전력 IT 기반 스마트 파워그리드 실증 보안 체계 설계

이명훈* · 배시화** · 손성용***

A Security Design for a Smart Power Grid Field Test based-on Power IT Systems

Myung-Hoon Lee* · Si-Hwa Bae** · Sung-Yong Son***

이 논문은 지식경제부 전력산업 연구개발사업(2010101040003B)의 지원으로 연구되었음

요 약

최근 진행되고 있는 제주 스마트그리드 실증에서 스마트 파워 그리드는 특히 기존의 전력 IT 기술의 통합을 통한 전력 계통 운영의 개선을 목표로 하고 있다. 스마트 파워 그리드의 구축을 위해서는 전력망의 실시간 양방향 통신과 상호연동성이 필수적이다. 그러나, 스마트그리드의 도입으로 인한 무선 센서 수와 통신망의 외부 노출 기회의 증가는 전력망의 보안 취약점을 증가시킨다. 또한, 통신망의 데이터 도청 및 위변조 공격을 통한 해커의 공격은 전력 계통 시스템에 대한 혼란을 야기 시킬 수 있다. 스마트 파워 그리드는 스마트그리드의 추진을 위해 가장 핵심이 되는 시스템의 하나로 문제의 발생시 스마트그리드의 존립을 위협하게 되므로 체계적인 보안 설계가 필수적이다. 본 논문에서는 국내외 스마트 그리드 보안 표준 및 전력 계통 시스템의 보안 취약점 및 요구사항 분석을 기반으로 스마트 파워 그리드 실증을 위한 2단계 보안 서비스 모델을 제안하였다.

ABSTRACT

Smart power grid is targeting to improve grid operation by integrating existing power IT technologies in the jeju smart grid field test. Real-time two-way communication and interoperability in power grid are essential to smart power grid. Adopting smart grid will increase security vulnerabilities in power grid by increasing the number of wireless sensors and the chances of the external exposure of communication networks. In addition, hackers can cause chaos in the power grid system with eavesdropping and forgery attacks in communication networks. Smart power grid is one of the most important systems in deploying smart grid, and it is important to design security system systematically since smart grid can be seriously damaged when problem occurs. In this paper, local and global smart grid security standard and security vulnerabilities in power grid are reviewed, and 2 level smart grid service model is proposed.

키워드

스마트 파워 그리드, 보안 체계, 전력 IT, 통합 실증

Key word

Smart Power Grid, Security Design, Power IT, Field Test

* 퓨쳐시스템
** 경원대학교
*** 경원대학교 (교신저자, xtra@kyungwon.ac.kr)

접수일자 : 2010. 09. 10
심사완료일자 : 2010. 11. 04

Ⅰ. 서 론

2004년 전력망 고도화를 위한 핵심 기술의 확보를 목표로 전력IT 10대 과제가 추진되었고, 추후 개발 기술의 성장 동력화의 필요성이 제기됨에 따라 실계통에서의 검증을 통한 조기 상용화를 위해 전력IT 실증사업이 추진되었다. 초기 전력IT 실증사업은 전력IT 10대 과제의 통합 검증을 중심으로 설계되었다. 그러나, 스마트 그리드의 이슈화에 따라 제주 실증사업은 스마트 그리드를 중심으로 스마트 플레이스, 스마트 트랜스포테이션, 스마트 리뉴어블, 스마트 서비스, 스마트 파워그리드 등 5개 분야로 재편되었다.

스마트 파워 그리드는 전력 계통 시스템의 효율적이고 안정적인 운영을 위해 SCADA, DAS, AMI 등의 내·외부 시스템과 상호 연동되며 소비자에 대한 실시간 전력정보 제공을 위하여 직·간접적으로 인터넷과 연동되기 때문에 "시스템의 접점 증가, 구성 장비 간 상호연결성 증가, 장비의 외부 노출에 의한 해커의 광범위한 접근 가능성, 상용 하드웨어와 소프트웨어 사용 증가" 등의 변화로 사이버 공격에 대한 위협요소는 증가될 것이다. 또한, 상호운용성 보장을 위한 실시간 양방향 서비스의 제공에 따라 외부 접속 구간 및 인터넷 연계구간을 이용하여 전력 계통망 접근에 따른 취약점에 노출될 것이다[1,2].

본 논문에서는 스마트 파워 그리드 보안 체계 설계를 위하여 국내외 보안 표준 및 지침을 분석하고, 제주 실증을 위한 스마트 파워 그리드 사업 범위 및 시스템 구성에 대하여 살펴보았다. 또한 전력 계통 시스템, 네트워크 통신, 사용자 관점에서 보안 취약점 및 요구사항 분석을 기반으로 스마트 파워 그리드 보안 체계를 설계하였다.

Ⅱ. 관련 연구

2.1 전력 IT 10대 과제

전력IT 통합 실증 연구과제는 전력망과 정보통신망을 융합하여 전력 설비의 안정화 및 고도화를 통해 국가경제의 발전을 도모하고, 연구 성과물의 해외시장 진출을 위한 기반 기술 확보를 목표로 하고 있다. 이러한 목표 하에 정부 주도의 산·학·연 88개 기관이 참여하여 공동연구 방식으로 표 1과 같이 10대 과제가 추진되었다[3].

표 1. 전력 IT 10대 과제 목록
Table. 1 the List of 10 Power IT Projects

총괄 과제명	총괄기관	사업 기간
IT 기반의 대용량 전력 수송 제어시스템	KEPCO	05.12~ 10.11
디지털 변전 시스템	KEPCO	05.10~ 11.09
배전 지능화시스템	KEPCO	05.10~ 10.09
UPLC 기술개발 사업	KEPCO	05.10~ 10.09
한국형 에너지 관리 시스템	전력거래소	05.11~ 10.10
지능형 송전 Network 감시 운영시스템 기술 개발	한국전기 연구원	05.10~ 10.09
능동형 텔레메트릭스 전력설비상태 감시 시스템	한전 KDN	05.12~ 09.11
M-Grid용 통합에너지 관리 시스템 개발	한국전기 산업조합	07.09~ 12.08
고부가전력서비스 수용가 통합자원 관리 시스템	경원대 산학협력단	05.10~ 10.09
분산발전 및 산업용 인버터용 전력반도체 기술	반도체 연구조합	05.12~ 10.11

2.2 스마트 그리드 해외 보안 동향

- NIST CSCTG(Cyber Security Coordination Task Group)

NIST CSCTG는 벤더, 서비스 제공자, 학계, 규제 위원회, 연방 정부 등 200개 업체 이상이 참여하였고, 사이버 보안 표준을 기반으로 스마트 그리드를 위한 보안 전략 전반에 걸쳐 도메인 형식이나 일반적인 위협요소, 시스템 특징별 보안 요구사항, 상호운용성을 기반한 보안 기능 등 유무선 정보통신에서 발생 가능한 보안 요구사항의 제시를 목적으로 하고 있다. NIST CSCTG는 스마트 그리드 보안 표준 제정을 위하여 보안위협에 대한 시나리오를 선정·분석하고, 취약점과 위협에 대한 위험 평가를 수행하고 있으며, 스마트 그리드 인프라 및 인터페이스 연결에 따른 보안 구조 개발과 사이버보안 표준 및 적합성에 대한 평가를 수행중이다.

2010년 02월에 발표된 "Smart Grid Cyber Security Strategy and Requirement" 드래프트 문서에서 스마트그리드의 사이버 보안 위협 관리 기반과 전략 수립을 위한 사이버 공격의 위험요소로 정보통신과 전력망 통합에 따른 통신 회선의 추가로 인한 "의도되지 않은 공격의 발생가능성 증가, 내부 통신 네트워크의 일반적인 취약점이 등장, 소프트웨어와 시스템의 통합에 따라 악의적인 소프트웨어가 등장, 통신 경로 및 접속 지점의 증가에 따라 취약점이 증가, 고객의 개인 정보 노출에 따라 사생활 침해가 가능" 등의 측면을 제시하였다. 또한, 이러한 위험을 사전에 방지하기 위하여 사이버 보안을 고려한 use cases를 선택하고, 상위수준 보안 요구사항 정립을 위하여 표2와 같이 18범주의 논리적 인터페이스를 제시하였다[4,5].

표 2. 보안 설계를 위한 논리적 인터페이스
Table. 2 Logical Interface Categories for Security Design

No	구분	No	구분
1a	고가용성, 대역폭	9	센서네트워과제어
1b	대역폭제약 조건	10a	AMI 네트워크
1c	고가용성	10b	고가용성 AMI
1d	고가용성의 대역폭	11	소비자 네트워크
2a	내부 제어시스템	12	외부 시스템과 소비스 사이트
2b	외부 제어시스템	13	시스템과이동장치
3a	내부 업무지원	14	계량 장비
3b	외부 업무지원	15	운영 결정 지원
6	B2B 연결	16	유지보수시스템과 제어장치
7	제어시스템과 비제어	17	제어시스템과벤더
8	환경 매개변수 측정 센서 네트워크	18	관리 콘솔과 네트워크 시스템

그리고 각각의 논리적 인터페이스를 대상으로 표3과 같이 기밀성(C), 무결성(I), 가용성(A)에 대한 보안의 영향력에 따라 보안 서비스의 수준을 높음(H), 보통(M), 낮음(L)으로 구분하여 보안 레벨을 제시하였다.

표 3. 18범주에 대한 보안 레벨
Table. 3 Security Levels for 18 Categories

구분	C	I	A	구분	C	I	A
1a	L	H	H	9	L	M	M
1b	L	H	M	10a	L	H	L
1c	L	H	H	10b	L	H	H
1d	L	H	M	11	L	M	M
2a	L	H	M	12	L	M	L
2b	L	H	H	13	L	H	M
3a	L	M	L	14	L	H	L
3b	L	M	L	15	L	H	M
6	L	M	M	16	L	H	M
7	L	H	M	17	L	H	L
8	L	M	M	18	H	H	H

- UtiliSec

UtiliSec은 UCA International Users Group (UCAIug)의 Open SG(Smart Grid) 산하 그룹으로 ASAP-SG에서 제시하는 보안 요소 및 청사진에 따라 Open SG와 함께 스마트 그리드 응용 시스템과 관련된 사이버보안 이슈 사항에 대하여 벤더 중심으로 표준 개발을 진행하였다. 2008년 12월 UtiliSec의 하위그룹인 AMI-Security TF에서 공개한 "AMI System Security Requirements v1.01 (SSR)"는 AMI 시스템 보안을 위하여 기밀성, 무결성, 가용성, 식별, 인증, 권한 부여, 부인 봉쇄, 과금 등에 대한 요구사항을 제시하였고, 이를 현실화하기 위한 기술로 오류 검색, 범위 서비스, 암호화, 메시지 통보, 자원관리, 신뢰와 인증 등 시스템 보안 요구사항에 대하여 제시하였다[6,7].

- IEC 62351

전력망의 데이터 전송을 위한 보안 표준인 IEC 62351은 전력 계통 시스템의 제어·운영 메시지 전송을 위한 정보보호 표준이다. IEC 62351은 표 4와 같이 1~8 시리즈로 구성되었고, IEC 60870, 61850, 61970, 61968 시리즈에서 정의한 프로토콜의 종단간 보안문제 해결을 위하여 제정되었다. 이 표준은 기밀성, 무결성, 가용성, 부인봉쇄 등 보안 요구사항에 대한 서비스 제공을 위하여 프로토콜의 접근 방법에 따라 네트워크 통신 데이터 보호 방안을 제시하였다. 그러나, 보안 서비스는

시스템 간의 통신 데이터를 기준으로 제시하였기 때문에 보안 정책, 보안 시행, 침입 탐지, 내부 시스템과 응용의 온전성 등의 추가적인 보안 서비스 제공 방안이 필요하다[8].

표 4 IEC 62351 보안 표준
Table. 4 IEC 62351 Security Standard

표준	보안 범위	보안 요구사항
62351-3	TCP/IP를 이용한 원격 조작	기밀성, 무결성, 메시지 수준 인증 제공
62351-4	MMS, ISO 9506 프로토콜 통신	응용(5~7) 및 전송 계층(1~4)에 대한 요구사항
62351-5	원격제어 장비와 시스템의 전송	응용계층에 대한 보안 제공
62351-6	61850에 기반한 모든 프로토콜	변전소 통신보안을 위해 암호화 제공
62351-7	단말간의 통신 프로토콜	네트워크/시스템 관리
62351-8	61850 데이터의 접근 제어	Role-Based 접근 통제

2.3 국내 스마트그리드 보안 동향

- 한국 스마트그리드 사업단 표준 동향

한국 스마트그리드 사업단은 2009년 8월 지식경제부 산하의 재단법인으로 스마트그리드 사업을 총괄 관리하여 2030년까지 세계 최초 국가단위의 스마트그리드 구축을 목적으로 설립되었다. 사업단은 실증단지의 각 컨소시엄간의 정보 교환을 위한 인터페이스 및 상호운용성에 대한 표준을 제정하고 있으며, 시험 인증 및 사이버 보안 지침 확보를 목표로 운영 규정 개정안을 추진하고 있다[9].

실증단지 사이버 보안 지침 분야에서는 제주 스마트그리드 실증단지의 구축 및 운영에 관한 사이버 보안 확보를 목표로 하고 있으며 표 5와 같이 "통합운영센터와 기간시스템 연계 구간 보호, 정보통신망 보호, 정보시스템 보호, 컨소시엄 운영센터와 기기 연계 구간 보호"으로 보안 서비스 영역을 분리하고 있으며, 사이버 공격 대응 및 조치를 위하여 통합 보안관제를 위한 체계의 지원에 대하여 명시하고 있다.

표 5 한국스마트그리드 사업단 보안 지침
Table. 5 Korea Smart Grid Institute Security Guide

구분	연계 구간	보안 요구사항
Legacy 망 연계	전력거래소, EMS 송, 변전 시스템 배전 시스템	-시스템 연결 일원화 -접점에 침입차단시스템 설치 -망연결 구간에 DMZ 설치
통신망 보호	TOC와 컨소시엄 운영센터	-데이터의 위변조 방지 -침입차단 및 방지시스템 설치
시스템 보호	TOC와 컨소시엄 운영체제	-악성코드 탐지 -보안패치 최신 유지 -불필요한 서비스 제거 -사용자 접근 인증
내부 시스템	스마트 기기와 컨소시엄 운영센터	-사용자 접근 및 기기 인증 -시스템 접근 통제
관제센터	TOC	-통합보안관제 수행
	컨소시엄 운영센터	-사이버 공격 모니터링 -보안관제 수행 -TOC의 보안 관제 지원

Ⅲ. 스마트 파워그리드 보안체계 설계

스마트 파워 그리드의 보안 체계 설계를 위하여 우선 전력 IT와 스마트 파워그리드 과제의 연구 내용과 실증 범위를 조사하였다. 스마트 그리드 보안 표준 및 지침을 기반으로 스마트 파워그리드의 보안 취약점 및 요구사항을 전력 계통 시스템, 네트워크 통신, 전력망 내부 사용자로 구분하여 분석하였고, 전력 IT 과제 실증에 따라 발생가능한 문제의 사전 예방을 위한 보안 체계를 설계하였다.

3.1 스마트 파워 그리드 실증 범위

전력 IT 10개 연구과제 성과물을 상호 연동하여 실증하고, 그 결과를 기반으로 전국의 전력망에 확대 적용하기 위하여 2008년 12월 KEPCO를 비롯한 산·학·연 13개 기관과 전력 IT 통합실증기술개발 및 Test Bed 구축을 위한 협약을 체결하였다. 그러나, 2009년 4월 CO_2 배출 감축 및 에너지 소비절감 등 환경문제에 대응하고, 녹색성장기술 조기 개발 및 선점으로 미래의 신성장 동력 창출을 위해 기존 전력 IT 실증사업은 스마트그리드 실증사

업으로 확대되었고, 기존 전력 IT 실증사업은 Smart Power Grid로 변경되면서 연구범위가 전력IT 4개 연구 성과물 실증으로 축소화되면서 스마트그리드 실증사업을 지원하게 되었다.

초기 전력IT 연구 성과물의 통합실증을 위한 통합 실증 계획은 K-EMS/SCADA, 디지털 변전, 배전 지능화를 중심축으로 실증플랜트 통합 미들웨어에서 데이터 수집하고, 기존의 발전에서 소비자단으로 연결되는 전력망에 각각의 연구 성과물을 병렬로 설치하여 실증하도록 구성하였다. 그렇게 되면 실계통에서 오동작을 예방하고, 기존 시스템과 신규 개발된 기기의 성능을 안전하게 규명할 수 있기 때문에 전력IT 10대 과제의 통합 실증이 가능하였다. 그러나, 과제 범위가 변경되면서 지능형 송전, 디지털변전, 능동형 텔레메트릭스, 배전지능화 등 전력IT 4개 연구 성과물에 대한 실증을 중심으로 범위가 축소되었다.

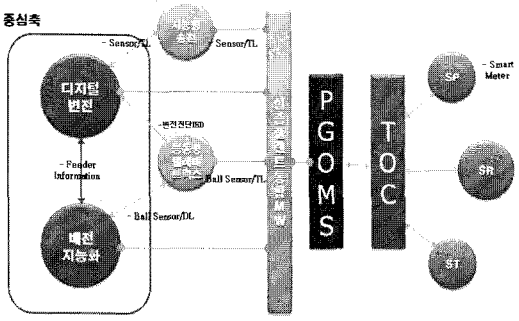

그림 1. 제주 실증 스마트 파워그리드 구성
Fig. 1 Smart Power Grid in Jeju Field Test

3.2 스마트 파워 그리드 구성도

스마트 파워 그리드의 통합 실증을 위하여 그림 2와 같이 지능형 송전, 능동형 텔레메트릭스, 디지털 변전, 배전 지능화 등 전력 계통 시스템에서 수집한 현장 정보를 PGOMS에 전달하여 통합 운영하는 형태로 구성되었다. 전력 계통 시스템은 현장 정보를 수집하는 스마트 기기들과 수집된 정보를 DB 서버에 전달하기 위한 통합 모뎀, 정보의 수집 및 운영 관리를 위한 DB 서버로 구성되어 있으며, PGOMS는 전력 계통 시스템에서 수집된 정보를 제공받아 통합 운영을 위한 관제 시스템이다.

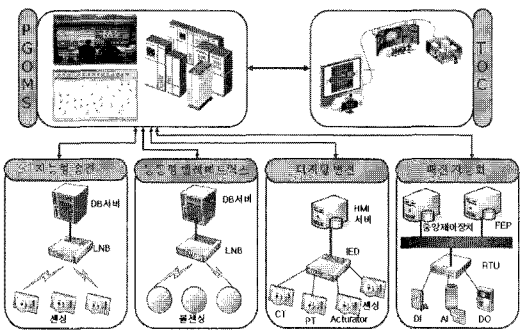

그림 2. 스마트 파워 그리드 시스템 구성도
Fig. 2 Smart Power Grid System Configuration

PGOMS는 TOC와 연동하여 전력 계통 시스템에서 수집된 운영 정보를 제공하고, Legacy, Smart Place (SP), Smart Renewable (SR), Smart Transportation (ST) 부문에 대한 정보를 제공받아 운영·관리 및 제어서비스를 제공한다.

3.3 보안 취약점

기존 전력 계통 시스템은 폐쇄망으로 구성되었고, 외부 노출 장비도 물리적인 보안 시스템 설치에 따라 외부 공격에 대한 위협을 사전에 차단하였다. 그러나 스마트 그리드의 도입에 따라 증가하는 스마트 파워 그리드의 보안 취약점을 네트워크, 시스템, 응용 프로그램으로 구분하여 위협을 분석하였다.

- 네트워크 보안 취약점

전력 계통 시스템에 새롭게 도입되는 외부 센서와 스마트 기기 등 많은 기기가 개방된 유·무선망을 이용하여 데이터를 전달하기 때문에 공격자는 데이터 접근에 따른 도청이 가능하고, 위변조 공격에 따라 바이러스나 웜과 같은 악의적인 프로그램 삽입과 센서 데이터를 이용한 DoS 공격에 대한 위협이 존재한다. 그리고, TOC 구간의 경우 SP, ST, SR 시스템과 연결되어 있으며, 각각의 시스템은 소비자의 전력 사용정보 등을 제공하기 위하여 인터넷과 연동되기 때문에 Zero Day 공격이 발생할 수 있으며, 제어 시스템을 손상에 따른 대규모 정전 위협이 존재한다.

- 내부 시스템의 보안 취약점

PGOMS 내부망에 공격자가 침입할 경우 로컬에 단말

을 연결하여 통신데이터의 도청이 가능하고, 공격자는 전력 계통 시스템 해킹에 따라 시스템 제어 권한을 획득하여 정전사태를 발생시킬 수 있다. 내부의 정당한 사용자가 시스템 조작의 실수로 정전사태가 발생할 수 있으며, 오염된 USB나 외부 저정장치 연결에 따라 제어 시스템에 악성코드가 전염되어 시스템을 마비시킬 수 있는 보안 위협이 존재한다.

- 응용 프로그램 보안 취약점

PGOMS에 설치 운영되는 시스템의 대부분은 윈도우나 리눅스 운영체제를 기반으로 구축될 것이고, 데이터베이스를 설치하여 고객 및 전력 사용정보를 저장할 것이다. 운영체제의 보안 취약점은 운영·관리의 편리성 제공을 위하여 FTP, TELNET과 같은 다양한 원격 접속 서비스를 설치할 것이고, 관리자는 원격으로 접근하여 서버 설정 또는 고객의 정보를 수정할 수 있다. 만약, 관리자 정보가 노출될 경우 외부에서 서버의 제어권을 얻게 될 것이고, 서버의 정보 및 연계 시스템까지 공격할 수 있는 취약점이 존재한다.

데이터 베이스 프로그램의 경우 고객 정보를 저장하고 있으며, 서버 관리자는 자유롭게 고객의 정보 확인할 수 있을 것이다. 만약, 관리자가 악의적인 의도로 데이터베이스에 접근할 경우 고객 정보를 추출하여 외부에 판매할 수 있으며, 고객의 전력 이용정보를 위변조하여 요금 정보에 혼선을 제공할 수 있다.

3.4 보안 요구사항

현재 정보통신망의 사이버 공격은 지능화되어 가고 있으며, 피해 범위도 범국가적인 차원으로 확대되고 있다. 이러한 지능화된 공격에 대응하기 위하여 네트워크·시스템 보안 및 보안 관제에 따른 트래픽 접근제어, 통합인증, 데이터 기밀성, 무결성, 가용성, 접근제어 등 데이터 보호 체계 설계 및 이상 트래픽, 자동 침입탐지, 분석, 대응 등 네트워크 통신 데이터 보호를 위한 보안관리 시스템 구축의 필요하다.

인증은 사용자 및 장치간 인증으로 구분한다. 사용자 인증은 시스템 내의 장치 인증외에 장치를 사용하는 사람의 신원확인을 위한 사용자 인증 기능이 반드시 필요하다. 제어망에서 생체인식, 패스워드, 인증서, 스마트카드 등 다양한 사용자 인증 기술의 활용이 가능하겠지만, 장치의 낮은 성능을 고려하여 사용자 인증 기술의 활용 및 적용성을 검토해야 한다.

SCADA 시스템을 안전하게 유지하고, 운영하기 위하여 중앙센터와 RTU 간의 안전한 데이터 통신이 가능해야 한다. 전화 또는 네트워크 회선을 통한 평문 통신의 경우 데이터 통신의 도청에 따라 스니핑과 같이 외부에서 데이터 도청에 따라 스푸핑, DoS, Replay 공격이 가능하고, 이러한 공격에 대하여 사전에 대비하기 위하여 기밀성을 제공해야 한다[10].

전력 계통 시스템의 센서들은 전력의 원활한 공급을 위하여 온도나 선로 정보를 주기적으로 측정된 정보를 기반으로 전력의 송신가능성을 검토하기 때문에 정확한 정보의 전달을 위한 무결성은 전력망에서 아주 중요한 보안 기술이다. 만일 전송되는 데이터가 악의적인 공격자에 의해서 변경된다면 장비의 오작동을 유발할 수 있고, 많은 보안 사고로 연결될 수 있기 때문에 메시지의 무결성을 제공해야 한다.

전력 계통 시스템에서는 정보통신망과 다르게 가용성이 기밀성보다 중요하다. 전력 계통 시스템은 지속적으로 전력 공급 및 회선에 대한 정보를 주기적으로 제공해야하며, 만일 어떠한 공격에 의하여 작동이 멈추게 되면 그 즉시 정전 피해가 발생하고, 원상태로 복구하기 위해서는 많은 비용과 시간이 소요된다. 그러므로 암호화와 같은 보안 대책은 가용성이 허용되어야 한다[11].

시스템내의 사용자 및 단말 인증을 위한 가장 유용한 방법은 인증에 따른 접근제어 방식의 도입이다. 접근제어는 다단계로 수행해야 하며, 물리적 접근과 시스템 접근으로 구분을 한다. 물리적 접근은 운영되는 서버실의 출입 권한에 대하여 정당한 이용자를 판별하는 기능으로 생체 인식이나 스마트카드를 이용하여 출입에 대한 신뢰성을 보장하고, 시스템 접근에서는 운영체계에서 제공하는 사용자 인증과정과 전력 제어 시스템에서 제공하는 접근제어 서비스를 제공해야 한다. 그러나, 현재 개발된 보안 장비는 정보통신망 시스템 성능을 기준으로 개발되었기 때문에 전력망 시스템과는 처리 성능 및 저장 공간, 통신 프로토콜 등 차이가 있다. 스마트 그리드가 현실화되는 과정에서 보안 기술을 정립하여 그리드 환경에 최적화된 보안장비 개발되어야 한다. 이러한 관점에서 보안 기술 정립을 위한 체계 설계는 표 6과 같이 보안 영역, 보안 요구사항, 적용 장비 분류하였고, 보안 정책 제정의 기준과 점검사항을 기반으로 구간별 상황에 맞는 보안 요구사항을 정립하였다.

표 6 스마트 파워 그리드 보안 요구사항 정립
Table. 6 Smart Power Grid Security Requirements

구분	보안영역	보안 요구사항	적용 장비
공통 사항	시스템 서버	사용자 인증, 바이러스	백신, SecureOS
PGOMS	TOC	기밀성, 무결성, 인증	방화벽, IPS
	내부	무결성, 가용성	방화벽, IPS
배전 지능화	PGOMS	무결성, 가용성	방화벽, IPS
	내부 통신	인증, 무결성	무선 데이터 보안
	내부 RTU	사용자 인증	물리적 보안 장비
변전 자동화	PGOMS	무결성, 가용성	방화벽, IPS
	내부 통신	인증, 접근통제, 무결성	무선 데이터 보안
	내부 IED	사용자/단말 인증, 네트워크 접근제어	무선 데이터 보안
지능형 송전 & 텔레메트릭스	PGOMS	무결성, 가용성	방화벽, IPS
	서버	무결성, 인증	무선 데이터 보안
	무선	기밀성, 무결성, 인증	무선 데이터 보안

3.5 보안 체계 설계

제주 실증 단지의 스마트 파워그리드의 보안 체계 설계에 있어 정보통신망 보안 서비스 동향을 반영하여 2단계 보안 모델을 설계하였다.

- 1 단계 보안 서비스 모델

1단계 보안 서비스 모델은 Legacy 시스템 및 전력 IT 과제에서 개발된 장비를 그대로 유지하면서 보안 서비스를 제공하는 모델이다. 보안 서비스는 정보통신망 보호, 정보시스템 내부 보안 등으로 구분하였고, 각 구간별 보안 요구사항 및 설치 장비에 대하여 제시하였다.

그림 3과 같이 구간별 데이터 보호를 목적으로 일반적인 보안 요구사항 "무결성, 기밀성, 인증" 등 보안 서비스를 제공을 목표로 설계하였다. 무결성, 기밀성, 부인봉쇄는 전력 시스템의 낮은 처리 성능을 고려하여 네트워크 기반의 보안 체계를 설계하였다. 인증의 경우 단말 접근을 위한 사용자 인증 방식으로 단말 해킹에 따른 피해를 최소화하기 위하여 Secure OS와 DB 보안 솔루션 도입에 대하여 고려하여야 한다. 추가적으로 네트워크에서 악의적인 공격을 사전에 탐지 및 차단을 위하여 방화벽과 IPS 장비 도입이 필요하고, 외부 노출 장비의 경우 해커의 침입을 사전에 탐지하기 위하여 물리적으로 접근 탐지 장치를 설치하여 운영해야 한다.

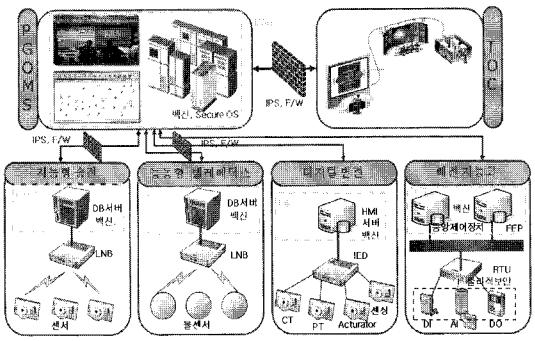

그림 3. 스마트 파워 그리드 1 단계 보안 모델
Fig. 3 Smart Power Grid Level 1 Security Model

- 2단계 보안 모델

2단계 보안 모델은 성능보다는 보안성을 강화한 모델이다. 보안 서비스는 정보통신망, 내부보안, 연계구간, 단말 인증, 관제 등으로 구분하였고, 각 구간별 보안 요구사항 및 설치 장비에 대하여 제시하였다.

그림 4와 같이 정보통신망 및 내부 보안은 1단계의 보안 장비에 추가적으로 네트워크 접근 통제를 위한 NAC(Network Access Control) 장비를 적용하고, 전력 IT 실증 서버와 데이터 통신을 위한 외부 연계구간은 서버 인증을 기반으로 기밀성 및 무결성 서비스를 제공을 위한 VPN(Virtual Privacy Network) 기술을 도입한다. 단말 인증 서비스는 인증서버를 도입하여 센서들에 대한 네트워크 통합 인증 서비스를 제공하고, 지역별로 통합 보안 관제 센터 운영 및 관리를 위하여 ESM(Enterprise Security Management), TMS (Threat Management System) 시스템을 설치하여 보안 장비의 로그 정보를 수집하여 실시간 보안 관제 서비스를 제공한다.

접근통제 장치의 기능을 스마트 기기 영역까지 확장할 경우 불법적인 접근에 대한 무결성 제공이 가능하고, 계통의 신뢰성 및 안정성을 향상시킬 수 있다. 그러나 네트워크 접근 통제도 신호의 위조 및 변조에 대한 대응이

어렵기 때문에 추가적으로 방화벽과 IPS(Intrusion prevention system)에서 수집된 공격 패턴 분석 및 통합 보안 관제를 위한 ESM 설치가 필요하고, Zero Day 공격과 같은 알려지지 않은 공격에 대한 대응을 위하여 TMS 도입이 필요하다.

보안관제 서비스는 관리 영역 내의 대상 서버나 네트워크 장비 등에 장비의 상태, 즉 훼손, 침입 등을 탐지할 수 있는 에이전트를 설치해 놓고 이를 보안 관제 센터에서 모니터링하는 형태의 서비스가 이루어지고 있다. 점차 시장의 확대와 요구사항의 변화에 따라 포괄적인 보안 장비 구축 컨설팅에서 취약점 점검 및 리포팅, 침입뿐만 아니라 바이러스 대응, 사후 데이터 복구, 직원들의 교육에 이르는 제반 보안 관련 업무들을 총체적으로 대행해 주는 전문 업체들이 늘어나고 있다.

추가적으로 보안 서비스 강화를 위하여 스마트 기기와 같은 내부 통신 장비의 무결성, 가용성, 기밀성 제공을 위한 단대단 전용 암호솔루션 개발에 따라 데이터 보안 서비스를 제공하고, 전력 계통 및 내부 RTU의 외부 침입을 사전에 차단하기 위한 네트워크 기반 접근 통제 시스템을 도입한다. 또한 관제 시스템은 외부 보안 관제 센터와 연계하여 신규 공격에 대한 실시간 정책 업데이트에 따라 능동형 보안 서비스 제공이 필요하다.

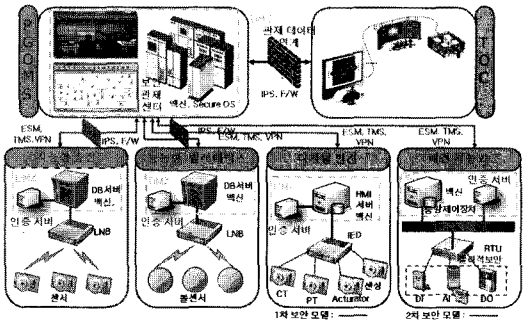

그림 4. 스마트 파워 그리드 2 단계 보안 모델
Fig. 4 Smart Power Grid Level 2 Security Model

Ⅳ. 보안 이슈 및 고찰

4.1 스마트 파워 그리드 보안 이슈

정보통신 기술과 전력망 융합에 따라 생기는 사이버 보안 위협에 대한 우려의 목소리가 높다. 지능형 전력망에서는 시스템의 안정적인 동작을 위한 중요 데이터들이 통신망을 통해 전송되는데, 이러한 데이터들은 누락되거나 변형되었을 시에 전력 서비스에 치명적인 영향을 줄 수 있기 때문에 스마트 그리드의 보안을 위해서는 암호화, 접근제어와 같은 다양한 보안 서비스가 제공되어야 한다.

전력망의 경우 가용성에 따른 실시간 서비스 제공을 중요시하고 있기 때문에 송신자의 데이터 가공 시간과 데이터 통신 채널 형성 시간, 데이터 통신 채널을 따라 수신되는 시간, 수신자가 메시지를 받아 재가공하는 시간이 모두 포함된다. 예를 들어, 전력선에 위치한 위상 측정 센서가 측정 정보를 변전소에 보내는 통신에서는, 센서가 전기 위상 값을 측정한 시점부터 변전소가 데이터를 받아서 위상 값을 읽는데 까지 걸리는 총 시간이 통신지연이 되기 때문에 통신 지연 조건이 만족되지 않으면 전력망에 치명적인 악영향을 줄 수 있기 때문에 가용성은 반드시 만족되어야 한다. 그러나, 메시지 암호화를 사용하면 암호화 알고리즘을 처리하기 위한 CPU 처리 시간이 늘어남으로써 전체 통신 시간을 지연시키기 때문에 실시간 통신을 요하는 환경에서는 보안서비스의 사용이 상당히 제한된다. 이러한 환경에서는 통신 지연 조건을 위반하지 않는 범위 내에서 적절한 보안 서비스를 선택하여 사용하여야 한다.

4.2 제안 모델 고찰

현재 실증 단지의 데이터 통신은 외부와 차단된 폐쇄망으로 구성되었기 때문에 네트워크망은 안전하다는 전제로 내용을 전개하였고, 이슈사항에서 제시한 것과 같이 시스템의 성능 문제를 중심으로 보안 모델을 설계하였다.

1 단계 보안 서비스 모델은 시스템의 성능에 미치는 영향을 최소화하고, 최고의 보안 효과를 제공하기 위하여 시스템 및 네트워크 보안으로 구분하여 보안 모델을 설계하였다. 시스템 관점에서는 내부자의 범죄가 전체 해킹의 70% 이상을 차지하기 때문에 내부자에 대한 정보 유출을 사전에 방지하기 위한 DB 보안 및 관리자의 조작 오류에 따른 피해 최소화를 위한 Secure OS에 대하여 제시하였다. 그리고, 전력 IT 과제의 결과물에서 전송하는 데이터의 신뢰성 향상을 위하여 PGOMS에 방화벽과 IPS를 설치하고, DMZ 구간을 생성하여 외부 데이터에 대한 악성코드나 유해 트래픽에 대한 차단 기능을 제

안하였다.

2 단계 보안 서비스 모델은 1단계의 보안 체계를 수용하면서 보안성 향상을 위한 인증 서비스 및 안정성 제공을 통합 보안 관제 서비스를 추가하였다. 보안성 향상을 위한 인증 서비스는 사용자 및 단말로 구분하였고, VPN 서비스를 기반으로 인증 및 기밀성, 무결성을 동시에 제공하는 방안을 제시하였다. 안정성을 위한 통합 보안 관제는 IPS나 IDS (intrusion detection system)와 같은 네트워크 보안 장비의 로그를 제공받아 네트워크 공격 위협 및 문제가 발생할 경우 실시간으로 대처하고, 외부 관제 센터와 연계하여 실시간으로 보안 취약점에 대한 사전 대응을 위한 시스템을 제안하였다. 1단계 보안 서비스 모델은 네트워크 성능 유지 측면에서 장점이 있는 대신 외부 공격에 대한 취약성이 여전히 존재한다. 2단계 모델은 보안성이 향상되는 반면 통신 속도의 저하를 발생시킬 수 있다. 따라서, 실질적 보안 시스템의 도입시에는 반드시 성능에 대한 검증이 병행되어야 할 것이다.

V. 결론

본 논문은 스마트 파워 그리드 통합실증 기술개발 및 Test Bed 구축에 따라 발생 가능한 보안 위협 및 취약점에 대한 사전 방어를 위하여 전력IT과제 및 국내외 스마트 그리드를 위한 보안 표준 및 지침에 대하여 분석하였다. 국내외 스마트 그리드 보안 표준 및 지침에서 국외의 경우 NIST와 UCAIug, IEC에서 제시한 보안 표준 및 드래프트 문서를 기반으로 스마트 파워 그리드를 위한 보안 취약점 및 요구사항에 대하여 조사하였다. 국내의 경우 스마트 그리드 사업단 및 한전 내부 스마트 그리드 ICT의 제주 실증을 위한 보안 지침에 대하여 분석하였고, 이를 기반으로 스마트 파워 그리드 실증을 위한 영역을 전력 계통 시스템, 네트워크 통신, 사용자로 분류하여 보안 취약점 및 요구사항에 대한 분석에 따라 스마트 파워 그리드 보안을 위한 2단계 보안 서비스 모델을 설계하였다.

참고문헌

[1] Tony Flick, "Hacking the Smart Grid", BlackCat.com, 2009. 6.

[2] JUDE CLEMENTE, "The Security Vulnerabilities of Smart Grid", Journal of Energy Security, 2009. 6. 18.

[3] 황우현, "전력IT 통합실증 기술개발 및 Test Bed 구축 추진 현황", 전기설비학회, 제23권 제6호, 2009. 12.

[4] Annabelle Lee, "Smart Grid Cyber Security Strategy and Requirements", NIST, 2010. 2.

[5] 장동원, 이영환, "스마트 그리드 표준화 동향 연구", 주간기술동향 1417호, 2009.10. 7.

[6] Bobby Brown, "AMI System Security Requirements", UCAIUG, 2008. 12.

[7] 이명훈, 김창섭, 손성용, "미국 스마트 그리드 사이버보안 동향분석", 주간기술동향, 2010.01.

[8] "IEC 62351 1-8:Power Systems Management and Associated Information Exchange-Data and Communication Security", IEC.

[9] 한국스마트그리드사업단장, "제주 실증단지 운영규정 개정(안)", 스마트 그리드 사업단, 2010.03.

[10] 김영진, 이정현, 임종인, "SCADA 시스템의 안전성 확보방안에 관한 연구", 정보보호학회, 2009. 09.

[11] 임일형 외, "배전자동화 시스템 통신망에 대한 사이버 공격에 대해 인증의 기법을 이용한 보안 알고리즘 적용방안", 대한 전기학회, 2008.01.

저자소개

이명훈(Myoung-Hoon Lee)

2001년 배재대학교 학사
2003년 배재대학교 석사
2006년 배재대학교 박사
2009년 ~ 현재 퓨쳐시스템 MSS 사업부 과장

※관심분야 : 스마트 그리드 보안, 그린 홈 보안

배시화(Si-Hwa Bae)

1976 서울대학교 건축학과 학사
1979 서울대학교 건축학과 석사
1992 서울대학교 건축학과 박사
1992년 ~ 현재 경원대학교
건축학과 정교수

※관심분야 : 스마트 그리드, 그린 홈

손성용(Sung-Yong Son)

2000년 Univ. of Michigan 박사
1992 ~ 1995년 LG 소프트웨어
2000 ~ 2004년 포디홈네트
2004 ~ 2005년 아이크로스테크
놀로지
2006년 ~ 현재 경원대학교 정보통신공학과 조교수
※관심분야 : 스마트그리드, 스마트홈