전력 IT Cyber Security 취약성 검토

김학만, 박재세, 정동효
시립인천전문대학

Consideration of Cyber Security Vulnerability in Power IT

Hak-Man Kim, Jae-Se Park and Dong-Hyo Joung
Incheon City College

Abstract - Power IT is very important infrastructure in the country. In general, Power IT is disclosed to cyber attacks. To enhance cyber security in Power IT area, first of all, vulnerability in the area should be defined. In this paper, we consider the cyber security vulnerability in Power IT and introduce the vulnerability. Also, we suggest the research areas for enhancing cyber security in Power IT.

1. 서 론

전력의 안정적인 공급은 국가적인 차원에서 중요한 문제이다. 최근 IT(Information Technology) 기술의 발달로 전력시스템의 감시와 제어는 IT과 접목되어 이루어지고 있으며, 전력시스템이 지역적으로 광범위하게 분산되어 있어 통신 매체를 통하여 이루어지고 있다. 전력시스템의 안전성을 유지하기 위하여 시스템 자체의 기능과 성능의 고도화도 중요하지만 사이버 공간에서의 안전성 또한 중요한 문제이다.

특히, 최근 전 세계적으로 발생하는 사이버 공간에서의 문제에 의해서 전력공급이 원활하지 못한 경우가 발생하고 있으며, 이에 대해서 Cyber Security 향상을 위한 많은 연구와 노력들이 이루어지고 있는데, 국내에서도 이에 대한 발생 가능성을 우려하고 있으며, 이와 관련된 기초적인 연구가 진행되고 있다.

본 논문에서는 전력 IT에서 가장 중요한 해결 문제 중의 한 가지인 Cyber Security의 취약성에 대해서 검토하였다. 구체적으로 이를 위해서 외국에서 조사된 문헌을 토대로 취약성에 대해서 검토하였고 이를 소개하고자 한다. 또한 전력 IT의 발전 전망에 전력 IT의 Cyber Security 향상을 위한 연구 분야를 제시하였다.

2. 전력 IT Cyber Security 취약성

2.1 전력 IT의 사이버 공격

그림 1은 외국에서 발생한 2002년에서 2004년 사이 산업용 제어 시스템 별 사이버 공격의 비율을 보여주는데, 이 중에서 전력산업과 관계하여 빈도가 약 20%를 차지하고 있는 것을 보여준다. 그림 2는 사이버의 공격이 2001년 이전의 경우는 내부인에 의해서 발생하는 것이 많은 비중을 차지한 반면, 2001년 이후에는 외부에서 의도적으로 이루어지고 있음을 나타내고 있다. 그리고 외부에 의한 의도적인 사이버 공격이 점차 증가할 전망이다.

2.2 Cyber Security 취약성

전력 IT Cyber Security 취약성은 사이버 공간에서 외부에서 해킹과 바이러스, 악성코드 등의 수단을 이용하여 고의적으로 공격하는 행위에 대한 취약한 가능성을 의미하며, 이는 또한 전력 IT Cyber Security 향상을 위한 보안 정책, 수단 개발에 중요한 기본 자료가 된다.

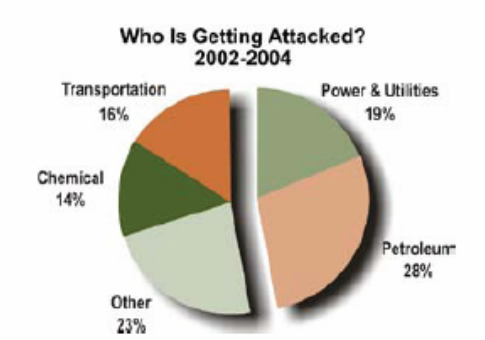
그림 3은 일반적인 프로세서 제어 시스템의 보안 운영을 도시화 한 것으로 전력 IT 시스템에도 적용되며, 효율적인 시스템의 보안 운영을 위해서는 Cyber Security의 취약성의 분석이 그 출발점이라 할 수 있다. 외국에서 발간된 자료 [1-3]를 토대로 소개된 전력 IT 시스템의 취약성을 분석하여 정리하면 다음과 같다.

2.2.1 운영 시스템의 취약성

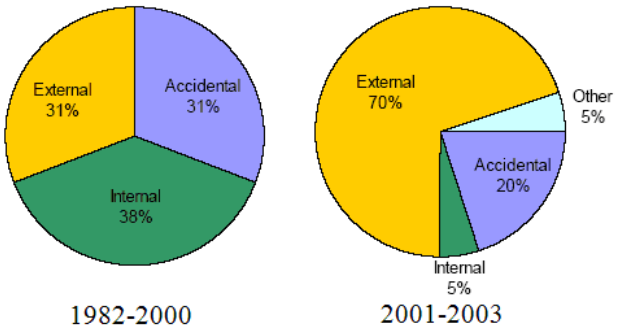
운영 시스템은 마이크로 소프트, UNIX와 같은 범용적인 운용체계를 사용하는 등 표준적인 기술로 구성되어 있어 이와 관련되어 이미 취약성은 많이 노출되어 알려져 있으며, 따라서 운영 시스템에서 취약성이 내재되어 있다.

2.2.2 통신망의 취약성

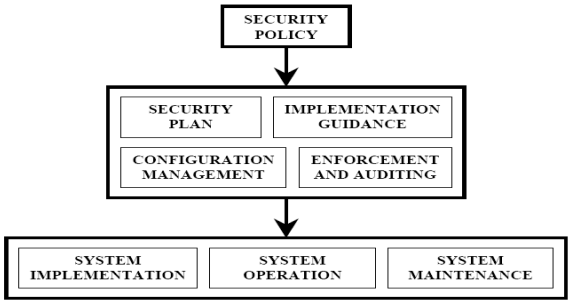
전력 IT의 통신망은 현재는 광통신 기반 전용망을 많이 활용하지만, 광통신의 경우에도 외부에서 tapping을 통한 네트워크의 공격이 가능한 것으로 알려져 있으며, 특히, 공격자가 전문가로 구성될 경우에는 쉽게 공격되어 진다[4]. 또한, 점차 TCP/IT 통신이 보급될 전망인데, 이 경우는 이미 취약성이 널리 알려져 있다. 특히, 시스템의 공급자의 보수유지 등의 목적으로 된 외부 네트워크와의 연계는 공격의 가능성이 더 높아진다.



<그림 1> 다양한 산업의 제어 시스템에 대한 사이버 공격 [1]



<그림 2> 사이버 공격 유형 [2]



<그림 3> 프로세서 제어 시스템의 보안 운영 [3]

2.2.3 전력 IT 시스템의 안전 운영 측면

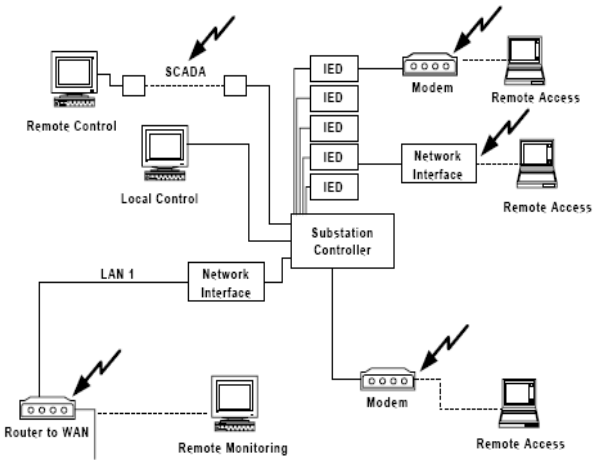
표 1은 프로세서 제어 시스템의 안전 운용 측면에서의 취약성을 나타낸 것으로 포괄적인 전력 IT 시스템에서 표 1과 같이 안전 운영 측면에서의 취약성 문제가 있다.

<표 1> 프로세서 제어 시스템의 안전 운영 측면에서의 취약성 [3]

분류	취약성
정책	- 상세하게 문서화된 보안 정책이 없음
절차	- 상세하게 또는 문서화된 보안 계획이 없음 - 설비와 시스템에 대한 수행 가이드가 없음 - 시스템 lifecycle에서 안전성을 강제하기 위한 행정적인 메카니즘이 없음 - 안전성의 감사가 거의 없거나 없음
훈련	- 정규적인 안전성 훈련이나 공식적으로 문서화된 안전 절차가 없음
구성 관리	- 형식적인 구성 운형이 없거나 사무적으로 공식적으로 문서화된 절차가 없음

2.2.4 변전소 사이버 취약성 예시

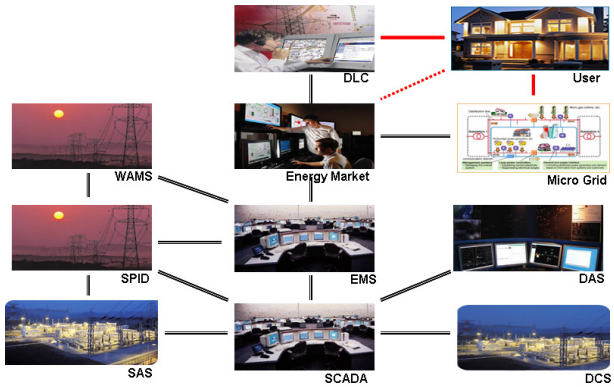
그림 4는 가상적인 변전소 구성에서의 취약성을 나타낸다. 그림 4에서 IEDs(Intelligent Electronic Devices), 제어기, SCADA(Supervisory Control and Data Acquisition) 시스템에 원격 접근을 수행할 때 다중의 취약성이 존재함을 확인할 수 있다.



<그림 4> 변전소 시스템에서 보안 취약성 [5]

2.3 전력 IT 전망과 Cyber Security 향상

그림 5의 나타나 있는 개별 전력 IT 시스템들은 궁극적으로 그림 5와 같이 네트워크들이 연계 운영될 전망이다. 통합 운영될 경우 개별 네트워크나 시스템에서의 사이버 취약성은 전체 전력 IT 시스템에 악영향을 미치며, 사이버 공격이 가해졌을 때 그 손실은 전시에 준하는 국가적인 문제가 될 것으로 예상된다.



<그림 5> 전력 IT의 통합 운영 전망 [6]

그림 5에서 시스템별 정식 명칭은 표 2와 같다.

<표 2> 전력 IT 시스템

Abbr. Name	Full Name
DAS	Distribution Automation System
DCS	Distributed Control System
DLC	Direct Load Control
EMS	Energy Management System
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SPID	Strategic Power Infrastructure Defense
WAMS	Wide Area Measurement System

Cyber Security 향상을 위해서 다음과 같은 다방면에서 연구와 보급이 이루어져야 한다.

- 보안 정책
- 취약성 분석
- IT 시스템 모델링
- 시스템 접근제어
- 전력 IT 시스템의 프로토콜별 전용 방화벽
- 침입 탐지 시스템
- 시스템 및 통신 데이터 암호화 및 키관리 기술
- 프로토콜 자체 안전성
- IT 시스템 탑재 s-OS
- 기술 표준
- 보급 확대를 위한 가이드라인
- 기타

3. 결 론

국가의 주요 에너지원인 전력을 감시, 제어하는 전력 IT는 점차 IT의 기술이 발달하여 전력시스템의 많은 개별 시스템이 IT와 접목되어가고 있다. 전력 IT에서 Cyber Security 문제는 전력시스템 전체의 문제로 발전되고 또한 국지적인 문제가 아닌 국가차원의 문제로 확산된다. 이런 이유로 전력 IT Cyber Security 향상을 위해서 선행되어야 하는 것이 보안의 취약성을 파악하고 분석하는 것이다.

본 논문에서는 전력 IT에 대한 사이버 취약서을 검토하여 이를 소개하였다. 또한 장기적으로 전력 IT의 발전 방향과 전력 IT의 Cyber Security 향상을 위한 연구 분야에 대해서 제시하였다. 본 논문에서 소개한 전력 IT의 사이버 취약성과 향상을 위한 연구 분야는 추후 전력 IT Cyber Security 향상을 위한 연구의 기본 자료로 활용이 예상되며, 또한 보안 정책 수립의 기초 자료로 활용이 기대된다.

[참 고 문 헌]

[1] Jack Eisenhauer, Paget Donnelly, Mark Ellis, Micheal O'Brien, Roadmap to Secure Control Systems in the Energy Sector, Energetics Incorporated, Colombia, Maryland, 2006

[2] Eric Byres, Justin Lowe, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, British Columbia Institute of Technology, PA Consulting Group

[3] J. Stamp, J. Dillinger, W. Young and J. DePoy, Common Vulnerabilities in Critical Infrastructure Control Systems, Sandia National Lab. Report, May 2003

[4] K. Witcher, Fkiber Optics and Its Security Vulnerabilities, Report, Univerity Mary Washington, Feb. 2005

[5] P. Oman, E. Schweitzer, and J. Roberts, "Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions". Proceedings of the 2001 Western Power Delivery Automation Conference, Paper No. 1, April 2001

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