情 報 保 護 學 會 誌
第22卷 第5號, 2012. 8

제어 시스템 보안을 위한 해외 테스트 베드 구축 현황

박 동 규*

요 약

제어 시스템 보안을 위하여 보안 적합성 확인과 유효성 검사 및 사고 발생 시 제어 시스템의 피해 상황 및 영향 범위에 대해 실제의 제어 시스템 구성 요소를 분석하는 환경이 필요하며, 실제 기기와 시뮬레이션을 이용하여 취약성을 검증하기 위한 환경 및 제어 시스템 구성 요소의 취약성을 발견하는 도구가 필요하다. 본 논문에서는 제어 시스템 보안 및 국내 제어 시스템 테스트 베드 구축을 위하여 선진국들의 제어 시스템 테스트 베드 구축 현황 및 사례에 대하여 설명하고자 한다.

Ⅰ. 서 론

제어 시스템은 주요 산업에서 현장설비를 제어 및 모니터링하기 위해 구축하는 IT 기반의 산업 자동화 시스템으로 초창기에는 독자적이고 폐쇄적인 시스템으로 구축되고 운영되어서 사이버 보안의 위협이 적다고 인식되어 왔으나 현재에는 상용 개방형시스템으로 구축 운영되어서 사이버 보안의 위협 가능성이 증대되고 있는 상황이다. 그러나 현재 제어 시스템 사이버보안에 대한 국내 연구체계는 부재한 상황으로 국내 제어 시스템 환경에 맞는 제어 시스템 보안 가이드라인을 마련하고, 주요 산업계에 이를 적용하도록 하는 등의 적극적인 사전 연구 및 대응이 필요한 시점이라고 할 수 있다. 해외에서는 제어 시스템 보안의 중요성을 인식하고 제어 시스템 보안을 위한 테스트 베드를 구축하여 활용하고 있는 상황이다. 본 논문에서는 제어 시스템 보안 및 국내 제어 시스템 테스트 베드 구축을 위하여 해외 선진국들의 제어 시스템 테스트 베드 구축 현황 및 사례에 대하여 설명하고자 한다.

Ⅱ. 해외 제어 시스템 테스트 베드 구축 현황

제어 시스템 보안을 위하여 보안 적합성 확인이나 유효성 검사를 실시하거나 또는 확인하는 방법 그 자체를 연구할 필요가 있다. 그러기 위해서는 실제로 사용하는 제어 시스템 및 구성 요소를 대상으로 평가 실험을 거듭 해 나갈 필요가 있기 때문에 제어 시스템 전체의 보안을 확인하는 공통 기반 기술을 개발해 나갈 필요가 있다. 제어 시스템 보안에 관한 국제 표준화 IEC62443의 개발이 검토되고 있는 것과 동시에, 그 국제 규격을 준수하는 제어 시스템 보안 대응의 인증 서비스가 전 세계에서 진행되고 있다. 그리고 사고 발생 시 제어 시스템의 피해 상황 및 영향 범위에 대해 실제의 제어 시스템 구성 요소를 분석하는 환경이 필요시 되고 있다. 즉, 사고 지원을 위해 실제 기기와 시뮬레이션을 이용하여 취약성을 검증하기 위한 환경 및 제어 시스템 구성 요소의 취약성을 발견하는 도구가 필요하다. 특히, 취약성의 영향 및 취약성에 대한 패치 적용에 의한 영향에 대해서는 실행중인 제어 시스템에서 검증하는 것이 어렵기 때문에 테스트 베드에서 확인하는 것이 바람직하다.[10]

2.1 미국의 제어 시스템 테스트 베드 구축 현황

미국에서는 에너지 절약 (DOE) 국립 연구소 시설에서 국토 안보부 (DHS)와 공동으로 제어 시스템에 대한 보안 테스트 베드가 구축・운영되고 있다. 예를 들어, 아이다호 국립 연구소 (INL)는 2004년 3월 SCADA 테스트 베드를 구축하고, SCADA 시스템 보안 검증을 실시하고 있다. 검증 결과를 바탕으로 제어 시스템 보안

* 순천향대학교 정보통신공학과 (dgpark@sch.ac.kr)

표준화 활동을 지원하고, 개발한 사이버 보안 분석도구를 사용하여 보안 위험 경감을 위한 보급 계발 활동 등을 실시하고 있다. 또한 제어 시스템 권장 보안 요구 사항 표준 모음(Catalog of Control System Security : Recommendations for standards Developers)을 발행하였다.

미국의 제어 시스템 테스트 베드 프로그램은 에너지 분야 제어 시스템 보안성 제고를 위한 대규모 테스트 베드 운용 프로그램으로 미국 에너지부(DOE)자금 지원으로 설립되었다. 이 프로그램은 NSTB(National SCADA Testbed) 프로그램으로 추진되었고 6개 국립연구소(INL, SNL, PNNL, ORNL, ANL, LANL) 중심으로 다양한 제어 시스템에 대한 취약성 분석 서비스, 차세대 안전한 제어 시스템 보안 아키텍처 및 기술 연구, 제어 시스템을 위한 침입탐지 및 대응 기술 연구, 제어 시스템 사이버 보안 교육 서비스, 파트너십 및 아웃리치 활동을 수행한다. INL SCADA 테스트 베드는 완전한 크기의 전기 전력 그리드를 포함하고 있다. INL 전력 그리드는 시스템 내에 3000개가 넘는 관찰 제어 지점들을 가지고 61마일 128KV 전송 루프, 13.8KV 분배 선들, 7개의 변전소들을 포함하고 있다. 추가적으로 INL SCADA 테스트 베드는 TCP/IP, ATM, 802.11, GSM 그리고 모뎀 통신 신호의 시뮬레이션과 시험을 위하여 무선 테스트 베드 설비를 포함하고 있다. 지원되는 유선 통신 표준들은 ICCP, MODBUS, DNP3 그리고 다른 등록된 공중영역 프로토콜을 포함한다. 마지막으로 사이버 테스트 베드는 방화벽과 VPN 시험을 지원하기 위하여 이용된다.

NSTB는 사용자 및 공급업체와 계약(보통 3개월 소요)을 하고 2~3 주 간의 교육을 실시하며, 900시간의 평가 기간과 약 700 시간의 엔지니어링 지원을 거쳐서 테스트 결과를 발행 하게 된다. 전체 테스트 절차는 약 5~9 개월이 소요 (1년 이상의 경우도 있음)된다. NSTB는 4 시간 코스의 초급 SCADA 보안과 8 시간 코스의 중급 SCADA 보안 그리고 5일 간의 실제 SCADA 네트워크 모델을 이용한 실습을 수행하는 고급 SCADA 보안 교육 프로그램을 수행한다.

NSTB는 INL(Idaho National Lab.)에서 2003년부터 2011년 9월까지 37개 에너지 분야 제어 시스템에 대한 취약성 분석을 실시하였다. 4개 개발사의 컴포넌트와 15개 개발사의 제어 시스템 및 8개 운영사이트에 대한 취약성을 분석하였다. 또한 제어 시스템 보안기술 연구개발 사업으로 '09년 27개 보안과제 연구개발 사업을 진행하였으며, 제어 시스템 개발사 및 운영사에서 참조할 수 있도록, 제어 시스템에 공통적인 취약점을 분석하여 보고서로 공개하였다.

미국은 NSTB 구축을 위해 '05년~'06년 1,000만 달러를 지원하였으며, '08년 미국 에너지부(DOE)의 230만 달러 예산 지원으로 7개 제어 시스템 제품에 대한 취약점을 분석하였고, 4곳의 운영 중인 제어 시스템 분석을 수행하였다. '10년 에너지부에서는 스마트 그리드를 포함한 에너지 분야 사이버보안을 위해 Cybersecurity for Energy Delivery Systems(CEDS) 프로젝트에 2010년~2012년까지 8,000만 달러를 투자하였다.

2.2 유럽의 제어 시스템 테스트 베드 구축 현황

유럽에서 테스트 베드는 아직 구축 개발 단계이며, 현재는 노하우의 공유 및 국제 표준을 공동 제안하는 단계는 아니다. 그러나 앞으로 노하우의 축적 및 국제 협력이 가속화될 것으로 전망된다.

2.2.1 중요 에너지 기반 시설을 위한 SCADA 보안 시험 센터(ESTEC)

ESTEC는 SCADA 제조자, 학술 연구자와 다른 관련된 사람들을 위하여 실제 세상에 대한 시험 설비들을 제공하도록 유럽연합에 의해 2008년에 제안되었다. 중요 에너지 기반 시설을 위한 SCADA 보안 시험 센터의 유럽 네트워크(ESTEC)는 유럽의 SCADA 테스트 베드를 위한 설계를 정의하기 위해 설립되었다. 이 센터에서는 SCADA 취약성 시험과 공격 시뮬레이션 수행 등 다양한 실험을 수행하며, 또한 표준 개발과 관련 시험을 수행한다. 이 센터는 ICS 시험 센터의 범위를 정의하고 그들을 요구사항으로 정리하며, 시험 센터의 개념적인 설계를 개발하고 시스템 요구사항과 주요 요소들의 개념적인 구조를 정의한다. 또한 시험 센터에 대하여 전 세계적으로 보고를 하고 국제 협력의 가능성과 이익을 추구하며, 유럽 내에 분포된 시험 센터의 네트워크에 대한 분석을 수행하며, ERN-CIP 개발을 위한 EU내의 정책과 절차에 대한 제안을 수행한다.[4]

ESTEC는 에너지 중요 기반 시설을 위한 유럽 안전

시험 센터로 반복적인 보안 요구사항의 성능 평가를 통하여 알려지거나 또는 알려지지 않은 위협에 대한 ICS의 취약성을 평가(레드 팀)하고 새로운 기술적인 해결책과 대응방안의 효율성과 호환성을 평가(블루팀)한다. 보안 실험이 에너지 중요 기반 시설과 연결된 운영 ICS상에서 수행되며, 실험을 통하여 운영 ICS상에 보안 데이터를 생성하고 보호 요구사항과 실습과 정책의 확인을 지원하며, ICS를 위해 여전히 정의되지 않은 보안 표준의 검증을 지원한다.

ESTEC의 에너지 기반시설 시험 범위와 테스트 베드는 에너지 기반 시설 운영과 관련해서 ICS 취약성의 식별을 지원하며, 사이버 공격 시뮬레이션을 위한 완전한 크기의 산업 제어 시스템 기준 시험 범위와 테스트 베드 시설을 제공함으로써 침투시험과 대응 방안 설계와 평가를 지원한다. 통신 네트워크 테스트 베드와 시험 범위는 복잡한 분산 기반 시설의 취약성과 회복력 평가를 지원하며, 실험 수행, 보안 평가 방법 설계 그리고 보안 표준과 검증을 위한 보안 연구소를 포함하고 있다.

ESTEC는 두 개의 분야 즉 전기 (전력 발전소, 전송선, 분배선)와 석유와 가스 (추출, 정제, 처리, 저장, 송유, 발송센터)와 관련된 테스트를 수행한다. 보안연구소는 재생된 ICS/CI에 대한 외부적인 기능들을 수행하며, 시험 수행 전에 실험 설비의 설정을 담당하고, 시험 수행 중에는 실시간 모니터링, 데이터 수집, 시험 중인 시스템의 상호작용을 관장하며, 시험 수행 후에는 오프라인 데이터 가공을 수행한다.

향후계획으로 ESTEC은 전기와 석유 & 가스 등 현재 중점을 두고 있는 중요 기반시설 이외에 많은 다른 중요 기반 시설들로 확대(예 화학, 교통, 제약 등)를 고려하고 있으며, ESTEC에서 수행된 연구를 모든 ICS 제어 유럽 중요 기반시설에 점차 확산하려고 하고 있다.

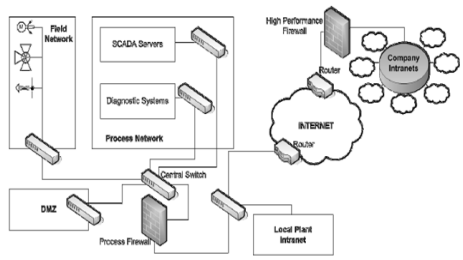
2.2.2 산업 장치 프로세스 연구소(Industrial Instrumentation Process Lab)

영국 콜롬비아 기술 학회(BCIT)는 장치 프로세스 연구소로 알려진 SCADA 테스트 베드를 소장하고 있다. 이 연구소는 다양하고 복잡한 제어 프로세스들을 생성할 수 있는 것이 특징이며, 증류 기둥, 증발기, 배치 펄프 침지기, 화학 혼합 반은 프로세스, 전원 보일러 등을 갖추고 있다. BCIT실험실은 Emerson DeltaV와 Provox 분산 제어 시스템, F&P MC5000 제어기, Foxboro IA 디지털 제어 시스템, Rockwell PLC-5s, Groupe Schnieder 984와 양자 PLC, Honeywell TDC 3000 분산 제어 시스템, BaileyNet90 분산 제어 시스템, 그리고 Genius I/O를 갖춘 GE/Fanuc Series 90/70, Series 90/30 PLC를 포함한 다양한 SCADA 장비를 포함하고 있다.[5]

2.2.3 SCNI SCADA Testbed(JRC - IPSCEU)

SCNI SCADA 테스트 베드는 이탈리아 북부 이스뿌라의 연구시설에 설치되어 센서, 액추에이터를 탑재한 실제 부분과 SCADA 시스템, 시뮬레이터로 구성된 테스트 베드를 운영하고 있다. 이 테스트 베드는 중요 기반 시설 보호를 위한 목적으로 설립되었고, 정보시스템, 통신 네트워크, 산업 제어 시스템을 포함한 네트워크로 연결된 기반 시설의 보안에 대한 정책 지원과 연구를 수행한다. 또한 기반시설, 그들의 연관성, 그들의 취약성, 잠재적으로 악의적인 위협, 관련된 치명적인 공격, 대응방안 등을 연구한다.[6]

이 테스트 베드의 목적은 SCADA 시스템의 구조 연구 및 SCADA 시스템의 새로운 취약성의 효과에 대한 연구, 새로운 취약성하에서 산업 통신 프로토콜 시험이며, 현재 수행하고 있는 프로젝트로는 SCADA 구조와 프로토콜의 취약성 평가, 산업용 프로토콜을 위한 IDS 시스템, 산업용 통신 프로토콜을 위한 암호 연구 등을 들 수 있다. 다음 [그림 1]은 SCNI SCADA연구소 네트워크 전개도이다.



〔그림 1〕 SCNI SCADA 연구소 네트워크 전개도

2.3 일본의 제어 시스템 테스트 베드 구축 현황

일본에서는 제어 시스템 안정성 확보를 위하여 일본 경제 산업성에서 2010년 12월 “사이버 보안과 경제 연구회”를 개최하여 “제어 시스템의 안정성 확보 방안”을

논의하였으며[7], 제어 시스템에 대한 실무 검토를 진행하기로 결정하고 그것을 위한 “제어 시스템 보안 검토 위원회를 2011년 10월에 발족했다. 이 위원회에서는 지역 내에 있는 중요한 인프라에 대한 정보 보안 대책 강화 및 해외 무역 장벽이 될 제어 시스템 보안 인증에 대한 대응, 스마트 커뮤니티의 도입 촉진을 포함한 인프라 수출 촉진을 위한 공통 기반 강화 방안에 대해 검토하였다.[8]

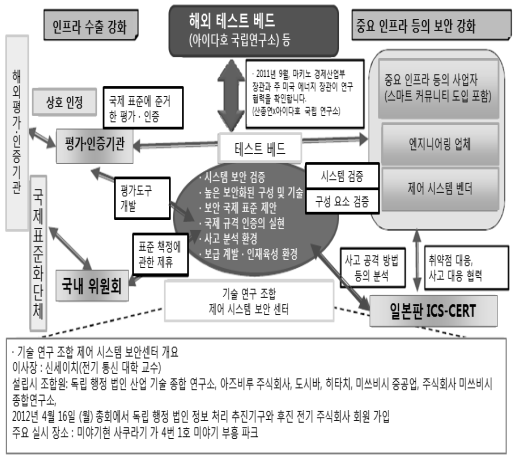
일본의 제어 시스템 보안 대책의 방향은 크게 세 가지로 첫 번째로 국제 표준화 추진, 실증 실험의 실시 및 평가・인증 체계 구축 등을 통해 사고 미연 방지를 위한 노력을 들 수 있으며, 다음으로는 사고 등에 대한 대응으로 사후 대책이고, 이것을 지원하는 공통 기반으로 인재육성과 보급계발이 고려될 수 있다.

먼저 미연 방지 대책으로 일본에서는 서양체제와 동향을 주시하면서 전략적인 표준 환경을 만들고 있으며, 또한, 외국과의 상호 인정을 목표로 일본에서도 평가・인증 체계를 시작하고 있다. 또한 사고 대응체제에 있어서는 일반 정보 시스템에 대한 CERT는 이미 운용되고 있지만, 산업용 제어 시스템에 대해서는 향후 검토 과제로 되고 있는 상황이다. 또한, 제어 시스템 보안에 대한 고급 지식이 요구되는 제어 시스템과 정보 보안을 모두 이해하는 인재를 육성하고자 하고 있으며, 안정성 확보에 대한 위험과 비용에 대한 의식을 포함한 사용자 기업 등에 보급 계발을 추진하고 있는 중이다. 그래서 일본에서는 제어 시스템 보안의 실현을 위해 “테스트 베드 WG, 표준화 WG, 평가・인증제도 WG, 사고처리 WG, 인재육성 WG, 보급계발 WG”등 6개의 WG를 설치하여 각 WG별로 구체적인 과제에 대해 검토 추진 중이다.[8]

테스트 베드 WG에서는 일본의 테스트 베드에 대해 연구 개발, 국제 표준화 및 평가 인증에 대한 대응, 사고 지원, 인재 육성・보급계발의 필요성에 대한 요구사항이 정리되었다. 요구사항에서 이끌어진 기능을 기술 연구 조합 제어 시스템 보안 센터가 중심이 되어 2012년 미야기 부흥 파크 사이버 보안 테스트 베드를 구축할 예정이다.[8]

Ⅲ. 관련 연구

다양한 방법들이 소규모 SCADA 설비와 시뮬레이션 되는 SCADA 환경을 포함하여 제안된 산업용 제어 시



〔그림 2〕 일본 기술 연구 조합 제어 시스템 보안 센터와 테스트 베드

스템 보안 해결책의 시험을 지원하기 위하여 학술 연구자들에 의해 사용되어 왔다. 다중의 연구 그룹들이 제어 시스템과 그들의 통신 네트워크 그리고 제어 시스템에 대한 사이버보안 공격을 모델링하기 위하여 시뮬레이션 기반 시스템을 제안하였다. [18]에서 Montague는 프로세스 설계와 모델링, 운영자 훈련과 사고 응답 모델링을 위하여 산업용 제어 시스템 영역 내에 시뮬레이션의 도입을 설명하였다. 대부분 SCADA 보안 테스트 베드는 시스템의 사이버 공격을 시작하기 위한 메카니즘과 프로세스 시뮬레이터, 네트워크 시뮬레이터를 포함한다. [11]에서 Davis 등은 네트워크 트래픽과 사이버 보안 공격을 시뮬레이션 하기 위하여 PowerWorld 시뮬레이터, 가상의 네트워크 클라이언트, 가상의 제어 및 전력 시스템 측정 정보 그리고 네트워크 보안 실습을 위한 시뮬레이션 기반 접근 방식을 토의하였다. [12]에서 Giani등은 시뮬레이션 되는 SCADA 보안 테스트 베드를 기술하였다. 이 테스트 베드는 제어 시스템과 구현 플랫폼을 모델링하기 위하여 MathWorks Simulink를 사용 하였으며, 저자들은 이 시뮬레이션 모델을 가상의 공격을 포함하도록 확장하려고 계획하고 있다. Giani등은 또한 상업용 하드웨어와 소프트웨어로 SCADA 테스트 베드를 구현하려고 계획하고 있다. [13]에서 Queiroz등은 시뮬레이션 되는 SCADA 보안 테스트 베드를 위한 구조를 제안하였다. 이 시스템은 센서와 액추에이터와 같은 하드웨어 장치들을 시뮬레이션 하기 위하여 LEGO Mindstorm NXT 장치들을 사용하였다. OMNET++는 이산적인 이벤트를 모델링하기 위하여

사용되며, libModbus C 라이브러리는 MODBUS 네트워크 트래픽과 TCP/IP 지원을 위한 INET 프레임워크를 모델링하기 위하여 사용된다. [16]에서 Chabukswar 등은 SCADA 사이버보안 공격을 시뮬레이션 하는 것을 토의하였다. Chabukswar는 다른 시뮬레이터로부터의 결과를 통합하기 위하여 C2WindTunnel프레임워크를 사용하였다. OMNET++, Simulink, 및 NetworkSim는 전체 시뮬레이션 환경 내의 부분요소들이다. [17]에서 Bergman는 파워 그리드를 모델링하는 SCADA 보안 테스트 베드를 위한 시뮬레이션 프레임 워크를 기술하였다. DL 테스트 베드는 전기 생성, 전송 그리고 적재를 모델링하기 위하여 PowerWorld를 사용하였다. PowerWorld는 TCP 프로토콜 시뮬레이터 상에 RINCE 네트워크 시뮬레이터 DNP3에 연결되어 있으며, 가상 릴레이들이 테스트 베드 내에 제어 시스템 지능형 전자장치(IED)로 작용하도록 모델링되어 있다. 시뮬레이션 테스트 베드는 산업용 제어 시스템에 사이버 보안 공격의 효과를 모델링하기 위한 적은 가격의 방법을 제공한다. 그러나 시뮬레이션 테스트 베드는 제어 시스템 요소들의 상호작용을 완벽하게 모델링하는 능력은 부족한 단점이 있었다. [10]

상업용 제어 시스템 하드웨어와 소프트웨어를 사용하는 두 개의 중요한 테스트 베드에 대한 연구가 존재한다. [14]에서 Fovino등은 터보 가스 전력 시설내의 요소들을 포함한 SCADA 사이버 보안 연구를 위해 사용되는 연구소에 대하여 상세히 설명하였다. 이 테스트 베드는 파이프, 밸브, 센서, 펌프와 같은 물리적인 장치들과, 다중의 판매자로부터 공통의 제어 시스템 장비, 전력 생성과 관련된 장비를 상호 연결하기 위한 프로세스 네트워크, RADIUS 서버를 통하여 프로세스 네트워크와 연결된 가상의 사무실 인트라넷, 고속 데이터베이스 서버가 위치하고 있는 DMZ, 제어 시스템으로부터 제어 시스템 상태에 영향을 미치지 않고 공격과 관련된 정보를 수집하고 분리된 관측 네트워크, 그리고 외부 인터넷에 대한 연결을 포함하고 있다. 이 테스트 베드는 전력 생성 설비의 완벽한 모델이라고 할 수 있다. [15]에서 Hahn등은 한 개의 제어 센터에 연결된 두 개의 전기 변전소를 모델링하기 위한 테스트 베드를 문서화하고 있다. 자동 변압기와 회로를 가진 파워 소스는 높은 전압 라인을 모델링하기 위하여 사용된다. 변전소는 두 개의 과전류 방지 릴레이에 연결된 소프트웨어 기반 원격 터미널 유닛을 포함하며, 제어 센터는 HMI 소프트웨어와 이력 기록 서버를 포함한다. 이 테스트 베드에 사용된 공통의 상업용 제어 시스템 통신 프로토콜들은 DNP3와 IEC 61850를 포함하고 있으며, 변전소와 제어 센터는 기본 방화벽 능력을 포함하고 있는 VPN 서버 장치를 통하여 연결된다. 위의 테스트 베드는 둘 다 전력 시스템 요소들을 모델링하고 있다. 첫 번째는 전력 생성을 모델링하고 두 번째는 전력 전송을 모델링한다. 이 논문에서 기술된 MSU 테스트 베드는 전력 전송 시스템을 모델링하기 위하여 하드웨어와 소프트웨어를 포함하고 있으며, 실시간 디지털 시뮬레이터 (RTDS)가 하드웨어 설정으로 대규모 실시간 전력 시스템 시뮬레이션을 제공하기 위하여 사용되고 있다. 추가적으로 테스트 베드는 광대역 측정 관측시스템 (WAMS)과 특별한 보호 책략(SPS) 연구가 가능하도록 하기 위하여 페이저 측정 유닛, 페이저 데이터 집중장치 그리고, 상업용 에너지 관리 시스템(EMS)을 포함하고 있다.

[10]논문은 미시시피 주립 대학교 SCADA 보안 연구소와 전력 및 에너지 탐구 연구소 테스트 베드를 설명하고 있다. 이 연구소는 경로 설정이 가능하거나 불가능한 일반 산업 제어 시스템 네트워크를 통하여 상업용 하드웨어 및 소프트웨어에 의해 제어되는 기능적이고 물리적인 프로세스들을 가진 테스트 베드를 생성하기 위하여 다중의 중요한 기반 시설을 가진 산업들로부터 모델이 되는 제어 시스템을 결합하고 있다. 테스트 베드는 사이버 보안 취약성을 발견하고, 제어되는 물리적인 프로세스들에 대한 취약성의 영향을 이해하기 위하여 사용되며, 식별된 문제들은 형태와 효과 측면에서 치명도와 유사성에 의해 분류된다. 그리고 마지막으로 사이버 보안 감소 방안들이 테스트 베드 내에서 개발되고 있으며, 테스트 베드는 이 방안들이 검증되는 연구 과정을 위해 사용되고 있다.

Ⅳ. 결 론

제어 시스템 보안을 위하여 실제로 사용되는 제어 시스템 및 구성 요소를 대상으로 평가 실험을 거듭 해 나갈 필요가 있으며, 사고 발생 시 제어 시스템의 피해 상황 및 영향 범위에 대해 실제의 제어 시스템 구성요소를 분석하는 환경이 필요시 되고 있다. 특히, 취약성의 영향 및 취약성에 대한 패치 적용에 의한 영향에 대해

서는 실행중인 제어 시스템에서 검증하는 것이 어렵기 때문에 테스트 베드에서 확인하는 것이 바람직하다. 본 논문에서는 제어 시스템 보안 및 국내 제어 시스템 테스트 베드 구축을 위하여 해외 선진국들의 제어 시스템 테스트 베드 구축 현황 및 사례에 대하여 설명하였다. 향후 효율적인 제어 시스템 테스트 베드 구축을 위한 연구가 수행되어야 할 것으로 사료된다.

참고문헌

[1] Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program. Idaho National Laboratory. IdahoFalls, Idaho 83415. November 2008. http://www.inl.gov/scada/publications/d/inl_nstb_common_vulnerabilities.pdf

[2] Fink, R. Spencer, D., and Wells, R. Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems. Idaho National Laboratory. Idaho Falls, Idaho 83415. September 2006. http://www.inl.gov/scada/publications/d/nstb_lessons_learned_from_cyber_security_assessments.pdf.

[3] Wireless Procurement Language in Support of Advanced Metering Infrastructure Security. Idaho National Laboratory. Idaho Falls, Idaho 83415. August 2009. http://www.inl.gov/scada/publications/d/inl-ext-09-15658_ami_proc_language.pdf.

[4] ESTEC Project. http://www.estec-project.eu/.

[5] Industrial Instrumentation Process Lab. http://www.bcit.ca/appliedresearch/tc/facilities/industrial.shtml.

[6] SCNI ACTION - IPSC - Europa ipsc.jrc.ec.europa.eu/fileadmin/.../JRC54499.pdf.

[7] “2010年度　制御システムの情報セキュリティ動向に關する調査報告書”, IPA, 2011. http://www.ipa.go.jp/security/fy22/reports/ics_sec/index.html.

[8] “制御システムセキュリティ檢討タスクフォース報告書”. 經濟産業省, 2012. http://www.meti.go.jp/committee/kenkyukai/shoujo/controlsystem_security/report01.html.

[9] Reaves, B., Morris, T., Discovery, Infiltration, and Denial of Service in a Process Control System Wireless Network. IEEE eCrime Researchers Summit. October 20-21, 2009. Tacoma, WA.

[10] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu, R. Reddi, A control system testbed to validate critical infrastructure protection concepts, International Journal of Critical Infrastructure Protection (IJCIP), Volume 4, Issue 2, August 2011, Pages 88-103.

[11] C. Davis, J. Tate, H. Okhravi, C. Grier, T. Overbye, and D. Nicol, “SCADA Cyber Security Testbed Development,” in Power Symposium, 2006. NAPS 2006. 38th North American, pp. 483-488, 2006.

[12] Annarita Giani, Gabor Karsai, Tanya Roosta, Aakash Shah, Bruno Sinopoli, and Jon Wiley, “A testbed for secure and robust SCADA systems,” in 14th IEEE real-time and embedded technology and applications symposium (RTAS ’08) WIP session, 2008.

[13] C. Queiroz, A. Mahmood, Jiankun Hu, Z. Tari, and Xinghuo Yu, “Building a SCADA Security Testbed,” in Network and System Security, 2009. NSS ’09. Third International Conference on, pp. 357-364, 2009.

[14] I. Fovino, M. Masera, L. Guidi, and G. Carpi, “An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants,” in Human System Interactions (HSI), 2010 3rd Conference on, pp. 679-686, 2010.

[15] A. Hahn et al., “Development of the Power Cyber SCADA security testbed,” in Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW ’10, p. 1, 2010.

[16] Rohan Chabukswar, Bruno Sinpoli, Gabor Karsai, Annarita Giani, Himanshu Neema, and Andrew Davis, “Simulation of Network Attacks

on SCADA Systems," in First Workshop on Secure Control Systems, 2010.

[17] Bergman, David C., "Power grid simulation, evaluation, and test framework," Master's, University of Illinois, 2010.

[18] Jim Montague, "Simulation Breaks Out," Control Global, pp. 52-61, Sep-2010.

〈著者紹介〉

박 동 규 (Park DongGue)
종신회원

1992년 2월: 한양대학교 전자공학과 박사
1992년 3월~현재: 순천향대학교 정보통신공학과 교수
<관심분야> 시스템 보안, 네트워크 보안, 제어 시스템 보안