JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 25, No. 10: 1381~1390, Oct. 2021

지능형 전력망의 안전성과 신뢰성 확보를 위한 보안위협과 정책 분석

이대성*

Security Threat and Policy Analysis to Secure the Safety and Reliability of the Smart Grid

Daesung Lee*

*Associate Professor, Department of Computer Engineering, Catholic University of Pusan, Busan, 46252 Korea

요 약

지능형 전력망은 제어시스템, 전력망, 수용가로 구성되는 세 가지의 광범위한 보안 영역을 다루는 대표적인 4차 산업혁명 시대의 융합 신기술이다. 융합 신기술인 만큼 향후 국가의 기술발전과 성장동력, 경제성 등에 많은 긍정적인 영향을 미칠 수 있지만, 만약의 보안사고 발생 시에는 막대한 피해가 예상되기 때문에 에너지 관련 기관은 최신의 각종 보안 사고들을 예측하고 대응할 수 있는 다양한 보안대책들이 마련되어야 한다. 본 논문에서는 국내외 스마트그리드 현황과 보안표준 동향, 그리고 취약점 및 위협을 살펴보고, 앞으로의 스마트그리드 보안기술 전망에 대해 고찰해 보고자 한다.

ABSTRACT

Smart grid is a representative convergence new technology in the era of the 4th industry revolution that deals with three broad security areas consisting of control system, the power grid, and the consumer. As it is a convergence new technology of the 4th industrial society, it is true that it can have a positive effect on the country's technological development, growth engine, and economic feasibility in the future. However, since the smart grid is expected to cause enormous damage in the event of a security accident, energy-related organizations must prepare various security measures to predict and respond to the latest security incidents. In this paper, the current status of domestic and foreign smart grids, trends in security standards, vulnerabilities and threats, and prospects for smart grid security technologies are to be considered.

키워드 : 스마트그리드, 마이크로그리드, 첨단계량 인프라, 에너지저장 시스템, 에너지관리 시스템

Keywords : Smart grid, Micro grid, Advanced metering infrastructure, Energy storage system, Energy management system

Received 25 August 2021, **Revised** 9 September 2021, **Accepted** 15 September 2021

*** Corresponding Author** Daesung Lee(E-mail:dslee@cup.ac.kr, Tel:+82-51-510-0653)
Associate Professor, Department of Computer Engineering, Catholic University of Pusan, Busan, 46252 Korea

Open Access http://doi.org/10.6109/jkiice.2021.25.10.1381 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

지능형 전력망(Smart Grid)은「발전-송전-배전-판매」로 구성되었던 일방향 전력망을 [그림 1]과 같이 ICT 기술이 갖는 실시간 양방향성 특성과 결합시켜 공급자와 소비자가 에너지 정보를 서로 교환함으로써 전력의 안정적인 수급과 온실가스, 미세먼지 감축 등 친환경 에너지 이용 효율의 최적화를 목표로 한다[1].

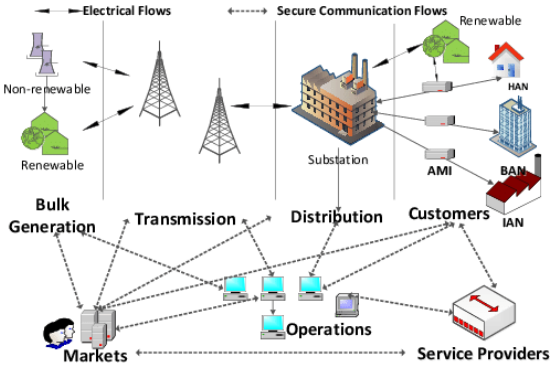

Fig. 1 NIST's Smart Grid Conceptual Model

하지만 최근 들어 기후변화 협약과 화석연료의 고갈 추세 등에 따라 신재생에너지의 보급이 활발해지고, 수요반응자원(Demand Response) 거래시장 제도가 도입되면서 다양한 전력계통간의 상호접속 및 운용의 필요성이 급증함에 따라 스마트그리드와 마이크로그리드 연계 위협에 대한 보안대책도 새로운 단계를 맞고 있다.

그동안 지능형 전력망은 인터넷 기반의 개방적 구조 특성과 적대적인 국가를 대상으로 대규모 정전사태(Black out)를 유발하여 중요 산업시설을 마비시킬 목적으로 핵티비즘적(Hacktivism) 사이버 공격의 주요 목표가 되어왔다.

2009년 악성코드 Stuxnet에 의한 이란 핵 시설 공격이 보고된 이래, 2011년에는 글로벌 에너지 기업을 대상으로 한 스피어피싱 Night Dragon 공격이 있었던 것으로 밝혀졌고, 2012년 런던 올림픽 개회식장의 전력시스템에 대한 공격 시도, 2015년 우크라이너 변전소에 대한 악성코드 CrashOverride의 공격으로 8만 가구에 전력공급이 중단되었다. 또한 2017년 5월에는 마이크로소프트 제품의 취약점을 악용한 랜섬웨어 WannaCry가 세계 150개국에 확산되어 상당한 피해를 유발시켰다[2].

현재 지능형 전력망은 IoT를 기반으로 하는 마이크로그리드가 확산되어 에너지 인프라의 초연결화가 진행되고 있으며, AI/빅데이터 분석을 기반으로 한 스마트그리드 설비 운영의 효율화·최적화, 5G 무선 인프라를 기반으로 하는 광대역 무선방식의 적용범위가 확대되고 있다.

따라서 본 논문에서는 지능형 전력망의 안전성과 신뢰성을 확보하기 위한 보안위협과 대책을 첨단계량인프라(AMI), 에너지저장시스템(ESS), 에너지관리시스템(EMS)를 중심으로 살펴보기로 한다.

Ⅱ. 국내외 스마트그리드 동향

2.1. 스마트그리드 구조

스마트그리드는 광역 모니터링 및 제어, 송전망· 배전망 관리, 신생 에너지 등 에너지 생산 부문에 대한 구조 개선과 더불어 지능형 원격 검침체계인 AMI, 전력 운영환경 관리체계인 EMS, 에너지 저장체계인 ESS 등 에너지 소비 부문을 중심으로 기술개발이 진행되고 있다.

AMI(Advanced Metering Infrastructure)는 수요 반응(DR; Demand Response) 체계[3]를 구현하고 운영하는 핵심 수단이며, 수용가 인접점에 설치되는 스마트 미터, 스마트 미터에서 정보를 수집하는 DCU(Data Concentration Unit)와 DCU로부터의 정보를 관리하는 MDMS(Meter Data Management System)로 구성되는 계층적 구조의 인프라이다[그림 2]. 스마트 미터와 DCU 간의 통신에는 PLC, Zigbee, Wi-SUN, Wi-Fi 등 운영환경에 따라 다양한 통신방식이 사용된다.

1) 지능형 전력망에 대한 정의는 국가별로 다소 상이하지만, 국내에서는 지능형전력망법 제2조제2호에 따라 "전력망에 정보통신기술을 적용하여 전기의 공급자와 사용자가 실시간으로 정보를 교환하는 등의 방법을 통하여 전기를 공급함으로써 에너지 이용효율을 극대화하는 전력망"으로 정의

2) The Shadow Brokers(2016)라는 해커 그룹이 공개한 EternalBlue라는 마이크로소프트 윈도우의 파일 공유에 사용되는 서버 메시지 블록(SMB) 원격코드의 취약점을 악용한 사례로, 인터넷 접속만으로 전 세계 150여개국에서 최소 30만대 이상이 컴퓨터 시스템이 감염되었다.

3) 전기 사용자가 전력공급 상황, 피크 부하율, 전력 생산·공급가격에 따라 전력수요를 자율적으로 조절하는 매커니즘이다.

따라서 전력회사의 입장에서 AMI는 전력사용과 요금정보 등 전력사용에 대한 신속하고 정확한 판단을 할 수 있게 지원해 주지만, 스마트미터와 홈게이트웨이가 소비자 영역에 위치하고, 인터넷망과 소프트웨어에 대한 기술 의존도가 매우 높기 때문에 서비스 거부공격, 계량 사용정보 변경, 장치 오작동 유도 등의 보안 위협에 노출되어 있다.

이를 위해 기기 인증과 키관리, 데이터의 암호화 통신, 장치의 오작동 유도 방지를 위한 펌웨어 조작 및 물리적 해체/교체 공격, 스마트 미터링 데이터의 부인 방지기술 등이 연구되고 있다.

현재, AMI 기술개발은 ICT 기술과의 융합이 필수적이기 때문에 소프트웨어 플랫폼 개발에서는 IBM, SAP, Oracle 등 글로벌 기업이 참여하고 있으며, 국내에서는 한국전력공사, 한국조폐공사와 민간기업인 키페어 등이 암호모듈을 자체 개발하고 있다[1].

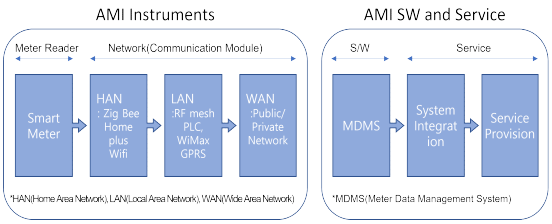

Fig. 2 AMI Diagram[1]

에너지 관리시스템 EMS(Energy Management System)는 에너지 정보시스템(EIS), 에너지 제어시스템(ECS), 에너지관리 플랫폼 등 세 가지 서브시스템으로 구성되며, 공장, 빌딩, 가정, 교통, 금융 등 사회 인프라에 에너지를 효율적으로 공급하고 소비하기 위한 통합 솔루션이다[그림 3]. 소비 분야별로 FEMS(공장, 산업단지), BEMS(빌딩, 상가, 학교), HEMS(아파트, 주택), CEMS(지역), MGEMS(마이크로그리드)[4], REMS(재생에너지), TEMS(전기차 충전소)로 분류된다[2].

그동안 EMS는 에너지 시각화와 분석을 중심으로 발전해 왔으나, 현재는 클라우드 기반으로 설치 및 사용방식이 변화하면서 수요 반응(DR)과 설비 관리 등 서비스 기능이 확대되는 추세를 보이고 있다. 이에 따라 EMS에서는 데이터 유출이나 손실, 계정 도용이나 악의적인 내부자, API 우회 공격 등의 위협이 존재한다.

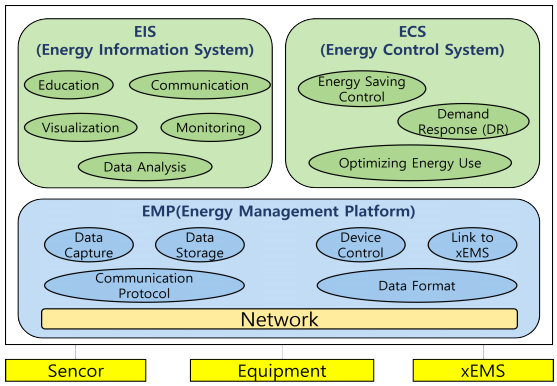

Fig. 3 EMS Diagram[2]

에너지 저장시스템 ESS(Energy Storage System)는 생산한 전력을 저장했다가 필요한 시기에 저장 전력을 공급하는 시스템이기 때문에 전력 사용의 효율을 높이기 위해 전력의 품질을 위한 주파수 조정, 발전량의 평준화를 위한 부하 조정, 정전이 발생했을 때 무정전 전원의 역할을 한다. 따라서 신생에너지와 같이 에너지 공급이 일정하지 않은 경우에는 ESS의 활용이 필수적이다.

ESS는 전력 저장원, 전력변환 장치(PCS; Power Coversion System)[5], 에너지관리시스템(EMS)으로 구성되며. EMS를 통해 ESS의 충전과 방전 조건을 제어하기 때문에 효율적인 에너지 저장관리에 매우 중요한 역할을 한다[그림 4].

전력 저장원의 저장 방식은 배터리/화학적 방식과 비 배터리/물리적 방식으로 구분된다. 배터리 방식에는 리튬(Li) 전지, 나트륨황(NaS)전지, 레독스 흐름 전지, 슈퍼 캐패시터 등이 있으며, 비 배터리 방식에는 양수 발전, 압축공기저장, 플라이휠 등이 있다. 하지만 최근 ESS의 보급용이 늘어나면서 화재나 폭발 같은 사고가 증가하여 안전사고 예방을 위한 기술 대책이 시급하다[1].

4) 마이크로그리드(Microgrid)는 작은 단위의 스마트그리드로, 기존의 광역 전력 시스템으로부터 독립된 소규모 전력 체계를 따로 구성하여 자체 전력망 내에서 전기수요를 100% 충당할 수 있도록 구성한 국소적인 전력 공급 시스템이다.

5) ESS 내의 발전원에서 전력을 입력받아 배터리에 저장하거나 계통으로 방출하기 위하여 전기 특성을 변환하고 감시-제어, 독립 운전, 계통 연계 보호 기능 등을 하는 시스템

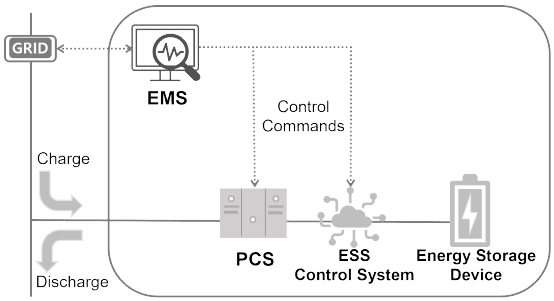

Fig. 4 ESS Diagram[1]

2.2. 스마트그리드 정책 동향

2.2.1. 국내 정책 동향

우리나라는 스마트그리드 산업의 세계시장 선점을 위하여 2009년부터 지능형 전력망, 지능형 소비자, 지능형 운송, 지능형 신재생, 지능형 서비스 등 5대 스마트그리드 실증사업을 제주단지에서 진행하였다. 2012년에는 2030년까지 국가단위 스마트그리드를 구축한다는 목표 아래 제1차 지능형전력망 기본계획(2012~2016)을 수립하고, 2013년 11월부터는 지능형 전력망 촉진법의 시행과 함께 스마트그리드의 핵심 시스템인 스마트미터, 에너지저장장치, 전기차 충전 시설을 중점적으로 확충하기 시작하였다.

2018년 7월에는 지능형 전력망의 구축 및 이용 촉진을 위해 제2차 지능형전력망 기본계획(2018～2022)을 수립하여 추진 중에 있다. 이 계획은 에너지 전환 시대, 소비자가 중심이 되는 전력시장 생태계를 조성한다는 목표 아래 계절별·시간대별 요금제 확대, 국민 DR로 확대 개편, 전력중개사업 도입·시행 등 새로운 서비스를 활성화하고 AMI 인프라 확충, 전력망의 ICT 인프라 확충 등 스마트그리드 인프라 및 설비 확충을 중점 추진한다. 2020년에 분산형 에너지 시스템의 확산을 위해 에너지 신기술 신뢰성 확보, 고출력·고신뢰성 ESS 및 사이버 보안에 1,365억 원이 투자될 예정이다.

이를 위해 검침 서버에서 통신 모뎀까지 AMI 시스템 구간 암호모듈을 적용하고, 암호모듈이 적용된 전력량계를 개발·실증 등 AMI 기반 인프라를 확충하고, 송·배전망 연계 신재생 관제시스템 구축, 신재생에너지 감시·예측·제어시스템 구축, 발전기의 실시간 운영여건을 고려한 운영발전계획 시스템을 구축할 예정이다[3, 4, 5].

또한 전력망의 ICT 인프라를 확충하기 위해 SCADA를 기반으로 다양한 전력시스템과 연계한 전력망 통합 운영 플랫폼 및 IoT 기반으로 전력설비 자가진단·고장자동판단 등 자율운전 지능형 변전소 구축하고, 원격 감시/제어시스템과 배전망 복잡화에 대비해 효율적 망 운영을 위한 차세대 배전 지능화시스템(ADMS; Advanced Distribution Management System)을 개발하고 이를 실증할 계획이다[6].

2.2.2. 주요국 정책 동향

신재생에너지 등 분산 전원의 증가와 에너지 수요효율화 요구가 높아지면서 세계 주요국들은 전력 수요 안정에 필요한 AMI, ESS, EMS 고도화 정책을 추진하고, AI/빅데이터 분석 기반의 IoT, 광대역 모바일 기술의 활용을 위해 민간 기업의 적극적인 참여를 유도하고 있다[7].

미국은 경기 부양책의 관점에서 노후된 전력망을 스마트그리드로 대체한다는 목표 아래 2016년까지 80억 달러를 투자하여 지역별 실증사업, AMI, 송·배전망 등 융자지원 및 표준화 사업을 추진하였으며, 현재는 구글 딥마인드, Opower, AutoGrid, 테슬라 등의 글로벌기업들이 스마트그리드 사업에 참여하여 인공지능과 빅데이터, 배터리 기술의 사업화를 시도하고 있다.

미 국방부(DoD)도 에너지 안보 강화를 목표로 하여 2050년까지 자체 전력 에너지 수요의 25%를 재생 에너지로 충당하고, 스스로 제어 가능한 마이크로 그리드를 구축하고 있다. 특히, P2P 전력 거래와 신재생에너지의 생산 비율 확대를 목표로 AI/빅데이터 분석과 블록체인 등 4차 산업혁명의 핵심 기술을 에너지 분야에 접목하는 시범 프로젝트를 진행 중이다[1, 7].

EU는 에너지원의 다변화를 통해 2030년까지 1990년 대비 온실가스 40% 감축을 목표로 하고 있으며, 회원국들의 다양한 특징을 하나의 에너지 시장으로 통합하기 위해 EU Framework Project를 추진하고 있다. 2004~2017년간 950개 사업에 약 50억 유로가 투자되었는데, 전력망 관리, 소비자 수요관리, 분산전원과 저장기술 분야에 전체 투자액의 81%가 집중되었다. 최근에는 배전망·지역 단위의 ESS 실증사업이 활발히 진행중이다. 주요 기업으로는 Siemens(독, 에너지), Next Kraftwerke (독, VPP), Piclo(영, P2P), ABB(스위스) 등이 참여하고 있다[1, 7].

중국은 2020년까지 송배전 설비에서 세계적 수준 달성을 목표로 하고 있으며, 매년 발전량이 증가하여 2019년에는 7.3조kWh에 달하고 있다. 이 중 태양, 풍력, 수력

등 재생에너지의 비율은 26%이었으며, 발전 출력이 불안정한 태양광과 풍력은 9%를 점하고 있다.

IoT와 AI 등 차세대 ICT 기술과 제조업간의 융합을 목표로 계획된「중국제조(中国製造) 2025」에서 스마트 그리드는 10개 중점분야 중 하나로 선정되었다. 이를 통해 신재생에너지 설비, 첨단 에너지저장장치(ESS) 등 개발, 핵심부품 및 기술개발을 목표로 대규모 고효율·청정 화력 발전기의 산업화 및 시범 응용을 추진하고, 신재생에너지 설비, 첨단 에너지저장장치, 스마트 그리드용 송배전 등 설비 발전을 추진한다[8].

한편, 중국 과학기술부는 2018년에 재생에너지의 그리드 접속, 마이크로그리드, 스마트그리드 기초기술 국산화를 목표로 3억 8천만위엔을 투자하고, 2020년에는 전력소비자, 송배전사업자, 발전사업자, 소판매전기사업자 간에 전력소비, 발전량, 축전량 정보를 공유하는「유비쿼터스 전력 IoT」사업에 8,755만위엔을 투자할 예정이다.

중국 정부도 전력거래 활성화 정책을 추진하기 위해 신규 그리드 건설에 박차를 가하고 있으며, 시범 프로젝트의 개발과 관련 기술개발에 대한 정부지원 규모를 높여 가고 있다. 현재 19개 프로젝트에 3.7억 위엔을 투입하였으며, 상해와 강소성에서 10MW 이상의 가상발전소(VPP) 프로젝트를 진행중이다.

일본은 2014년 12월 에너지 관계 기술개발 로드맵을 발표하였으며, 2016년 4월에는 에너지 관련제도의 정비와 온실가스의 절대 감축을 위한 에너지·환경혁신전략을 발표했다. 2018년에는 제5차 에너지 기본계획을 발표하고, 후쿠시마 원전사고를 교훈 삼아 원자력 안전 확보와 에너지 Mix에 의한 원자력 의존도 감소, 에너지 비용 억제와 에너지 자립이라는 두가지의 큰 축의 에너지 목표를 밝혔다. 그리고 이를 안전성(Safety)을 전제로 에너지의 안정공급(Energy Security), 경제효율성의 향상(Economic Efficiency), 친환경(Environmrnt)을 구현한다는 3E+S로 요약하였다.

이러한 목표아래 일본은 2030년까지 태양광 발전량을 100GW까지 늘리고, 경제산업성을 중심으로 연구회를 운영하면서, 관리·재난대비용 마이크로그리드 중심의 스마트그리드 기술개발과 표준화 전략을 검토하고 있다.

2016년 4월에는 전력산업구조를 개편하여 판매시장을 개방함에 따라 에너지회사, 통신사, 유통업체, 지자체 등 350여개사가 진입하여 다양한 요금제・결합서비스를 제공하고 있다. 기존의 지역별 10개 전력회사들은 스마트미터 보급과 소비자 서비스 개선 등 변화를 시도하고 있다[9].

Ⅲ. 스마트그리드의 취약점 및 위협

스마트그리드는 신재생에너지원와 친환경 관리를 위해 다양한 IoT들이 인터넷을 이용해 복합적으로 연계되어 있기 때문에 보안 리스크의 범위가 계속 늘어나고 있다. 폐쇄망 내에 위치한 제어시스템은 HW나 SW의 유지보수 및 패치 설치에서 취약점 평가가 이루어져 비교적 안전하다는 평가를 받고 있으나, 여전히 네트워크 공격의 핵심 목표가 되고 있으며, AMI 해킹이나 스마트그리드 참여자의 과도한 정보 수집으로 인한 개인정보 보호 노출 문제도 당면 과제로 부각되고 있다.

IoT와 광대역 무선인프라 등 4차 산업혁명 시대의 스마트그리드에서 고려되어야 할 보안 취약점과 보안 위협을 정보보안의 기본 기능과 스마트그리드 시스템 분야별 Matrix로 정리해 보면 [표 1]과 같다[6, 10, 11, 12].

Table. 1 Security Matrix by Smart Grid System Field

Category		AMI	ESS	EMS
Confidentiality	Incoming unauthorized communication data	●	●	
	Communication/ Storage information leakage			●
	Sending illegal control commands		●	
	Personal information disclosure	●		●
Integrity	Executable code/Data forgery	●		●
	Exchange message leakage/Falsification	●	●	
Availability	Physical approach attack	●		
	Network Attack	●		●
	Operation center invasion Attack			●

Category		AMI	ESS	EMS
Authentication·Authorization	Unauthorized access	●	●	●
	Elevation of privilege			●
	Camouflage service			●
	Denial of Message/Conduct	●		●

Source: Reconstructed by citing the Smart Energy Cybersecurity Guide (2019.12)

3.1. 기밀성(Confidentiality)에 대한 위협

【비인가 통신 데이터 유입】

- PLC, Zigbee, Ethernet, LTE 등을 경유하는 통신 프로토콜의 취약점을 이용하여 외부망과 연결된 스마트미터, 데이터집중장치(DCU)[6]등 ESI(Energy Service Interface) 접점에 대한 비인가 통신 데이터 유입 시도
- SCADA 시스템은 폐쇄망 내에 위치하므로 주기적인 보안 점검으로 비교적 안전한 것으로 판단되지만, 배전 자동화 시스템인 FRTU((Feeder Remote Terminal Unit)는 무인 시스템으로 위치하므로 펌웨어 해독을 통해 암호키의 노출 가능성
- ESS와 DSC(Distribution Substation Controller), 또는 SCADA간의 통신 연계구간을 통해 ESS에 대한 불법적인 침입을 시도

【통신·저장 정보 유출】

- HAN 기기에서 서비스 운영 및 제공을 위해 저장하고 있던 데이터를 공격자가 삭제, 변조, 유출하여 정상적인 동작을 차단
- 외부 IP 및 모바일망을 통해 모니터링 정보를 제공하는 경우, 홈게이트웨이 암호·인증 취약성[7]을 이용한 원격제어 정보 노출 및 전력사용 정보의 위·변조가 발생할 수 있음.
- 전력회사의 중요 정보시스템 설계도면 등의 유출

【불법 제어 명령 전송】

- 배전관리시스템(DMS)에 의한 변전소 정보 원격 취득 및 제어 등을 수행하는 과정에서 위협 발생 가능
- ESS에 인가되지 않은 제어명령(On/Off, Open/Close 등 개폐명령)로 전송 시도
- AMI 제어 정보를 조작하여 기기의 오동작을 유도하며, 전력요금 과다 청구 및 전기요금 축소 등 요금 체계에 혼란 발생

【개인정보 노출】

- 개인정보 수집·공유 및 다양한 이해 관계자들, 통신망의 취약점 등을 이용하여 개인 식별정보, 에너지 사용현황 등 개인정보 유출 및 생활패턴 분석에 의한 프라이버시 침해 시도

3.2. 무결성(Integrity)에 대한 위협

【실행 코드/데이터 위·변조】

- EMS의 무결성 검사를 수행하는 실행코드 또는 기기 설정 정보 변조를 통해 악의적인 서비스 설치하여 제어권을 획득하거나, 전력 사용량 데이터를 위·변조하여 금전적 피해 유발
- 스마트 댁내기기들의 소프트웨어 업데이트 시 메시지 위변조를 통해 관련 기기들에 악성코드를 삽입하여 장치들의 오동작을 유발

【교환 메시지 유출/변조】

- AMI Headend - MDMS(Meter Data Management System)[8] - 스마트미터CPE-의 각 연계구간에서 교환되는 메시지 스니핑 및 데이터 변조에 의한 기기 오동작 유발
- ESS와 DSC(Distribution Substation Controller)간, PMS와 Distribution SCADA 간 통신연계 구간에서 교환되는 메시지에 대해 불법적으로 유출 및 변조

3.3. 가용성(Availability)에 대한 위협

【물리적 접근 공격】

- 스마트미터, DCU 등에 대한 템퍼링 공격[9] 으로 중요

6) 가정, 빌딩, 공장에 연결된 스마트 미터로부터 유효전력, 무효전력, 최대수요 전력, 평균전압전류, 로드 프로파일(LP) 등의 각종 검침정보를 수집한다.

7) 인증키가 노출되면 스마트미터 위장을 통한 개인정보 노출, 서비스 거부 공격, 과금조작 등 2차 피해를 유발할 수 있음

8) 스마트미터로부터 수요측 데이터를 수집·분석 후 가치 있는 정보로 변환시켜 전력 소비자와 유틸리티에 유용한 서비스를 제공하는 시스템

9) 디바이스의 하드웨어적 파괴 또는 분해를 통하여 해당 디바이스의 불법 개조 또는 보안정보를 추출하여 공격. EEPROM (Electrically Erasable Programmable Read-Only Memory) 메모리, 마이크로컨트롤러 덤프, 버스 스니핑 및 다이분석 기법을 활용한 사용자 아이디·비밀번호, 환경설정 정보, 암

정보 추출, 악성코드 삽입, 계측된 계량 정보 조작 및 상위 제어시스템 공격 시도
- 스마트미터, 홈 게이트웨이 등 스마트 댁내 기기의 소프트웨어(펌웨어) 업데이트 또는 물리적인 교체 시에 악성코드를 삽입하여 메시지 위변조에 의한 기기 오작동이나 PDoS[10] 공격 발생 가능
- 스마트 댁내 기기의 기능 중 허용되지 않은 기능을 사용하거나 불법사용 기기를 연결하여 소비자 정보를 취득하거나 기기 오작동 유발

【네트워크 공격】
- AMI, EMS에 대한 DDoS 공격을 시도하여 기기·센서의 통신과 제어 기능을 마비시키거나 기기 오작동 유발
- 전력 사용정보 수집/관리 서버, 과금 및 포털 서버, EMS, MDMS 등 주요 서버를 공격할 수 있으며, 전력 사용에 대한 과금체계 혼란 및 정전 사태 유발 가능

【운영센터 침해 공격】
- 웹서비스 취약점을 이용한 공격[11], 전자메일을 통한 악성코드 설치 유도, USB 메모리를 통한 바이러스 감염, 정보보호시스템 정책의 미비점을 악용하여 운영센터 내부의 시스템 및 네트워크에 대한 침해 공격
- 시스템 유지보수를 위해 운영센터 외부 네트워크에서 시스템 접속을 허용하는 경우, 취약한 계정관리나 원격 서비스 취약점을 이용해 운영센터 내부로 침입

3.4. 인증 · 인가에 대한 위협

【비인가 접근】
- 외부로부터 연결된 네트워크를 통해 BAN 또는 HAN에 연결된 ESS 시스템에 인가되지 않은 접근을 시도
- 직원의 웹 서비스와 침입차단시스템(FW)에서 허용한 포트를 통해 웹셸 설치, SQL Injection 공격 등을 수행하여 서버 제어, 악성 스크립트 삽입, 서버 및 DB 시스템 개인 정보 유출 등의 공격

【권한 상승】
- EMS에 설치된 플러그인(plugin)를 통해 과금 정보 또는 고객 프로파일, 암호키 등 권한 범위 이외의 민감한 정보에 접근 시도
- 운영센터 직원의 악성코드가 은닉된 전자메일 및 취약점을 가진 웹 브라우저를 통해 백도어를 설치하여 루트 권한에 접근

【위장 서비스】
- 사용자가 쉽게 접근하고 취약점이 알려진 웹서비스를 악용하여 공격자가 위장 기기에 접속을 유도하거나 공급자에게 서비스를 요청하는 과정에서 위조된 IP 패킷 또는 DNS 패킷을 삽입하여 악의적인 사이트로 연결되도록 유도

【메시지 및 행위 부인】
- HAN 기기가 수행한 메시지 전송, 명령 수행 등의 사실을 부인하고, 전력사용량, 과금과 관련된 내용을 부인

Ⅳ. 스마트그리드 보안표준 동향

미국은 2009년에 SGIP(Smart GridInteroperability Panel)를 설립하고, 그 산화에 8개 서브그룹이 활동하는 CSWP(Cybersecurity Working Group(CSWP) 이 AMI의 보안 프로파일을 비롯하여 스마트그리드 사이버 보안가이드라인, 스마트그리드 사이버 보안 테스트 가이드를 개발하였다.[12]

SGIP는 2017년에 SEPA(Smart Electric Power Alliance)로 개편되었으며, 현재 스마트그리드 보안을 포함하여 Energy Storage, Grid Architecture, Community

---

호화 키, 펌웨어 등 추출

10) 네트워크를 기반으로 하는 펌웨어(Firmware)를 업데이트 할 때 그 안에 악성코드를 삽입해 시스템을 다운시키는 새로운 형태의 서비스거부 공격 방법

11) 운영센터의 내부 네트워크 장비 및 시스템에 기본적으로 설정된 서비스를 수행하거나 Telnet, FTP 등과 같은 원격 접속 서비스를 허용할 경우, 공격자가 구성설정 및 불필요한 원격 접속 서비스의 취약점을 이용해 스마트그리드 운영을 위한 네트워크에 침입할 수 있다.

12) 이 시기에 NTIS는 Energy Storage, Demand Rerponse & Consumer Energy Efficiency, Wide-Area Situational Awareness, Electric Transportation, Advanced Metering Infrastructure, Distribution Grid Management, Cyber Security, Network Communications를 스마트그리드 표준화 우선 추진 분야로 정하였다.

Solar, Testing and Certification 등과 관련된 표준 및 제도 개발을 수행하고 있다.

Cyber-Physical Resiliency에 대한 작업은 NIST SP 800-160가 채택한 시스템 엔지니어링에 관한 IEEE 규격을 중심으로 검토하고 있다. 특히, 인터넷에 접속되는 배터리, Thermostat[13], 인버터, EV 충전기 등 에너지 IoT에 대해서는 알려진 사이버 보안 위협을 중심으로 검토가 진행 중이며, DERMS 보안도 요건정의 문서의 일부로 다루어지고 있다.

Energy Service Interface(ESI)는 에너지 공급자와 소비자를 연계하는 것으로, 복수의 SEPA 워킹그룹이 TF를 만들어 작업 중이며, 이용 사례로는 ESI를 활용한 분산전원의 전압관리, 이종 서비스나 이종 디바이스를 포함한 어플리케이션, 소매시장과 거래 에너지의 연계 등이 있다.

Non-Wire Alternatives(NWA) 프로젝트에서는 송·배전망의 복잡한 구성으로 인해 재정비가 필요한 경우 해당 지역 내에 분산형 에너지원(DER)을 활용함으로써 투자 재원을 절감하면서 그 일부를 새로운 시스템을 도입한 운영자에게 지원하는 방식을 적용하고 있다. 가령 해당지역 내에 마이크로그리드를 도입하여 새로운 변전소의 구축에 필요한 비용 일부를 마이크로그리드 운영에 환원함으로써 경제성 검토만으로는 투자가 곤란한 경우에 효과적이다.

분산형 에너지원(DER)의 활용 이외에 DR 에너지 효율 향상, 전기와 열 저장, 부하 관리, 요금 설계에도 적용 가능하며, 현재 뉴욕 주와 캘리포니아 주에서 실증 프로젝트가 진행 중이다[13].

EU에서는 CEN (European Committee for Standardization), CENELEC(European Committee for Electrotechnical Standardization), ETSI(European Telecommunications Standards Institute)의 3개 표준기구가 합동으로 구성한 SEG-CG(Smart Energy Grid-Coordination Group)가 스마트그리드와 전력 이외의 에너지까지 포함한 표준화를 진행하고 있다. 현재 SEG-CG는 EC의 Clean Energy Package에 근거하여 표준화 대상에 추가해야 할 항목들을 검토하고 있다.

SEG-CG의 AHG CEP(ad hoc Group Clean Energy Package)는 Clean Energy Package를 스마트그리드로 구현할 수 있도록 표준화와 규제 관점에서 연계 영역을 발굴하고 있다. AHG CEP는 3개 Expert Group(EG)로 운영되고 있는데, EG 1은 전력 공급자와 소비자간 스마트미터의 데이터 교환에 관한 방법을 검토하며, 그 결과는 IEC 62325-451-10에 반영한다. EG 2는 사이버 보안에 대해 검토하며, DR에 관한 태스크포스(TF)인 EG 3은 DR에 관한 스마트그리드 시장의 유연성에 관한 기본 방향을 검토한다.

이 밖에 2015년부터 Smart Appliances REFerence (SAREF) ontology라는 프로젝트가 추진되고 있는데, 이는 빌딩이나 가정에 스마트 가전의 시맨틱 데이터를 분석하여 이기종 가전 정보와의 상호운용성 확보가 가능하도록 SAREF(Smart Appliances REFerence)라는 참조 Ontology 표준화가 진행 중이다[14].

IEC는 SG 3(Strategic Group 3)에서 스마트그리드에 대한 표준화를 추진하고 있으며, 하부조직으로 28개 기술위원회가 100개 이상의 국제표준 작업을 진행 중이다. SG3은 스마트그리드를 11개 분야로 나누고 있는데, 특히 배전망 관리, 수요가 에너지 관리, E-mobility 표준화에 주력하고 있다[7].

한편, TC13 전력량계, 부하계측장비에서는 스마트미터의 데이터 전송 표준화(IEC 62056 DLMS/COSEM 등), TC57에서는 전력관리시스템의 인터페이스와 수요가 시스템과의 인터페이스, 정보 모델의 표준화가 진행 중이다[15].

특히 TC57/WG17은 전력 유틸리티 자동화를 위한 통신 네트워크 및 시스템 분야 전력망 지능화를 위해 디지털 변전소의 감시·보호·제어 등을 수행하는 전력설비와의 통신방식을 지원하는 IEC 61850을 스마트그리드에 적용하기 위한 표준을 검토하고 있다. 여기에는 전기자동차나 배터리, CGS, 재생가능한 에너지와 마이크로그리드간 실시간 통신을 위해 인터넷 전송계층의 XMPP (eXtensible Messaging and Presence Protocol) 적용이 검토되고 있다.

IETF는 대규모로 설치되고, 수많은 노드들이 네트워크를 통해 연결되는 스마트 미터링의 보안을 위해 기존의 EAP(Extensible Authentication Protocol)를 사용해

13) 건물 내부의 온도설정 등 공조 기능을 일원적으로 관리하기 위한 장치

네트워크에서 디바이스 인증을 구현하는 IP 기반 프로토콜 PANA((Protocol for Carrying Authentication for Network Access)를 정의했다.

PANA는 네트워크 레이어 하단의 접근 기술과 관계없이, 네트워크 토폴로지에 관계없이 적용할 수 있는 네트워크 레이어 프로토콜이며, PaC(PANA Client), PAA (PANA Authentication Agent), AS(Authentication Server), EP(Enforcement Point)로 구성되어 있다. PaC는 PANA 프로토콜의 클라이언트를, PAA는 PANA 프로토콜의 서버를 의미한다[16].

Ⅴ. 스마트그리드 보안기술 전망

스마트그리드는 제어시스템, 전력망, 수용가로 구성되는 세 가지의 광범위한 보안 영역을 다루어야 하는 대표적인 융합 신기술이기 때문에, 에너지 관련 기관들은 각 연계구간에서 발생할 수 있는 최신의 위협 요인과 새로운 공격 형태 및 각종 보안 사고들을 예측하고 대응할 수 있는 다양한 보안대책들을 마련해야만 한다.

첫째, 이제까지 에너지 기반시설의 제어망은 인터넷망과 업무망이 철저하게 분리되어 운영되어 왔고, 대부분이 글로벌 벤더가 공급하는 외산 제품에 의존했기 때문에 초기 개발단계, 커스터마이징이나 오버홀(Overhaul) 기간 동안의 악성코드 유입을 확인하고 차단하는 공급망 공격(Supply Chain Attack)에 대응하기 위해 취약점 분석이나 평가에 보안의 초점이 맞추어져 왔다.

하지만 스마트그리드나 마이크로그리드에 Windows나 Linux와 같은 범용 SW가 사용되고, 네트워크 표준 프로토콜이 채택되면서 최종적으로 제어계 시스템(OT)을 목표로 하는 사이버 공격기법이 고도화되고 공격 횟수도 크게 증가할 것으로 예상된다. 따라서 화이트리스트를 우회하여 침입하는 Black energy나 WannaCry와 같이 기반시설을 공격목표로 하는 악성코드에 대한 보호대책을 마련해야 한다.

둘째, 전력생산 설비의 이상 징후 조기 탐지, 전력 효율 및 수요반응 관리 등을 위해 접속되는 IoT 수의 증가과 구역전기사업자의 시장 진입으로 인하여 사이버 공격대상이 확대됨에 따라 자동으로 신속하게 위협 의심정보를 식별하고 시각적으로 판단해 대응할 수 있는 SOAR(Security Orchestration, Automation and Response) 체계로 조속히 전환되어야 한다.

셋째, 제주 스마트그리드 실증사업 결과에서 보는 바와 같이 스마트그리드가 사업화에 성공하기 위해서는 다양한 전기요금을 선택할 수 있는 소비자들의 선택적 구매제도가 선결되어야 함은 물론, 기술적으로도 전력사업자의 보안구역 밖에 위치하는 AMI 보안통신이 보장되어야 한다. 이를 위해서는 스마트미터링 기기 인증 및 상호 운용성, 세션 키관리, 사용자 부인방지 및 개인정보보호 등 AMI 신뢰성(Trustworthy) 및 생존성(Dependability)을 보장하는 기술적 보안대책이 종합적으로 제시되어야 할 것이다.

ACKNOWLEDGEMENT

This paper was supported by RESEARCH FUND offered from Catholic University of Pusan(2020)

REFERENCES

[1] H. J. Kim, “Global Smart Grid Market Ecosystem Analysis,” Weekly KDB Report, pp. 9-13, Dec. 2018.

[2] S. I. Lee, “Policy and system implementation plan for the activation of IoT-based smart energy”, *Korea Energy Economics Institute*, pp. 13-15, Oct. 2017.

[3] Ministry of Trade, Industry and Energy, “2020 Energy Technology Development Action Plan (draft),” pp. 7-8, Jan. 2020

[4] Ministry of Trade, Industry and Energy, “2019 Smart Grid Implementation Plan,” pp. 5-7, Aug. 2019.

[5] Ministry of Trade, Industry and Energy, “The 2nd Smart Grid Basic Plan,” pp. 2-3, Aug. 2018.

[6] M. J. Kim and S. H. Choi, “Smart metering related IoT security technology and patent trends,” IITP: Weekly Technology Trend, pp. 14-28, Nov. 2019.

[7] H. D. Min, “Smart Grid/Micro Grid,” Korea IR Council, pp. 19-24, Aug. 2019.

[8] T. Y. Kim, S. G. Kang, and K. H. Lee, “Made in China 2025,” National NanoTechnology Policy Center, pp. 25-27, Oct. 2015.

[9] Japan Ministry of Economy, Trade and Industry, “5th Basic Energy Plan,” pp. 12-25, July. 2018.

[10] KISA, 'Smart Energy Cyber Security Guide," pp. 40-58, Dec. 2019.
[11] J. C. Kim, "Electricity security technology trends," IITP: Weekly Technology Trend, pp. 2-14, Apr. 2017.
[12] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-Security in Smart Grid: Survey and Challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469-482, Aug. 2018.
[13] Smart Electric Power Alliance [Internet]. Available: https://sepapower.org/plug-and-play-der-challenge/.
[14] *Work Programme 2019*, CEN and CENELEC, pp. 37-45, Dec. 2018.
[15] H. K. Lee, "Smart Grid Standardization Trend," Korea Agency for Technology and Standards: 11-1411095-000009-06, pp. 6-18, Jul. 2016.
[16] J. N. Kim. (2018, July). IoT Security, From intelligent remote meter reading infrastructure security [Internet]. Available: https://www.boannews.com/media/view.asp?idx=71542.

이대성(Daesung Lee)

부산가톨릭대학교 컴퓨터공학과 부교수(2012 ~ 현재)
경기대학교 정보보호대학원 연구교수(2008 ~ 2012)
인하대학교 정보공학과 공학박사(2008)
※관심분야 : 산업제어시스템보안, 융합보안, 네트워크보안