국내 에너지 산업 및 사이버보안 기술개발 동향

이동호
한국에너지기술평가원
융합인재양성팀

Ⅰ. 발 문

에너지 산업은 전통적으로 안전성을 최우선시 하는 분야로써 새로운 기술의 접목에 인색한 영역이다. 하지만 급변하는 IT기술의 발달, 사회 인식의 변화, 국가에너지기본계획 등 정책의 변화에 따라 사이버보안을 고려할 수밖에 없는 상황이 되었다. 속도는 더디지만 에너지 산업에서 사이버보안 기술은 전력IT 분야에서 시작해서 송배전분야, 원자력 발전 등 타 에너지 분야로 확산되고 있고, 당분간 사이버보안 전문가들의 활동 영역은 넓어질 것으로 예상된다. 본 고에서는 전력분야를 중심으로 에너지산업에 대한 이해를 돕기 위한 내용을 먼저 소개하고, 현재 에너지 분야 보안 기술 동향을 다룬다.

오늘날 정부의 에너지 정책이 "공급중심에서 수요 관리 위주"로, "대형발전소에서 분산형 발전시스템"으로 방향이 전환됨에 따라 수요자에게 에너지망이 오픈되었고, 이로 인해 사이버 보안에 대한 중요성이 크게 증가하였다.

Ⅱ. 최근 에너지 정부정책 방향

정부정책에서 에너지는 에너지기본법에 따라 연료 · 열 및 전기로 정의되는데, 5년마다 향후 20년 계획을 수립하는 「국가에너지기본계획」을 최상위로 하여 분야별로 다양한 하위 계획을 수립하고 실행한다. 2014년에 발표되어 2035년까지 에너지정책의 중장기 목표를 담은 제2차 국가에너지기본계획에서 주목할 말한 사항은 「공급중심에서 수요관리 위주」로, 「대형발전소에서 분산형 발전시스템」으로 정책방향의 전환이다[1]. 이와 관련된 전력시장 변화를 〈그림 1〉에 나타내었다. 이미 관련분야 전문가 사이에서는 나아갈 방향이라고 인식하고 있던 것이 2011년

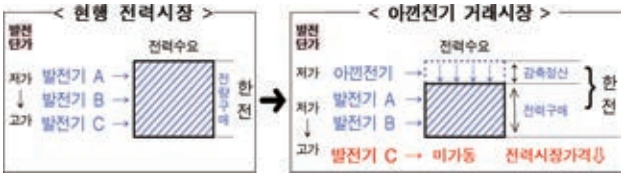
9 · 15순환정전사태 및 밀양 송전탑 이슈가 촉매 역할을 하여 자연스럽게 국가 최상위 정책에 스며들었다.

공급중심에서 수요관리로의 무게 중심의 이동은 기존의 대형 에너지공급원인 몇 개의 발전소만을 제어하는 구조에는 한계를 느끼고, 수많은 에너지 소비자의 수요량을 예측하고 일부 조율하는 정책변화를 의미한다. 이것은 단방향 전력공급에서 쌍방향 통신을 통해서 전력을 효율적으로 공급하겠다는 것이다. 따라서 기존에 접근이 어려웠던 에너지 망이 수요자 쪽에서는 오픈될 수밖에 없는 상황이 되어 사이버 보안을 더욱 고려해야 하는 환경이 된다. 대형 발전소에서 분산형 발전시스템의 확대 또한 같은 논리로 공급자 쪽에서도 오픈된다는 것을 의미한다.

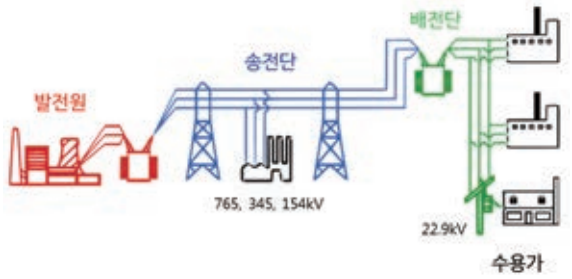
2차 에너지 기본계획에 따라 수립된 제3차 에너지기술개발 계획은 2023년까지 기술개발 방향을 담고 있는데, 이것에는 ICT기술을 이용한 에너지 수요관리기술을 주요 내용으로 하고 있다. 구체적으로 17개 기술개발 프로그램이 포함되어 있는데 IoT, 스마트 홈 · 빌딩, 스마트 마이크로그리드 등 사이버보안 기술이 빠질 수 없는 기술영역이 다수 포함되어 있다.

Ⅲ. 국내 에너지산업의 특징

에너지산업의 경계선이 모호하나, 통상적으로 에너지를 생산하는 발전기술, 생산된 에너지를 수요자에게 전달하는 송배전 기술, 에너지 소모량이 많은 기기의 효율향상 기술, 자원개발 기술 등이 포함된다. 이중 최근 변화된 에너지정책의 주요 영역을 차지하는 발전 및 송배전 산업은 한국전력공사를 중심으로 형성되어 있다. 2001년 한국전력공사의 발전부문을 5개 화력발전사(한국남동발전, 한국중부발전, 한국서부발전, 한국남부발전, 한국동서발전)와 한국수력원자력으로 분리하여 경쟁체재를 도입하



〈그림 1〉 전력시장 변화 개념도

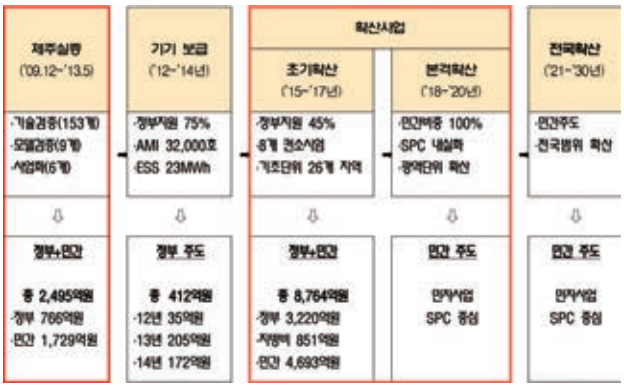


〈그림 2〉 국내 전력계통 개념도

〈그림 3〉 2015년 국내 전력 계통도

였고, 송배전분야는 여전히 한국전력공사가 독점적으로 담당하고 있다. 즉, 국내 전력산업은 6개의 대형 발전회사와 소형의 민간발전사들이 전력을 생산하고, 전력거래소에서 그것을 구입하여 한국전력공사가 수요자들에게 전달, 판매하는 구조이다[2].

국내 발전 및 송배전분야는 2011년 9 · 15순환정전 사태로 상처를 입기는 했지만, 대체적으로 안정적으로 운영되고 있는 모범적인 사례로 평가 받고 있다. 〈그림 3〉에서 나타낸 것처럼 현재 국내의 전력 계통도는 전국을 거미줄처럼 연결해서 하나의 신뢰도 높은 송전계통을 구축 운영하고 있다. 장거리 에너지를 전달하는 345kV, 154kV급 송전망과 단거리 22.9kV급 배전망이 다중 환상망(Multi-loop) 형식으로 구성되어 있다. 국내 전력산



〈그림 4〉 스마트그리드 전국망 구축 계획(안)

업이 훌륭히 운영되고 있다고 하지만 구조적인 취약점은 하나의 독립망으로 구성되어 있다는 것이다. 이것은 문제가 생겨서 Black Out 되면 복구가 매우 힘들다는 것을 의미한다. 만일 물리적인 사고, 사이버 공격 등으로 인해서 전체 전력망이 균형을 잃어버린다면 복구가 매우 어려운 치명적인 구조이다.

훌륭하게 운영되어 왔고 고도의 안정성이 요구되는 산업의 종사자들은 자연스럽게 새로운 기술의 접목을 매우 조심스러워 한다는 점을 정보통신을 주 영역으로 가지고 있는 연구자들이 에너지 산업에 접근할 때 첫 번째 겪는 어려움일 것으로 예상된다.

기술적 표준화 및 사이버 보안에 대한 기술 개발을 위한 중간 단계의 사업으로 "스마트그리도 상호운용성 시험센터 구축사업"이 2013년에 시작되었다. 이는 기존의 기술 개발 및 보급 과정에서 뒤늦게 보안의 중요성을 인식하고 반영하는 형태로 발전해 온 것을 의미한다.

Ⅳ. 스마트그리드 산업 동향

에너지 산업 중 가장 보안기술을 폭넓게 수용하고 있고 필요성이 인식되는 스마트그리드 산업의 동향에 대해서 살펴보자.

스마트그리드란 기존 전력망에 정보통신기술을 접목하여, 공급자와 수요자간 양방향으로 실시간 정보를 교환함으로써 지능형 수요관리, 신재생에너지 연계, 전기차 충전 등을 가능하게 하는 차세대 전력 인프라 시스템을 의미한다[3]. 2005년 전력IT 10대과제를 시작으로 관련 기술개발이 본격적으로 시작되면서 2009년 약 2,500억 원 투자해 3.5년간 추진한 제주 스마트그리드 실증사업이 2013년 5월 종료되면서 이제는 기술개발보다도 보급에 무게 중심이 이동해 있는 상태이다. 스마트그리드는 지능형 송배전(Smart Power Grid), 지능형 소비자(Smart Consumer), 지능형 서비스(Smart Electricity Service), 지능형 운송(Smart Transportation), 지능형 신재생(Smart Renewables) 5개 분야로 나뉘어 시행되고 있으며 관련 세부 기술개발 내용은 〈표 1〉과 같다.

〈표 1〉 스마트그리드 분야별 기술개발 내용

구분	기술개발 내용
지능형송배전	전력망 지능화, 개방화(EMS등), 스마트 배전시스템, 분산자원 통합 및 연계(VPP등)
지능형 소비자	표준화된 AMI개발, 수요관리, 변동부하 기반 수요반응, DIM기반 xEMS시스템, EV인프라 연계형 AMI시스템, 수용가 마이크로그리드
지능형 서비스	수요자원 통합, 수요자원 개발, 도매 전력거래시스템 지능화, 도매 전력거래시스템 고도화, 온라인 소비자 전력거래시스템, 온라인 소비자 전력거래시스템 고도화, RTP 요금제 및 실시간 DR운영 시스템
지능형 운송	EV 통합운영 및 연계시스템, V2G기술, V2G 계통연계 및 운용기술, 핵심부품 소재개발
지능형 신재생	신재생발전 등 분산자원 계통연계 안정화기술 개발 및 실증, 10MW배전계통연계, 배전급 마이크로그리드, 수백 MW급 전력저장 기술개발 및 실증

2013년 제주 스마트그리드 실증사업이 종료되고 당초 계획했던 7대 광역권별 스마트그리드 거점도시 구축에 앞서 계획에 없던 "스마트그리드 상호운용성 시험센터 구축사업"을 2013년 시작했다. 다양한 이유가 있었지만 기술적으로는 표준화와 사이버 보안의 기술개발이 미흡해서 중간단계의 사업이 필요하다고 판단해서였다.

다시 거슬러 올라가면 기술개발 측면에서는 2005년에 전력IT10대과제의 착수, 2009년 제주스마트그리드 실증사업이 시작되고, 보급측면에서는 한국전력공사에는 AMI보급사업을 2013년 시작했다. 한편 후술하게 될 보안 분야 기술개발에 있어서는 보안체계 연구가 2010년 12월에서야 착수하면서 본격적으로 시작했다. 기존의 기

〈그림 5〉 제주 스마트그리드 실증단지

술개발과 보급에서는 보안을 고려하지 않을 수 있는 구조였으며, 뒤늦게 반영해야 하는 상황으로 산업이 발전해 오고 있었다.

Ⅴ. 전력계통분야 보안기술 동향

전력계통분야 사이버보안 기술개발은 현재 운영 중인 단일 전력제어망의 취약점을 분석하고 보완하는 기술개발과 미래의 수요관리, 분산전원의 확대를 고려한 스마트그리드와 관련 기술개발로 구분할 수 있다. 전자는 성격상 접근이 쉽지 않고 한국전력공사가 주도적으로 연구개발이 가능한 영역으로 이미 100억 원 이상 규모의 연구개발 과제를 완료하고 일부 실계통에 적용 한 것으로 알고 있으며, 관련해서 지속적으로 연구개발이 이루어지고 있을 것이다.

기존의 중장기 연구 과제를 통해서 스마트그리드 분야의 사이버 보안 기틀은 마련된 것으로 평가되며, 보안과 다른 주제가 연계된 형태의 개발이 진행 중에 있다.

한편, 스마트그리드 관련 보안 기술은 한국전력공사, 국가보안기술연구소, 한전KDN이 주축이 돼서 연구개발을 진행 중인데 국가보안기술연구소는 가이드라인 등 기준제시, 한국전력공사는 관제기술, 한전 KDN은 스마트미터 등 기기 보안 기술을 중심으로 연구가 이루어지고 있다.

구체적으로는 2010년 12월부터 개체 암호 · 인증기술, 표준화, 접근제어 기술, 평가 · 인증체계, 이상 징후 탐색, 악성코드 공격대응, 인증운용기술 등 전범위에서 포괄적으로 보안 체계를 구축하고, 보안에 필요한 기술의 최소한의 가이드라인을 도출하는 목표를 가지고 "스마트그리드 보안 체계 연구"라는 제목의 연구과제를 2년간 진행해서 완료했으며 부수적인 성과로 2012년6월. 제정된 최초의 에너지분야 사이버보안 관련 고시인 "지능형전력망 정보의 보호조치에 관한 지침" 에 연구내용을 반영하였다. 세부적인 기술개발을 추진하는 "스마트그리드 핵심 보안기술 개발"제목의 과제를 2011년 7월부터 4년간 추진했는데 선행과제의 구체적인 기술내용을 포괄적으로 다루었다.

"스마트그리드 보안 체계 연구" 및 "스마트그리드 핵심 보안기술 개발" 2개의 중장기 연구과제는 스마트그리드 분야 사이버보안의 기틀을 마련했다고 평가될 수 있다. 이제는 보안을 주요내용으로 하는 중장기 과제 보다는 다른 주제의 연구개발과제에 보안기술이 부수적으로 녹아서 연구개발이 진행되고 있다.

Ⅵ. 원자력분야 보안기술 동향

원자력 시설은 외부와 통신망이 분리되어 있고 물리적으로도 접근이 어렵기 때문에 사이버보안에 있어서 안전한 편이라고 할 수 있다. 하지만 우리나라는 명백한 위험대상인 북한이 존재하며, 외국에서도 특정 시스템을 목표

로 하는 지능형 지속공격(APT)이 원자력 발전소를 대상으로 발생한 바가 있어서 관련 연구 개발은 어떤 분야보다 중요하다고 할 수 있다. 최근 한국수력원자력 직원 개인정보 유출, 스턱스넷 침투흔적 등 그 진위와 관계없이 원자력분야의 사이버 보안에 관한 언론에서의 뜨거운 반응은 관련 분야의 중요성을 증명한다.

한국수력원자력은 2010년 11월 원전사이버 보안 위험도 분석 및 평가 가이드라인에 관한 연구개발 2년간 진행하였으며, 2012년 8월 국가보안기술연구소가 중심이 돼서 한국형 원전인 APR1400의 사이버보안체계 개발을 2연간 추진하였다. 그 외에도 한국수력원자력은 2013년 "가동 원전 계측제어시스템 사이버보안성 통합평가 도구 개발" 연구과제를 착수하는 등 지속적으로 기술개발을 추진 중이다. 또한 국가보안기술연구소와 MOU를 체결하고, 원자력 사이버보안 현황 및 추진전략, 기술 등의 전문가 발표로 구성된 원자력 사이버 보안 워크샵을 개최하는 등 보안기술 개발 분야에 관한 투자를 확대하고 있다.

Ⅶ. 그 외 에너지 분야

전술한 바와 같이 우리나라는 단일 전력망으로 구성되어 있기 때문에 전력의 공급과 소비의 균형을 잃으면 걷잡을 수 없는 상태가 된다. 발전설비의 60%이상을 차지하는 석탄, LNG, 석유 등 화력발전 등도 사이버보안 기술개발을 추가해야 하는 영역이다. 또한 현재는 태양광, 풍력과 같은 분산전원에서의 사이버 보안의 중요성은 떨어지지만, 6차 전력수급계획에 따라 27년까지 발전량 비중 12%이상(발전설비 비중 20%) 확대되고 서해안 해상풍력과 같은 대단지의 공급원이 형성될 경우 매우 중요해질 것이다.

단일 독립 전력계통, 북한의 존재 등의 국내환경을 고려하면 단기적으로 신규로 건설되는 화력 발전원부터 장기적으로 신재생 분산전원까지 사이버 보안 기술개발이 다른 대부분의 에너지산업에도 필요할 것으로 보인다.

Ⅷ. 사이버보안 인식의 중요성

에너지 분야 사이버 보안 기술개발 필요성을 인식하는 것 자체가 매우 중요하다. 우리나라는 북한이라는 명백한 공격위험 대상이 존재하기 때문에 다른 나라에 비해 특히 경각심을 가질 필요가 있다. 하지만, 중요도에 비해 에너지 분야 사이버 보안기술을 연구 개발하는 인력은 매우 제한적이다. 정보통신분야를 주 무대로 활동하고 있는 많은 전문가들이 에너지 분야에 관심을 가져 주기를 기대한다.

참 고 문 헌

[1] 제2차 에너지기본계획, 산업통상자원부

[2] 2014년 전기연감, 대한전기협회

[3] 제1차 지능형전력망 기본계획, 대한민국 정부

[4] 2015년 전력계통도, 전력거래소

이 동 호

- 2004년 2월 고려대학교 공학사(전기전자전파)
- 2014년 2월 고려대학교 공학박사(전자전기)
- 2009년 1월~2009년 12월 LG전자기술원 촉탁연구원 (방문연구원)
- 2011년 5월~현재 한국에너지기술평가원 연구원

〈관심분야〉
스마트그리드, 마이크로파 무선전력전송