전력 IT Cyber Security 연구 동향

김학만, 박재세, 김상남
시립인천전문대학

Study Tendency of Cyber Security in Power IT Area

Hak-Man Kim, Jae-Sae Park and Sang-Nam Kim
Incheon City College

Abstract - Electrical Power System is very important infrastructure in the country. The functions of control, monitoring and so on in the electrical power system are implemented by information technologies(IT) through cyber space. Recently, many activities for enhancing cyber security in the world. In this paper, we introduce the study tendency of cyber security in power IT areas.

1. 서 론

국가의 주요 기간망인 전력망은 감시, 제어가 통신망을 통하여 이루어지고 있으며, 잘못된 정보로 인해 오부동작이 발생할 경우에는 그 피해는 국가적이 차원으로 확대된다. 외국에서 고의적인 해킹, 악성코드 또는 웜 바이러스 등에 의해서 전력 설비가 오부동작 되는 사례가 발생하여 사회적인 문제로 발전하였으며, 또한 사이버 공격은 테러와 전쟁에서 공격 수단이 되기도 하였다.

이런 이유로 세계적으로 Cyber Security에 대한 중요성이 부각되고 있으며, 이에 대한 보호 대책에 연구가 진행되고 있고 또한 가이드라인과 기술표준을 수립하는 등, 연구, 상용화, 보급 그리고 장기적으로 의무화를 위한 움직임과 노력들이 진행되고 있다.

국내의 경우는 전력 IT는 전용망을 사용하기 때문에 Cyber Security에 대한 관심이 전용망과 범용망을 사용하는 외국에 비해서 중요성의 인식이 부족한 실정이다. 그러나 외국의 자료에 의하면 전용망의 경우라도 의도적인 사이버 테러나 해킹은 어렵지 않다고 보고되고 있다. 또한 현재에는 시스템 별로 독립적인 전용망으로 운용되고 있지만 점차 독립 시스템들이 통합 운영되어 갈 것으로 예상되며, 한 곳의 통신망이 사이버 공격에서 피해를 보게 되면 모든 망이 피해를 주게 되며, 그 결과 그 파급은 치명적이 국가적인 차원 문제가 될 것으로 예상된다. 그림 1은 사이버 공격에 대한 변전소의 피해를 나타낸 것이다. 또한 전력설비의 사이버 공격은 이라크 전쟁에서도 계획된 바가 있었던 것으로 알려지고 있으며, 테러의 주요 대상이 되고 있다.

〈그림 1〉 사이버 공격에 의한 변전소의 피해 [1]

따라서 본 논문에서는 현재 외국에서 진행되고 있는 Cyber Security에 대한 연구 동향을 조사하고 이를 소개하고자 하고자 한다. 국가별로는 미국, 유럽, 아시아 등 전세계적으로 현재 연구가 진행되고 있는데, 특히 SCADA(Supervisory Control And Data Acquisition)의 문제로 인한 대정전과 911 테러에 큰 피해를 입어 국가차원에서 테러의 대한 다각적인 대책을 마련하고 있는 미국의 경우 Cyber Security에 대해서 국가의 중요 이슈로 상정하고 이에 DOE를 중심으로 많은 연구와 상용화, 보급에 대한 노력이 이루어지고 있으며, 본 논문에서는 미국을 중심으로 연구동향을 소개하고자 한다.

2. Cyber Security 연구 동향

2.1 Cyber Security

Cyber Security 문제는 감시, 제어 시스템이 사이버 공간에서 안전하게 시스템에 주어진 고유의 임무를 수행할 수 있는지에 관한 것이고, 특히 전력 IT Cyber Security 문제는 전력시스템과 관계되는 제반의 감시, 제어 및 기타 시스템들이 사이버 공간에서 안전하게 고유 임무를 수행할 수 있는지에 관한 문제이다.

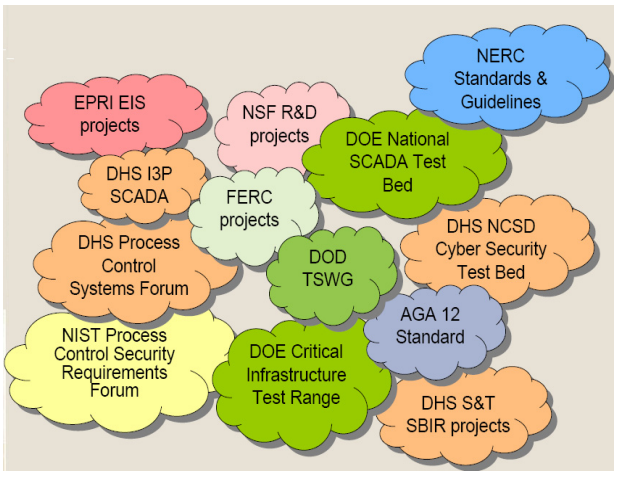
2.2 연구 분야

전력 IT는 전력시스템이라는 특수성을 가지는 시스템과 IT 기술이 접목되어 있는 융복합 기술이므로 전력 IT Cyber Security 문제를 해결하기 위해서는 전력회사, 관련 국가연구소, 관련 중전기 및 IT 회사, 대학이 연계되어 공동 연구를 수행해야 하며, 외국의 경우에도 다양한 관련 주체들이 참여하고 있다. 진행되고 있는 연구 분야를 정리하면 다음과 같다.

- 보안 정책
- 모델링
- 접근제어 (access control)
- 방화벽 (firewall)
- 침입 탐지 시스템 (intrusion detection systems)
- 암호화 (crytography)
- 키 관리 (key management)
- 프로토콜 안전성
- OS 안전성
- 기술 표준 및 가이드라인
- 기타

2.3 연구 활동

미국에서는 DOE를 중심으로 제어시스템 사이버 안전성 문제를 핵심 연구 기술로 선정하여 중장기적인 연구를 수행하고 있는데, SCADA, DCS(Distributed Control System)와 기타 제어시스템들이 주 대상이며, 그림 2는 이와 관련된 연구 및 기타 활동을 나타내고 있다[3]. 그림 2에서 기관별 정식명은 표 1과 같다.



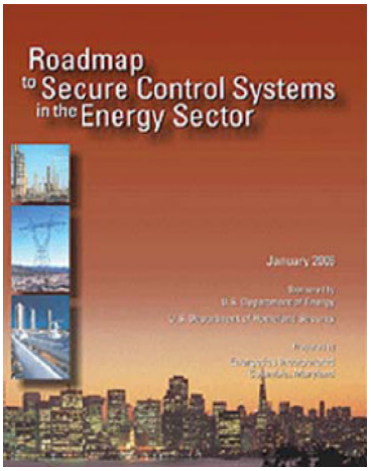
〈그림 2〉 Cyber Security와 관련된 연구 활동[3]

〈표 1〉 연구 기관

Abbr. Name	Full Name
AGA	American Gastroenterological Association
EPRI	Electric Power Research Institute
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
FERC	Federal Energy Regulatory Commission
NERC	North American Energy Reliability Council
NIST	National Institute of Standards and Technology
NSF	National Science Foundation

2.4 기술 개발 로드맵

진행되고 있는 다양한 연구 활동들을 더욱 효율적으로 진행하기 위하여 2006부터 2015년까지 10년간의 기술개발 로드맵을 이미 작성하여 연구를 수행하고 있다[4].



〈그림 3〉 제어시스템들의 Cyber Security 연구 개발 로드맵[4]

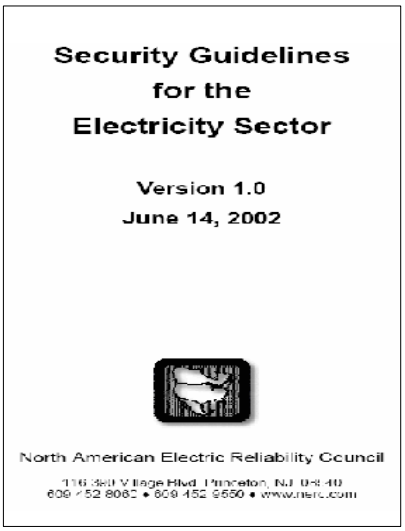
2.5 Test Bed

개발한 Cyber Security 기술을 검증하기 위하여 미국의 국가연구소인 Sandia National Lab과 Idaho National Lab에 미션을 주어 SCADA Test Bed를 개발하고 설치하여 운영하고 있다.

〈그림 4〉 Idaho National Lab.의 SCADA Test Bed

2.6 가이드 라인 및 기술표준

북미 전기 신뢰도 위원회(NERC)는 2002년부터 물리적인 Security 뿐만 아니라 Information Technology/Cyber Security에 대해서 가이드라인과 기술표준을 정하고 전력설비와 전력시스템, 관련 기기 등에 적용하고 있으며, 해마다 갱신하여 상용화와 보급에 힘쓰고 있다.



〈그림 5〉 NERC의 Security 가이드라인[5]

2.6 기타

그 이외 많은 대학과 컨설팅회사, 중전기기 및 IT 관련 회사 등이 Cyber Security에 대한 연구를 수행하고 있다.

3. 결 론

전력을 안정적으로 공급하는 것은 국가차원에서도 중요한 문제이다. 전력시스템이 지형적으로 광범위하게 분산되어 있기 때문에 전력시스템의 감시, 제어 등의 기능은 통신 매체를 이용하여 운용되고 있으며, 따라서 사이버 공간에서 안전성을 확보하는 것은 안정적인 전력 공급과 직결되는 문제다. 이런 이유로 최근 전 세계적으로 전력 IT의 Cyber Seucrity에 대한 관심이 고조되고 있으며, 이에 대한 다양한 연구가 진행되고 있다.

본 논문에서는 미국을 중심으로 전력 IT Cyber Security 분야에서 진행되고 있는 연구 동향을 소개하였다. 국내의 전력 IT 환경에서 현재 독립적으로 운용되고 있고 또한 개발 중에 있는 많은 시스템들이 추후에는 연계 운용될 것으로 전망된다. 따라서 국내에서 사이버 공간에서 안전성 문제가 구체적인 현안문제로 대두될 것으로 예상된다. 현재 국내에서 Cyber Security에 대한 많은 연구가 이루어지지 못하는 실정이지만 점차 전력 IT Cyber Security에 대한 관심이 고조되고 있으며, 현재 한국전기연구원과 일부 대학을 중심으로 기초적인 전력 IT Cyber Security에 대한 연구가 진행되고 있다. 추후 다양한 참여 기관의 참여를 기대하며 또한 본 논문에서 소개된 연구 동향이 국내에서 추후 추진될 더욱 다양한 전력 IT의 Cyber Security 연구 분야에 많은 활용이 되길 기대한다.

[참 고 문 헌]

[1] John Douglas, Grid Security in the 21-th Century, EPRI Journal, 2005

[2] J. Eisenhauer, P. Donnelly, M. Ellis and M. O'Brien, Roadmap to Secure Control Systems in the Energy Sector, Report, January 2006

[3] Hank Kenchington, Securing Control Systems in the Energy Sector", Presentation Material, DOE

[4] Rolf Carlson: *Sandia SCADA Program: High-Security SCADA LDRD Final Report*, Sandia Report, SAND2002-0729, April 2002

[5] NERC, Security Guidelines for the Electricity Sector, June 2002

[6] T. Kropp, "System Threats and Vulnerabilities", IEEE Power & Energy Magazine, pp. 46-50, March/April 2006

[7] H.M. Kim, D.J. Kang, "Security Issues & Application in Korea SCADA", Journal of the Korean Institute of Illuminating and Electrical Installation Engineers, Vol.21, No.9, pp.76-80, Nov. 2007.

[8] 김학만, 강동주, "전력 IT 네트워크 보안 전망", 2007년 대한전기학회 전력기술부문회 추계학술대회논문집, 2007

[9] 김학만, 강동주, "SCADA 네트워크 보안 이슈", 2007년 대한전기학회 전력기술부문회 추계학술대회논문집, 2007