gaoa, Kalyan Pavurapua, Ram Redd, “A control system testbed to validata critical infrastructure protection concepts”, www.dx.doi.org, 2011.

[9] 이철원, “주요 제어시설의 사이버보안동향”, 국가보안연구소, 2007.

[10] “제어시스템 취약점 분석·평가 지침”, 한국인터넷진흥원, 2012.

〈著者紹介〉

김 지 홍 (Ji-hong Kim)
정회원

1982년 2월: 한양대학교 전자공학과 학사
1984년 2월: 한양대학교 대학원 전자통신공학과 석사
1996년 2월: 한양대학교 대학원 전자통신공학과 박사
1995년 3월: 정보통신기술사
2010년 3월: 정보보호학회 부회장
1991년 2월~현재: 세명대학교 정보통신학부 교수
<관심분야> 네트워크 보안, 응용 보안, 의료정보 DB보안

유 천 영 (Choun-young Yu)
정회원

2005년 2월: 세명대학교 컴퓨터과학과 학사
2007년 8월: 세명대학교 대학원 전자계산 교육대학원 석사
2008년 2월~현재: 세명대학교 대학원 전산정보 박사수료
<관심분야> 정보보호, DB 보안, 네트워크 보안

김 성 용 (Sung-Yong Kim)
정회원

2007년 3월~현재: 세명대학교 정보통신학부 학사 재학
<관심분야> 제어시스템 보안, 서버 보안, 정보보호