한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

Smart Grid 인프라의 보안성 분석과 보안기술정책 연구

박대우°, 신진*
°*호서대학교 벤처전문대학원
e-mail: prof1@paran.com, korjin@empal.com

A Study on Security Issues and Security Technology Policy about Smart Grid Infrastructure

Dea-Woo Park°, Jin Shin*
°*Hoseo Graduate School of Venture

● 요 약 ●

저탄소 녹색성장 정책의 일환으로 추진되는 Smart Grid 사업은, 전력인프라와 IT인프라가 융합 되면서 지능화된 전기 에너지의 효율성 향상을 목적으로 전기망 내 송배전을 실시간으로 관리할 수 있게 운영 하는 지능형 전기망이다. 하지만 기존의 인터넷망과 IT 통신 인프라와 융합되면서 Smart Grid 인프라에서도 IT보안 취약점 문제가 존재한다. 본 논문에서는 Smart Grid 인프라를 요소별로 분석한다. 그리고 Smart Grid 인프라의 보안성 분석을 통하여 보안의 취약점을 가져 올 수 있는 Smart Grid에 대한 보안 이슈를 분석한다. 그리고 Smart Grid 보안성 기준에 따른 보안기술정책을 연구하고, 보안 표준과 보안 방안을 제시한다. 본 연구를 통하여 안전한 Smart Grid 보안기술정책을 위한 법 제정에 기초자료가 될 것이다.

키워드: 스마트 그리드 인프라(Smart Grid Infrastructure), 보안 이슈(Security Issue), 보안기술정책(Security Technology Policy)

I. 서론

Smart Grid는 최근 국내에서 전기망에 통신망을 융합시켜 에너지 사용의 효율을 최적화하고 안정성을 높여 실시간으로 데이터를 교환함으로써 지능화된 전력 에너지의 효율성 향상을 목적으로 전기망 내 송배전을 실시간으로 관리할 수 있게 운영 하는 지능형 전기망이다.

2009년 7월 9일 이탈리아 라퀼라에서 개최된 G8 확대 정상회의 중에 열린 기후변화 주요국 정상회의(MEF)에서 대한민국은 기후변화 대응의 7대 전환적 기술 중 Smart Grid 기술에 대해 표 1과 같이 선도국가로 지정되었다[1].

지능형 전기망을 위한 안전한 전기 서비스를 위해서는 IT인프라에서 발생하는 보안 문제를 해결할 필요가 있다.

표 1. MEF의 7대 전환적 기술
Table 1. MEF's seven transitional technology

NO	기 술	선도국가
1	Smart Grid	한국
2	에너지 효율	유럽연합•일본
3	태양광에너지	독일
4	탄소포집 저장기술(CCS)	호주
5	바이오에너지	브라질
6	첨단자동차	미정
7	고효율 및 저탄소 석탄 기술	미정

또한 IT 정보통신 네트워크 및 전력IT기기에서 발생하고 있는 보안문제를 Smart Grid에서도 해결 되어야 한다[2].

본 논문에서는 Smart Grid 인프라에 대한 전력인프라와 IT인프라에 대한 보안성 분석을 통하여 AMI, 기반통신, 스마트제어, 서비스제공에서 Smart Grid 인프라의 보안성 분석을 통하여 보안의 취약점을 가져 올 수 있는 Smart Grid에 대한 보안 이슈를 분석한다. 그리고 Smart Grid 보안성 기준에 따른 보안기술정책을 연구하고, 보안 표준과 보안 방안을 제시한다.

II. 관련연구

2.1 Smart Grid의 정의

국내에서 지능형 전기망 로드맵 추진위원회에서 기존의 전기망에 IT를 접목하여, 전력공급자와 소비자가 양방향으로 실시간 정보를 교환, 에너지효율을 최적화하는 차세대 전기망을 Smart Grid라고 정의한다. 미국은 에너지 독립 및 안보법에서 미래의 증가할 전력 수요를 해결할 수 있으면서도 전력 전송과 분배에 있어 신뢰성과 기반시설보호를 유지할 수 있도록 구조화된 국가 전력 전송 분배 시스템으로 정의하고, 유럽의 Smart Grid미래 전력 네트워크를 위한 유럽 기술 플랫폼에서는 지속가능하고, 경제적이며, 안전한 전기 공급을 효율적으로 전송하기 위해 연결된 모든 사용

자의 행위를 지능적으로 통합 할 수 있는 전기 네트워크로 정의한다[3][4].

2.2 Smart Grid의 필요성

석유 및 석탄과 같은 화석에너지로부터 신재생에너지로의 전환을 위해서 그리드 역할이 필요하다.

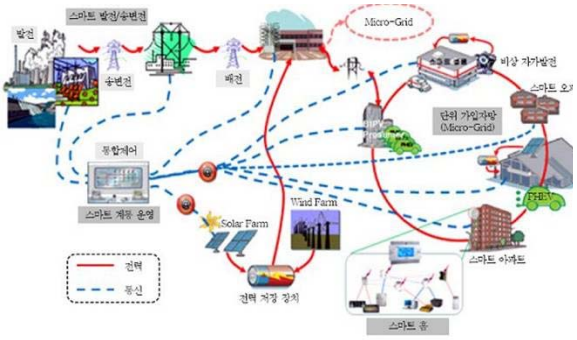

그림 1. Smart Grid 구성도
Fig. 1. Smart Grid configuration

그림 1과 같이 Smart Grid 구성에서 IT기반의 미래형 차세대 전기망으로 센서 · 통신 · 자동제어 등의 IT기술을 전기망에 도입함으로써 전력 인프라의 융통성 · 보안성 · 신뢰성 · 효율성 · 안전성 등을 향상시키고, 양방향 통신을 가능하게 하여 전력 선택 범위를 넓히고, 이를 통해 전반적인 전력 인프라 시스템의 효율성을 향상시킨다[5].

2.2.1 에너지·환경문제에 대응

국가 에너지 소비의 3% 절감 및 태양광·풍력 등 전력생산이 불규칙한 신재생발전원의 보급 확대 기반이 조성된다. 전기요금이 저렴하고 수요가 낮은 시간대로 전력수요를 분산함으로써 피크전력을 관리하여 확대되는 전력공급을 위한 전력시스템 신규 건설 등 투자비용을 절감한다. 전기차 보급인프라 구축 등을 통해 국가 CO2 배출량 41백만톤을 감축을 기대한다.

2.2.2 녹색성장시대에 신성장동력 창출

국내 68조원 규모의 내수시장 창출을 통해 그린 일자리를 50만개 창출하고 우리나라를 세계 Smart Grid 산업의 효과를 기대할 수 있고, 전력·중전·가전·통신부문에서 세계 일류기업군을 보유 하여 Smart Grid 제품에서 시너지효과 창출을 통해 2030년 세계시장 점유율 목표 30%를 기대한다.

2.2.3 저탄소·녹색생활 정착

2012년부터 아파트·관공서 주차장에 충전인프라 구축을 하고, 전기차 배터리 임대 비즈니스 모델을 활성화 할 것이다. Advanced Smart Meter 보급을 통해 소비자의 전기사용량을 15% 절감하고, 각 가정에 설치된 신재생·분산형 전원을 전력회사에 제공하여 효율을 증대 시킬 수 있다.

2.2.4 전력서비스의 고품질화

전기망의 자기치유 기능 극대화를 통해 고품질 전력서비스를 제공한다. 고품질의 전력을 제공함으로써 정전이나 불안전 전력으로 인한 피해를 줄일 수 있다[6].

III. Smart Grid 인프라의 보안성 분석

3.1 Smart Grid 인프라 분석

3.1.1 실시간 감시 시스템

송전선로에서 발생할 수 있는 위기상황을 실시간으로 감시함으로써 송전선로의 고장을 예방하고 아울러 설비의 융통전력의 여유를 고려하여 보다 효율적으로 송전선로를 운용하기 위한 기술이며, 전력시스템 광역감시시스템, 선로의 동적허용량 평가 기술, 누설 전류센서, 전자식 변압기 등이 포함된다.

3.1.2 PHEV(Plug-in Hybrid Electric Vehicle)

대체에너지를 이용한 운송수단으로 재충전이 가능한 전지의 전기를 사용한다. 하이브리드 자동차보다 큰 용량이 큰 배터리를 차량의 화물칸에 탑재하여 심

야의 저렴한 잉여 전력을 충전하여 근거리 이동에 필요한 에너지로 사용한다.

3.1.3 스마트 배전 기술

광범위하게 산재되어 있는 배전설비를 컴퓨터시스템을 이용하여 배전사령실에서 집중 원격 감시 · 제어하고 선로 고장구간 및 최적 계통전환 등 배전계통 운용업무를 현대화하는 설비 기술이다.

전력설비 자동화 시스템은 전력을 생산·수송·공급하는 대상설비에 따라 급전종합 자동화설비, 원방감시제어설비, 배전자동화 시스템으로 계층구조를 형성하고 있으며, 배전자동화는 모든 전력계통의 자동화를 완성할 수 있는 기반이 되는 기술로써 지능화하는 기술이다.

3.1.4 스마트 네트워크 기술

Smart Grid 요소 기술들을 위한 인프라를 제공하는 측면에서 통합 통신 플랫폼 기술이며, 상호호환성을 지원하는 개방형 통신 아키텍처가 필요하다. 모바일 네트워크, TCP/IP 초고속인터넷망 등이 사용자, 엑세스, 백본 전기망의 인프라로 적용 될 수 있다[7].

3.1.5 AMI(Advanced Metering Infrastructure)

원격검침에서 양방향 통신을 지원하고, 소비자의 에너지에 대한 다양한 정보를 수집한다. 사용자에게 전력사용 정보를 제공하고 수요반응을 통한 스마트 미터, 사용자의 에너지 사용량, 요금제도, 예상요금 등의 정보를 이용하여 자발적으로 에너지 절감을 하기위한 사용자 수요반응기기, 대용량 전력자원을 통합관리하기위한 전력정보관리시스템, 및 전력공급자와 사용자를 연계하는 전력서비스 네트워크로 구성된다.

3.1.6 스마트 계통 운영 기술

통신 및 제어 기술을 수단으로 녹색에너지원과 분산전원을 매끄럽게 기준 간선망에 연계시스는 기술로서, 산재생에너지, 분산전원, 배터리 저장 장치, PHEV, 전력전자소자, 실시간 요금체계 등의 모든 요소들이 안정적이며 신뢰할 수 있는 방법으로 통합될 수 있도록 하는 운영기술 및 제반 환경 관련 기술이다.

3.1.7 HAN(Home Area Network)

정보가전을 포함한 가정의 전력기기를 유무선통신 인프라를 통해 제어하고 관리하는 역할을 담당하고 있으며, Smart Grid 실현에 있어서 전력 스마트미터와의 연계가 필연적이다.

3.2 Smart Grid 인프라의 보안성 분석

전력IT기기가 융합됨으로서 전기망, 시스템, 서비스, 종단 장치 등 정보통신 네트워크 기기에서 발생하고 첨단 검침 인프라의 취약성을 이용하면 금전적 이득을 취할 수 있기 때문에 해커의 침입 및 보안 문제가 우려 된다[8].

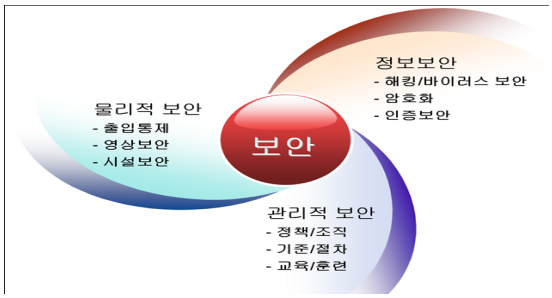

그림 2. 보안의 분류
Fig. 2. Security Classification

악성코드, DoS[9], 침해사고 등으로 인하여 전력 시스템의 마비가 가능하다. 그림 2처럼 보안을 분류하여 정확하고 안전한 Smart Grid 보안의 필요성을 인식하고 보안 대책이 마련되어야 한다.

미국의 전력업체 직원이 일반인이 흔히 사용하는 이메일 서비스를 이용하다가 악성 소프트웨어를 자신의 컴퓨터에 다운로드하게 되고, 나아가 발전소 전체를 마비시키는 과정을 상세히 보여줬다. 미국 보안 업체인 Core Security Technologies는 발전소, 석유정제소 등에서 운영 자동화용으로 사용되는 허점을 확인하였다. IOActive는 500 달러 장비와 전자기술 및 소프트웨어의 기초적인 지식을 갖고 있으면 Smart Grid 시스템이 교란 당하여 침투 할 수 있다고 한다. 2009년 4월 미국 전기망이 외국 해커들에 의해 침투되어 실제 전기망 교란을 시키는 소프트웨어를 설치하였다.

Smart Grid는 아직 보안이 취약한 관계로 개인정보보호 정책위반을 포함한, 정보 기밀성의 손상 가능성이 있다. 스마트 미터에 접근한 해커가 요금청구 정보, 기기 제어, 개인정보 보호, ID 정보, 통신을 이용해 악용 가능하다. 전기망을 전체적으로 확인하여 개인정보에 무단 접근하는 행위를 가능한 한 최소화하도록 해야 한다.

Smart Grid 설계원칙은 정보의 모든 사이버 안전 원칙을 고려해야한다. Smart Grid 설계는 우선 공격이 확산 되는 것을 막기 위해 Smart Grid 네트워크 전체에 걸쳐 보안을 취해야 한다[10].

3.3 Smart Grid 보안이슈 분석

3.3.1 스마트제어

스마트 제어를 위하여 스마트 전자제품에 대한 제어 신호가 입력되면 사용자와 기기 인증은 보안의 기본이다. 스마트 전자제품에서의 잘못된 인증이 단순히 해당 기기의 오작동뿐만 아니라, 타인 및 타기기에 의한 제어가 가능 할 수 있기 때문에 스마트 제어에 관련 된 보안 이슈가 존재한다.

3.3.2 AMI

AMI의 스마트 미터기는 전력 검침의 기능으로 인하여 스마트 미터기 기기의 보안 취약성이 존재하고, 스마트 미터기의 관련 데이터가 통합 되므로, 보안적으로 취약하여 개인 사생활의 문제가 발생한다. 또한 사이버테러로 인하여 스마트미터기의 접근 통제에 문제가 발생 하는 보안 이슈가 존재한다.

3.3.3 기반통신

기존 유무선 통신 네트워크에서 보안 취약성이 발생 한다. Smart Grid에서도 전력과 IT의 융합기술이므로 개방형 네트워크의 사용으로 해킹, DoS공격 등의 위협으로 인하여 보안 이슈가 된다.

3.3.4 서비스제공

서비스 제공 사업자가 소비자 데이터를 저장하기 때문에, 소비자 데이터 유출, 임의적인 변조나 조작 등을 통한 개인사생활 침해 가능성이 존재한다. 서비스 제공 사업자가 소비자 데이터를 처리하거나 제3자에게 제공하는 경우에도 개인사생활 침해가 발생가능하고, 소비자 데이터의 파기가 제대로 이루어지지 않는 경우도 침해 가능성이 존재하기 때문에 데이터 보관에 대한 보안이슈가 존재 한다.

IV. Smart Grid의 보안기술정책

4.1 보안성 기준에 따른 보안기술정책

보안 분석을 통해서 나온 보안이슈들을 분석하고, 이슈별로 보안정책을 수립하여 스마트그리드 보안성을 강화하여야 한다.

표 2는 보안성 기준에 따른 보안기술정책을 보안항목별로 나눈 것이다. 보안 정책은 정보보안을 위해 예상되는 공격을 방지하기 위해 기술과 절차가 필요한지를 결정 하고, 보안 항목을 통하여 보안기술정책이 수립된다.

보안성 기준은 인터넷 IT 보안성 기준인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability), 인증(Authentication), 부인방지(non-repudiation), 접근제어(access control)로 구분하였다.

표 2. 보안성 기준에 따른 보안기술정책
Table 2. Security Technology Policy by Security standards

보안성 기준	보안 기술정책
기밀성	비인가 된 사용자가 정보를 읽을 수 없도록 방지하며, 스마트 전자 제품에서 데이터 수집 시 요구
무결성	비인가 된 사용자가 정보를 가로채거나 수정할 수 없도록 하며, Smart Grid에서 사용되는 무선 센서의 보안 취약성 방지
가용성	서비스 거부공격 방지 등을 통해서 인가 된 사용자의 지체 없는 정보 접근을 보장하며, 스마트 전자제품 간의 인증
인증	통신 네트워크상의 사용자나 장치들이 각자 고유의 신분증을 사용하여 신뢰할만한 대상 인지를 판단하며, 스마트 미터기에 대한 접근 통제
부인방지	서명을 통해 정보의 송수신자가 자신의 정보 송수신 사실을 부인할 수 없도록 하며, Smart Grid에 도입되는 유무선 통신 기술에 내재된 취약성
접근제어	Smart Grid 시스템에 접근하는 대상 별로 시스템이 제공하는 서비스에 대한 접근 권한을 차등적으로 부여하며, 소비자 데이터에서의 프라이버시 유출과 관련하여 필요

4.2 Smart Grid의 표준과 보안기술 표준

Smart Grid는 다양한 시스템, 소프트웨어, 하드웨어 등의 상호운용성, 호환성, 신뢰성에 영향을 미치기 때문에 표준이 중요하다. 전기기술 표준은 IEC, IEEE, ISO, OpenAMI를 적용하고, 보안기술 표준은 IEEE, NERE, IEC, NIST를 적용하고 있다. 현재 국내 Smart Grid 표준은 IEC(International Electrotechnical Commission)를 적용하고 있다. IT분야 국제표준은 ISO, ITU를 적용하고 있다. Smart Grid 정책표준은 TTA, 기술표준원이서 적용하고 있다.

2009년 10월 '지능형 전기망 표준화 포럼워크숍'을 추진하여 해외 선진국의 Smart Grid 기술개발 동향과 표준화 동향을 공유하고, 2010년 4월에 국내 Smart Grid TTA표준화 활동을 진행할 예정이며, 디지털 홈 영역 내에서 스마트 미터, 스마트 가전 등 Smart Grid 관련 기기별 표준 추진을 목표로 다양하고 복잡한 유·무선 기술의 상호운용성 측면에 중점을 두며, 요구사항, 서비스 시나리오 정의를 시작으로 2011년까지 에너지 사용과 관련된 데이터 및 가전 제어 메시지 포맷 표준을 제정할 계획이다. ITU-T의 Smart Grid 포커스 그룹(Focus Group on Smart Grid)과 같은 국제 표준화 기구에서 국제표준화도 연계 추진함으로써 한국 표준의 확산에 기여한다는 방침이다.

4.3 Smart Grid 공격에 대한 보안 방안 연구

Smart Grid의 보안 강화를 위해서는 CIP 신뢰성을 기준으로 해야 하며, 물리적인 보안과 네트워크 보안, 인증 부문, 패턴 감시가 병행돼야한다.

CIP는 미국 에너지 규격을 총괄하고 있는 FERC (Federal Energy Regulatory Commission : 연방에너지규격위원회)가 2008년 1월 사이버보안 위협에 따른 미국전력시스템의 피해발생을 사전 차단하기 위해 NERC(North American Electric Reliability Corporation : 북미전기신뢰성위원회)가 마련한 8개의 신뢰성 기준이다. CIP 기준에는 중요사이버 자산 확인, 보안관리 통제, 적정인사 배치 및 교육, 전자적 보안경계 보호, 중요 사이버 자산의 물리적 보안, 시스템 보안 관리, 사고 보고와 대응책 기획, 중요 사이버 자산의 복구 계획 마련 등의 내용을 담고 있다.

물리적 보안 요소로는 옥외에 위치된 스마트 계량기의 보호, 1차원적 잠금장치, 전자기 펄스(EMP) 공격 대비, 조작가능 성 및 경보 기능 등 물리적인 위협에 대한 대비를 요구하고 있다. 네트워크적 보안요소로는 다양한 무선 표준 활용에 대한 보호 기준이 필요하며, 송 · 변전 감시(SCADA)나 배전(DAS) 등에서 명확한 네트워크 분리가 필요하며, 인증부분에서도 보안 등급별 접근요소의 차별화가 필요하다.

V. 결론

우리나라는 Smart Grid 사업 추진이 급속하게 진행 되고, Smart Grid 선도국가로 지정 되었다. 하지만 해커의 침해사고 및 사이버테러가 급격히 확산되고 있어 Smart Grid에 대한 보안이 필요하다.

본 연구에서는 Smart Grid에 대한 보안 이슈를 분석하고, 보안성을 강화하기 위한 보안기술정책에 대해서 연구함으로써 정보보안이 강화 될 때 Smart Grid는 실시간적인 양방향 에너지 사용 모니터링과 정보 공유를 가능케 해 개방형 정보통신 네트워크로의 Smart Grid 추진의 성공 핵심이 될 것이다.

향후 연구는 Smart Grid가 구축되고, 활용되는 실무과정에서 보안 이슈를 분석을 하고, 실무적인 보안 대응방안을 통한 보안기술정책 수립에 지속적인 연구가 필요하다.

참고문헌

[1] 태성환(필립피셔), "지금 스마트머니는 탄소에 투자한다," 한빛비즈
[2] 기후변화주요국회의(MEF)에서 선정된 '세상을 바꾸는 7개 기술' 및 선도국가, http://news.donga.com/3//20090710/8754041/1, 2009. 7.
[3] 이홍재, "Smart Grid의 소개 및 제언," 전기의 세계, 59(5), 14-18쪽, 2010. 5.
[4] 김홍래, 문승일, "Smart Grid(Smart Grid)의 이해," 전기의 세계, 58(8), 22-26쪽, 2009. 8.
[5] 전용희, "Smart Grid의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석," 정보보호학회논문지, 20(3), 79-89쪽, 2010. 6.
[6] 김영명, 이영우, "Smart Grid 서비스에 대한 고객 수용도 분석," 한국통신학회논문지, 35(9), 1399-1406쪽, 2010. 9.
[7] 전영애, 오미경, 신철호, 최상성, "스마트 유틸리티 네트워크 표준 기술 동향," 전자파기술, 22(2), 72-84쪽
[8] 이명훈, 배시화, 손성용, "전력 IT 기반 스마트 파워그리드

실증 보안 체계 설계," 한국해양정보통신학회논문지, 14(11), 2497-2506쪽, 2010. 11.

[9] 이건희, 서정택, 이철원, "스마트그리드와 사이버 보안," 한국통신학회지, 27(4), 23-30쪽, 2010. 4.

[10] 곽지섭, 김완홍, 강순희, 김재성, "한국의 Smart Grid 보안현황과 사이버 보안 추진방향," 대한전기학회, 하계학술대회, 2010.