정 보 보 호 학 회 지
제26권 제4호, 2016. 8

스마트그리드 서비스별 보안 표준화 동향

이 건 희*

요 약

지구온난화 등 환경문제 해결의 다양한 방법 중 하나로 스마트그리드 구축이 활발하게 이루어지고 있다. 스마트그리드를 통해서 신재생 에너지원을 사용하고, 전기 사용의 효율성을 제고함으로써 화석연료의 사용을 줄일 수 있기 때문이다. 하지만 스마트그리드는 다양한 최신 정보통신 기술을 사용하므로 현재 인터넷 및 사물인터넷 등에서 지닌 사이버 보안 문제를 동일하게 가지게 되며, 피해 발생 시 파급효과는 일반 인터넷 서비스와는 비교를 할 수 없다. 이에 스마트그리드에 대한 보안 강화 방안에 대한 고민은 연구개발, 정책, 표준화 등 다양한 방향으로 이루어진다. 본 고에서는 스마트그리드 보안기술에 대한 국내·외 표준화 동향을 살펴봄으로써 스마트그리드 구축 시 참조할 수 있는 다양한 기술을 소개하고, 이를 통해 향후 국내 스마트그리드에도 표준화된 보안 기술이 적용되는데 도움이 되고자 한다.

Ⅰ. 서 론

최근 지구온난화 등의 환경문제를 해소하기 위한 방안의 하나로 화석연료 사용을 최소화하기 위한 노력이 늘고 있다. 신재생 에너지원의 사용을 증가시키기 위한 정책이 지속적으로 발표되고, 전기차 도입이 늘고 있다. 더불어 전기에너지 소비를 효율화함으로써 화석연료를 사용한 발전량을 최소화함으로써 화석연료 사용을 줄이는 방법도 고려하고 있다. 이와 같은 모든 방법은 결국 깨끗한 전기에너지의 생산과 효율적인 전기에너지의 소비로 귀결된다.

하지만 기존의 전력시스템으로는 앞서 나열한 일들을 실현할 수 없다. 신재생 에너지원을 이용한 발전은 전기 품질이 일정하지 않아 사용하기 쉽지 않다[1]. 전기차 충전을 위한 전력소비 패턴의 예측과 시간·지역별 전기 소비량 예측이 쉽지 않아 과잉 생산된 전기는 버려질 수 있다. 이로 인해 전기차 충전을 위한 전기공급이 원활하지 않을 수 있고, 낭비되는 전기는 여전히 많을 수 있다.

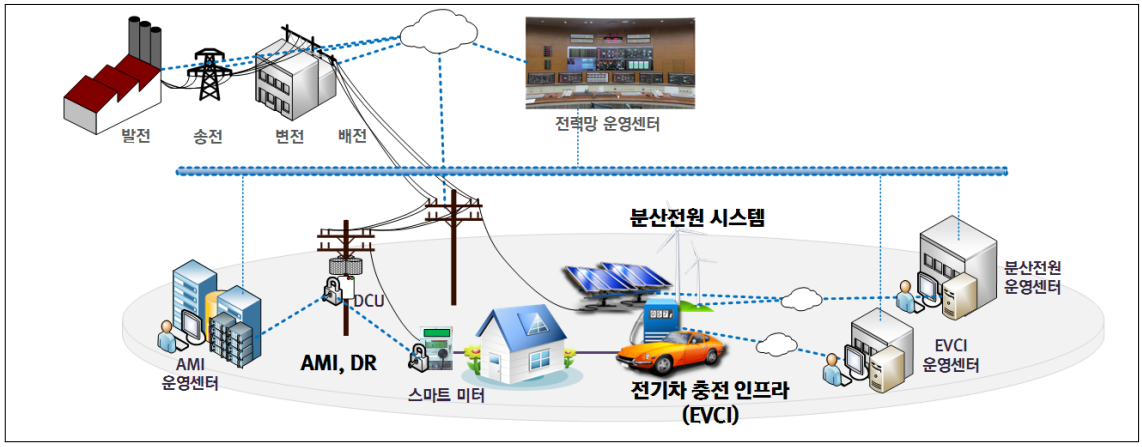
이러한 현재 전력시스템의 문제를 해결하기 위해서 스마트그리드를 고민하기 시작했다. 스마트그리드는 소비자로부터 전력소비 정보를 지속적으로 수집·분석하여, 이를 바탕으로 최소한의 전기를 생산·공급함으로써 효율성을 높일 수 있다. 또한 전기에너지 저장장치를 이용한 전력공급을 가능하게 함으로써 불안정한 신재생에너지 발전원의 전력공급 능력을 보정할 수 있다. 또한, 소비자의 잉여 전기 및 소비자가 생산한 전기를 나눠 쓸 수 있도록 함으로써 프로슈머라는 개념을 전기분야에도 도입하였다[2].

스마트그리드를 구축하기 위해서는 정보통신기술의 활용이 필수다. 전국에 흩어진 소비자로부터 전력사용 정보를 수집하고, 소비자에게는 전력공급 및 가격 등의 정보를 제공하기 위해 통신망이 구축되어야 한다. 더불어 수집된 데이터를 분석하여 유의미한 정보를 추출하기 위한 정보기술도 필요하다.

미래의 환경과 생활편의를 위해서 도입되어야 할 스마트그리드지만 정보통신기술의 융합으로 인해 기존의 전력망에서는 크게 다루어지지 않던 사이버 보안 문제가 스마트그리드에서는 중요한 이슈로 거론되고 있다. 정보통신기술이 이식되는 전력망인 스마트그리드에 기존의 정보통신기술에 대한 사이버 공격 위협들 역시 이식될 가능성이 대두되고 있다.

특히 접근이 쉬운 소비자 환경에 설치되는 기기에 대한 사이버 공격을 통해 전기소비량 예측에 오류가 발생하도록 함으로써 큰 규모의 정전을 유발하는 공격에 대한 연구가 많이 진행되고 있다[3][4]. 이 외에도 소비자

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. (No. 20141010501870)
* 한국전자통신연구원 부설 국가보안기술연구소 (icezzoco@nsr.re.kr)



〔그림 1〕 스마트그리드는 전력공급을 위한 전력망과 전력망의 지능화된 운용을 위한 정보통신망이 공존하는 복합 시스템

단에 설치된 기기를 공격하여 전기사용요금에 대한 부당이득을 편취하도록 하는 공격[5], 소비자 개개인 수준의 정전을 유발하는 공격[6], 전기사용량 정보 유출을 통한 개인 프라이버시 침해 등의 다양한 공격에 대한 연구가 진행되고 있다[7].

이렇게 사이버 보안 위협이 커짐에 따라 스마트그리드를 주도하는 미국, 유럽 등에서는 사이버 보안 강화가 스마트그리드 성공의 선결문제라고 판단하고, 사이버 보안 강화를 위해 연구개발 및 표준화에 많은 투자를 하고 있다. 특히 사회 기반 시설인 스마트그리드에 대해 동일한 수준의 보안대책을 적용되어야 하며, 시스템 간 연동이 많은 스마트그리드의 특성을 고려하여 서로 다른 시스템에 적용된 보안기능이 상호운용될 수 있도록 해야 한다. 이러한 목적을 위해서 스마트그리드 보안 표준화에 대해 세계적으로 많은 노력을 기울이고 있다. 이에 본 고에서는 국내는 물론 국외의 스마트그리드 보안 기술 표준화에 대한 동향을 살펴보고자 한다. 이를 통해서 향후 국가 스마트그리드 구축 시 활용할 수 있는 보안기술을 식별하여 활용할 수 있도록 정보를 제공함으로써 국가 스마트그리드의 보안 경쟁력 제고에 기여하고자 한다.

Ⅱ. 스마트그리드 서비스별 보안

스마트그리드를 구성하는 시스템은 매우 다양하다. 그리고 이러한 시스템들이 유기적으로 협업할 수 있어야 한다. 따라서 스마트그리드와 관련한 표준은 다양한 영역에서 개발되고 있다. 더불어 스마트그리드와 관련한 사이버 보안 표준 역시 스마트그리드 서비스별로 다양하게 개발되고 있다. 이에 본 고에서는 스마트그리드의 서비스를 기준으로 시스템을 구분하고, 이들 각자의 서비스 환경에 적용 가능한 보안기술 표준의 개발 동향을 살펴보고자 한다.

미국 국가기술표준원(National Institute of Standards and Technology, NIST)에서는 스마트그리드 프레임워크를 개발함에 있어 6개의 분야를 우선순위가 높은 기술분야로 지목하였다. 지목된 6대 분야는 전기차충전인프라, 전기에너지 저장장치, 광역 상황인지, 수요반응, AMI(Advanced Metering Infrastructure), 배전망 관리 등이다[8]. 우리나라의 스마트그리드 확산 보급을 위해서 추진되는 주요 사업도 주로 전기차충전인프라, 전기에너지 저장장치, 수요반응, AMI 등에 집중되고 있다.

따라서 본 고에서는 AMI 및 수요반응, 전기차충전인프라, 배전관리 및 분산전원 등을 대상으로 하는 스마트그리드 보안 표준들을 살펴보도록 한다. 더불어 스마트그리드 보안 아키텍처에 대한 표준화 현황을 살펴봄으로써 스마트그리드 전반의 보안 강화를 위한 방안을 살펴보도록 한다.

Ⅲ. 스마트그리드 보안 아키텍처

스마트그리드의 전반에 대한 보안 이슈는 스마트그리드의 태생과 함께 지속적으로 중요하게 다루어졌다. 이는 스마트그리드가 전기를 공급하는 중요 기반시설에 해당하기 때문이다.

미국 NIST에서는 스마트그리드 보안 가이드라인(NIST IR 7628)을 2010년에 발표하고, 2014년 개정판을 발표하였다. 스마트그리드 보안 요구사항 목록, 스마트그리드 인터페이스 유형별 보안 요구사항 수립 방안, 프라이버시 보호 이슈, 스마트그리드 보안과 관련한 연구개발 주제, 스마트그리드 보안 위험 분석 방법 등을 다루고 있다[8]. NIST IR 7628은 세계 최초의 스마트그리드 보안 아키텍처이며, 이에 따라 유럽을 포함한 전 세계에서 참고하여 자국의 스마트그리드 보안 가이드라인을 수립 중이다.

IEC는 IEC 62351-10 표준에서 스마트그리드 보안 아키텍처를 다룬다. 해당 표준에서는 스마트그리드 보안 대책 수립을 위한 절차를 제시하는 것을 목표로 스마트그리드 인터페이스 유형, 보안 통제사항, 인터페이스별 보안 통제사항 선정 방안 등을 제시한다[9]. NIST IR 7628과 달리 IEC 62351-10에서는 각 인터페이스별 보안 도메인을 결정하고, 보안 도메인의 보안 수준에 따라 동일한 인터페이스라도 다른 수준의 보안 통제사항을 적용하도록 요구한다.

ITU-T에서는 2016년 6월 스마트그리드 보안 기능 아키텍처를 ITU-T X.1111 표준의 부속서로 발간했다. 스마트그리드 서비스의 보안 위협, 보안 위협 해소를 위한 보안 요구사항, 스마트그리드 서비스 분야별 필요 보안기능 등을 제시하였다[10].

국내 한국정보통신기술협회(TTA)에서도 스마트그리드 보안 아키텍처와 관련한 표준들을 개발하였다. 그 중 스마트그리드 보안 요구사항 표준은 NIST IR 7628의 스마트그리드 보안 요구사항 중 일부를 한국 실정에 맞게 제시하며[11], 스마트그리드 시스템 보안 기능 요구사항 표준은 스마트그리드를 구성하는 서비스, 네트워크, 단말, 가입자 각각에 대한 보안 기능을 명세한다[12].

또, 한국스마트그리드협회에서 운영하는 스마트그리드표준화포럼에서는 단체표준으로 스마트그리드 표준의 보안성 확보를 위한 요구사항 표준을 개발하였다. 이 표준에서는 스마트그리드 표준을 개발할 때 각 신규 표준의 대상이 보안 기능을 포함해야 하는 지를 판단할 수 있는 가이드를 제시하고, 보안 기능이 필요할 경우 보안 위협, 보안 요구사항, 보안 기능 등을 식별할 수 있는 프레임워크를 제시한다[13]. 또한 소규모 스마트그리드라고 간주할 수 있는 마이크로그리드를 대상으로 최소한의 보안 요구사항들을 적시한 표준으로 마이크로그리드 구축 시 참조할 수 있는 마이크로그리드 보안 요구사항을 개발하였다[14].

Ⅳ. AMI 및 수요반응

효율적인 전기에너지 공급 및 생산이라는 스마트그리드의 목표를 달성하기 위해서 가장 중요한 것은 실시간 전력 사용 현황을 파악하고, 파악된 정보를 바탕으로 향후 사용 계획을 수립하고, 전력이 부족할 경우 소비자의 전력사용량을 능동적으로 조정하기 위해 수요반응(Demand Response) 기술을 사용한다. 이 중 실시간 전력 사용정보 수집을 위해 구축되는 지능화된 검침 인프라가 AMI며, 소비자의 전력사용량 조절을 위한 서비스가 수요반응이다.

4.1. AMI(Advanced Metering Infrastructure)

AMI는 소비자의 전력사용정보 측정 및 전송을 위한 스마트 미터가 가정, 건물, 상가 등에 설치되고, 이로부터 정보를 수집 전달하기 위한 데이터수집장치(DCU)들이 존재하며, 데이터수집장치로부터 수집한 데이터를 처리하는 서버시스템 등으로 구성된다.

AMI에서는 전력사용정보를 스마트 미터가 서버시스템으로 전송하는 과정에서 발생 가능한 보안 문제가 주요 이슈로 다루어진다. 전력사용 정보의 유출로 인해 개인의 생활패턴이 노출되는 등의 프라이버시 침해 문제와 스마트 미터 조작을 통한 전력요금 편취 및 전력수요 예측 시스템 오류 유발 등의 문제가 있을 수 있다[3-7]. 이에 따라서 스마트 미터와 데이터 수집 시스템 간 인증과 통신데이터 보호 기능을 추가한 통신 표준이 개발되고 있다.

IEC(International Electrotechnical Commission)의 TC13 WG14에서는 스마트 미터와 데이터 수집 장치 간 통신규격 개발하고 있다. 해당 표준은 IEC 62056 시리즈로 발표되고 있으며, 그 중 응용계층 표준인 IEC 62056-5-3에서 보안규격을 명시하고 있다. 이 규격은 2016년 3월 2.0이 발표되었으며, 동 버전에서는 스마트 미터와 수집장치 간 대칭키 기반의 인증과 통신 데이터 보호에 대한 규격을 명시하였다[15]. 현재 IEC TC13 WG14는 공개키 기반의 인증, 키 공유, 부인방지 기능

등을 포함하는 IEC 62056-5-3 Ed.3.0을 개발 중에 있다. 현재 국내에서는 AMI를 위해 DLMS/COSEM을 스마트 미터와 데이터 수집장치 간 통신 규격으로 사용할 예정이다.

IEC62056 시리즈의 대안으로 지그비 연합(ZigBee Alliance)이 주도하여 개발한 SEP(Smart Energy Profile)2.0을 들 수 있다. SEP2.0은 인증, 통신데이터 보호, 부인방지 등의 보안 서비스를 위해서 인증서 기반의 TLS를 사용할 것을 요구한다[16]. 현재 IEEE에서 SEP2.0을 표준으로 제정하였다[16].

이처럼 AMI 기기 간 통신에 대한 보안 규격은 표준화 기구에서 개발하고 있지만 AMI 전반에 대한 보안 아키텍처를 제시하는 표준은 아직 개발되지 않아 AMI 구축 사업자들이 보안대책에 고심하고 있다. 이에 국내에서는 스마트그리드표준화포럼을 통해 AMI 통신보안 사례를 제시하기 위한 단체표준 개발을 논의 중이다.

4.2. 수요반응(Demand Response)

수요반응은 전력수급 예측을 바탕으로 전력공급이 부족할 때, 소비자의 전력사용을 조절하여 전기의 공급과 소비의 균형을 맞추는 서비스다. 이를 위해 전력시장 운영자와 등록된 사용자 간 수요반응과 관련된 신호를 전달하기 위한 통신규약이 필요하다.

2012년 OpenADR 연합에서 수요반응과 관련한 통신규격으로 OpenADR 2.0을 발표했다. 이 규격에는 수요반응 신호를 교환하기 위한 데이터 유형부터 통신절차까지 다루고 있으며, 보안 규격도 함께 명시한다. OpenADR 2.0은 인증서를 사용하는 TLS (Transport Layer Security)를 통해 인증 및 통신데이터 보호 기능을 제공하도록 한다[17]. 더불어 보다 강력한 보안을 위해 부인방지 서비스가 필요할 경우에는 XML 전자서명을 추가하여 사용하도록 하고 있다.

OpenADR 2.0은 2014년 2월 IEC에 의해 수용되어 IEC PAS 62746-10-1로 발표되었다[17]. 더불어 국내에서도 스마트그리드표준화포럼을 통해 2015년 6월 국내단체표준으로 제정되었다[18].

4.3. 댁내 기기 보안

AMI 및 수요반응 등의 서비스는 결국 소비자 영역의 기기가 사용하는 전기사용량을 줄이거나 사용시간대를 이동하여 전기에너지 소비의 효율성을 제고하기 위한 것이다. 따라서 두 서비스는 소비자 댁 내의 기기와 상호연동될 가능성이 있으나, 물리적 보안 등이 취약해 새로운 공격 경로가 될 수 있다. 이에 댁내 기기의 사이버 안전성을 높이기 위한 보안 표준도 개발되는 중이다.

ITU-T(International Telecommunication Union – Telecommunication standardization sector) SG17에서는 HAN(Home Area Network)의 기기에 대한 보안 가이드라인을 표준으로 개발 중이다. 이 표준에서는 HAN 영역의 주요 기기에 대한 보안 위협과 보안 요구사항을 식별하고, 보안 요구사항을 만족시키기 위해 기기 및 기기 간 통신 구간에 적용되어야 하는 보안 기능을 명세한다[19].

국내에서는 TTA에서 스마트그리드와 연동하여 동작하는 가정 내 기기에 대한 보안 요구사항을 명시하는 스마트그리드 적용을 위한 HAN 기기 보안 메커니즘 표준[20]과 해당 보안 요구사항을 만족시키기 위해서 HAN 기기 각각에서 제공되어야 하는 보안 기능을 제시하는 스마트그리드 댁내 기기 보안 지침 표준[21] 등이 개발되었다.

Ⅴ. 전기차 충전 인프라

미래 전기차 세상을 생각해보자. 사람들은 전기차를 주요 교통 수단으로 활용할 것이다. 이 때 가장 중요한 문제는 전기차의 충전이다. 출퇴근용 차량은 출근 후 또는 퇴근 후 일정한 공간에서 충전이 이루어지겠지만 여가를 위한 사용의 경우에는 언제 어디서 충전이 일어날지 알 수 없다. 이로 인해 전기 공급을 책임지는 사업자 입장에서는 전력공급을 효율적으로 하기 위한 계획을 세우기 어렵다. 즉, 전력수요에 대한 불확실성이 발생한다. 이를 해결하기 위해서 전기차 충전 인프라를 구축하고, 수집되는 정보로 보다 빠르게 전기차 충전을 위한 전력공급을 효율적으로 추진하려고 한다.

이와 관련하여 전기차 충전 정보를 수집하고, 필요에 따라 전기차에게 충전기 관련 정보를 제공하거나 충전기를 제어하는 등의 역할을 수행하기 위한 전기차 충전 인프라가 구축될 예정이다. 이 인프라에서 전기차, 충전기, 충전기 관리 시스템 간 통신을 위한 규격에서 사이버 보안 이 반드시 고려되어야 한다.

ISO는 IEC와 협력하여 전기차와 전력망 간 통신 프로토콜에 대한 표준으로 ISO15118 시리즈를 개발하는 중이다. 현재 ISO15118 시리즈 중 1편부터 3편까지 3가지 표준이 발표되었고, 2편과 3편에 대한 적합성검증을 위한 표준이 개발 중이다. ISO 15118 표준의 2편인 ISO15118-2 표준은 네트워크 및 응용 계층 프로토콜 요구사항을 정의하며, 이 표준에서 인증서 기반의 TLS를 사용한 통신보안 기능의 구현을 요구한다[22]. 더불어 메시지 보안을 위해 XML에 대한 전자서명을 포함할 것도 요구한다.

Ⅵ. 배전관리 및 분산전원

스마트그리드의 또 하나의 목적은 전력시스템의 지능화된 운용이다. 지능화된 기기 및 기술을 통해 전력망에서 발생하는 문제를 빠른 시간에 탐지하고, 이를 적시에 해결함으로써 전력공급의 안정화 및 전기품질의 개선을 꾀한다. 이러한 목적 달성을 위해서 IEC 61968/61970, IEC62541, IEC61850, DNP3.0, Modbus 등의 다양한 정보통신 규격이 사용된다.

또한 풍력, 태양광 등의 신재생 에너지 발전원과 이를 통해 생산된 전기의 안정적 공급을 위한 전기저장시스템 등으로 구성되는 분산전원 역시 신뢰성 있는 운용을 위해서 지능화된 감시 및 제어가 이루어지며 이는 전력시스템을 위한 정보통신 규격과 동일한 규격이 사용된다.

이렇게 지능화된 전력시스템 및 분산전원은 통신과정에서의 정보유출 및 잘못된 정보의 삽입, 제어명령 조작에 따른 오동작 등의 보안위협에 노출되어 있다. 이에 따라 배전관리 시스템에 대한 전반적 보안관리가 이루어져야 하며, 지능화 기기 및 분산전원에 대한 안전한 통신을 위해 인증 및 데이터 보호 기능이 적용되어야 한다.

6.1. 전력시스템 보안관리

배전관리 및 분산전원 운용을 위한 전력시스템에 대한 보안관리에 대한 표준은 스마트그리드 개념이 도입되기 이전부터 개발 되고 있다.

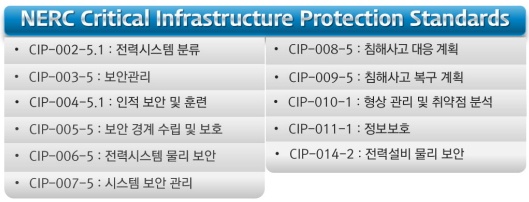
ISA(International Society of Automation)에서는 제어시스템에 대한 보안 가이드라인 표준인 ISA99 시리즈를 개발하였다. 제어시스템 구축, 운용 등의 전반에 걸친 보안 규정 수립·시행에 대한 내용을 담았다[23].

2010년 이후 ISA는 IEC와 협력하여 ISA99 시리즈를 IEC62443 시리즈 표준으로 통합하여 개발하고 있다. IEC62443은 제어시스템 운용 전주기에 걸친 보안 강화 방안을 제시하는 것을 목표로 표준을 개발 중이다. 보안정책 및 절차 수립, 시스템 수준의 보안 기술, 제어시스템의 콤포넌트(기기) 수준의 보안 기술 등을 모두 제시하고자 한다[23].

더불어 IEC는 2016년 IEC 62351-12 표준에서 분산전원 설비에 대한 보안 권고사항을 발표했다. 이 표준은 분산전원을 구성하는 각 설비에 대한 보안위협 및 운영상의 취약점 등을 식별하고, 식별된 위협을 제한하기 위한 권고사항을 제시하였다[25].

북미지역의 전력시스템 운영 신뢰도 보장 기구인 NERC(North-american Electricity Reliability Cooperation)은 전력설비의 사이버 보안 강화 기준으로 CIP(Critical Infrastructure Protection)를 개발하였다. 이는 스마트그리드에 특화된 보안 표준은 아니지만 스마트그리드의 근간이 되는 전력시스템 운용에 관계하는 정보통신시스템에 대한 보안기준이다. 정책수립, 인적 보안, 네트워크 보안, 시스템 보안, 보안관제, 사고조사, 복구, 물리보안 등에 대한 11개의 기준을 제시한다[26].

〔그림 2〕 IEC 62443 표준 개발 계획[24]



〔그림 3〕 NERC CIP 기준 목록

6.2. 통신보안 기능

배전관리 및 분산전원 운용을 위한 전력시스템은 원격 제어 기능을 가지고 있어 반드시 통신보안 기술이 적용되어야 한다. 그런데 앞서 밝힌 배전관리 및 분산전원 운용을 위한 프로토콜 중 IEC62541을 제외하면 통신보안 기능은 포함되어 있지 않다.

이에 IEC TC57 WG15에서는 배전관리 및 분산전원 운용을 위한 프로토콜에 대한 보안 표준인 IEC62351시리즈를 개발 중이다. IEC62351 표준에는 DNP3.0, IEC61850, IEC60870-5 TASE.2 (ICCP) 등의 표준을 위한 통신보안 표준을 개발하였다. 더불어 이러한 통신보안 표준의 보안성을 강화하기 위한 키 관리 기술 및 메시지 전자서명 기술 등도 개발하고 있는 중이며, 배전관리 및 분산전원 등의 전력시스템에 대한 보안 관리를 위한 네트워크 관리 및 접근제어 등에 대한 표준도 개발 하였다[27][28].

한편 IEC61968과 IEC61970등의 표준으로 정의된 전력시스템 정보를 시스템 간에 교환하기 위해서 IEC62541로 정의되는 통신표준을 사용한다. 해당 표준은 XML로 정의된 전력시스템의 공통 정보 모델을 전달하며, 이에 대한 보안 강화를 위해 인증서 기반의 강력한 보안 규격을 제시했다[29][30]. 인증서 기반의 기기 상호인증, 인증서 기반의 응용 프로그램 인증, 전송계층 보안, 응용 계층 메시지보안 등 통신보안 요구사항을 가장 강력하게 만족시키도록 보안 규격이 제시되었다.

Ⅶ. 결 론

지금까지 스마트그리드의 대표적인 서비스별로 각 시스템의 보안과 관련한 표준화 동향을 살펴보았다. IEC, ISO, ITU-T 등의 국제표준화 기구는 물론 NIST, NERC 등의 정부기구 및 규제기관에서도 스마트그리드 또는 전력정보시스템에 대한 보안 표준을 개발하고 있다. 또한 국내에서도 스마트그리드표준화포럼 및 TTA 등에서 스마트그리드 보안 표준을 활발히 개발하고 있다.

하지만 대부분의 표준이 전반적인 보안 요구사항 또는 특정 통신 프로토콜에 대한 통신보안 기술 등을 위주로 개발되었고, 현재 개발 중이다. 스마트그리드와 같이 복잡한 시스템 구성에서 시스템 단위 또는 프로토콜 단위의 보안 표준도 중요하지만, 서비스 사업자들이 구축 단계에서 보안 대책을 고려하고 도입할 수 있도록 서비스 자체에 대한 보안 대책 수립 가이드라인 역시 중요하다. 따라서 스마트그리드 분야 전문가와 정보통신 분야 전문가 및 사이버 보안 전문가 등이 융합하여 향후 스마트그리드 서비스에 대한 보안 가이드라인들이 표준으로 제정될 수 있도록 노력이 필요하다.

참 고 문 헌

[1] H. Holttinen and R. Hirvonen, Power system requirements for wind power, in Wind power in power systems(ed T. Ackermann), Jon Wiley & Sons, Ltd., pp. 144-167, Oct 2005.

[2] “스마트그리드 상호운용성 표준 프레임워크 및 로드맵 1.0”, 지식경제부 기술표준원, pp.27, 2012.

[3] S. Mishra, X. Li, A. Kuhnle, M. Thai and J. Seo, “Rate alteration attacks in smart grid,” Proceedings of the IEEE International Conference on Computer Communication, pp. 2353-2361, Apr 2015.

[4] O. Kosut, L. Jia and R.J. Thomas, “Malicious data attacks on smart grid state estimation: attack strategies and countermeasures,” Proceedings of the IEEE International Conference on Smart Grid Communications 2010, pp. 220-225, Oct 2010.

[5] A. Mohsenian-Rad and A. Leon-Garcia, “Distributed internet-based load altering attacks against smart power grids,” IEEE Transactions on Smart Grid, Vol. 2, No. 4, pp. 667-674, Dec 2011.

[6] D. Grochocki, J.H. Huh, R. Berthier, R. Bobba, W.H. Sanders, A.A. Cardenas and J.G. Jetcheva, “AMI threats, intrusion detection requirements and deployment recommendations,” Proceedings of the IEEE International Conference on Smart Grid Communications 2012, pp. 395-400, Nov 2012.

[7] D. Mashima, “Authenticated down-sampling for privacy-preserving energy usage data sharing,” Proceedings of the IEEE International Conference on Smart Grid Communications

2015, pp. 605-610, Nov 2015.

[8] "Guidelines for smart grid cybersecurity," NIST IR 7628, NIST, 2014.

[9] IEC, "Power systems management and associated information exchange – data and communications security – part 10: security architecture gudielines," IEC/TR 62351-10, Oct 2012.

[10] ITU-T, "ITU-T X.1111-Supplement on security functional architecture for smart grid services using telecommuinication networks," ITU-T Series X Supplement 26, Mar 2016.

[11] TTA, "스마트 그리드 보안 요구 사항," TTA.KO-12.0182, 2011년 12월.

[12] TTA, "스마트 그리드 시스템 보안 기능 요구 사항," TTA.KO-12.0209, 2012년 12월.

[13] 스마트그리드표준화포럼, "스마트그리드 표준의 보안성 확보를 위한 요구사항," SGSF-121-1, 2014년 3월.

[14] 스마트그리드표준화포럼, "마이크로그리드용 공통 플랫폼 사이버 보안 요구사항," SGSF-011-2, 2016년 5월.

[15] IEC, "Electricity metering data exchange – the DLMS/COSEM suite – part 5-3: DLMS/COSEM application layer," IEC 62056-5-3, Edition2.0, Mar 2016.

[16] IEEE, "IEEE adoption of smart energy profile 2.0 application protocol standard," IEEE Std. 2030.5-2013, Nov 2013.

[17] IEC, "Systems interface between customer energy management system and the power management system – part 10-1: open automated demand response (OpenADR 2.0b Profile Specification)," IEC PAS 62746-10-1, Feb 2014.

[18] 스마트그리드표준화포럼, "OpenADR 2.0 B 프로파일," SGSF-073-2-2, Ed. 1.0, 2014년 3월.

[19] 서정준, 고웅, 박해룡, "Security guidelines for home area network (HAN) devices in smart grid system," ITU-T X.sgsec-2, Mar 2016.

[20] TTA, "스마트그리드 적용을 위한 HAN 기기 보안 메커니즘," TTA.KO-12.0258, 2014년 12월.

[21] TTA, "스마트그리드 댁내 기기 보안 지침," TTA.KO-12.0287, 2015년 12월.

[22] ISO, "Road vehicles – vehicle-to-grid communication interface – part 2: network and application protocol requirements," ISO 15118-2, Apr 2014.

[23] IEC, "Industrial communication networks – network and system security – part 1-1: terminology, concepts and models," IEC 62443-1-1, Jul 2009.

[24] IEC, "Industrial communication networks – network and system security – part 3-3: system security requirements and security levels," IEC 62443-3-3, Aug 2013.

[25] IEC, "Power systems management and associated information exchange – data and communications security – part 12: resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems," IEC TR 62351-12, Apr 2016.

[26] J.M. Cole, "Challenges of implementing substation hardware upgrades for NERC CIP version 5 compliance to enhance cyber security," Proceedings of 2016 IEEE/PES Transmission and Distribution Conference and Exposition, pp. 1-5, May 2016.

[27] R. Tawde, A. Nivangune and M. Sankhe, "Cyber security in smart grid SCADA automation systems," Proceedings of 2nd International Conference on Innovations in Information, Embedded and Communication systems 2015, pp. 1-5, Mar 2015.

[28] IEC, "Power systems management and associated information exchange – data and communications security – part 11: security for XML documents," IEC 62351-11 FDIS, Mar 2015.

[29] A. Claassen, S. Rohjans and S. Lehnhoff, "Application of the OPC UA for the smart grid," Proceedings of IEEE PES International Conference and Exhibition on Innovative Smart

Grid Technologies (ISGT Europe), pp. 1-8, Dec 2011.

[30] IEC, “OPC Unified Architecture – Part 2: security model,” IEC TR 62541-2, Feb 2010.

〈저자소개〉

사 진

이 건 희 (Lee, Gunhee)

정회원

2001년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업

2003년 2월 : 아주대학교 정보통신전문대학원 정보통신공학과 석사

2009년 2월 : 아주대학교 정보통신전문대학원 정보통신공학과 박사

2009년 3월 ~ 현재 : ETRI부설국가보안기술연구소 연구원(선임연구원)

<관심분야> M2M 인증, Authorization, 스마트그리드, DER, EVCI