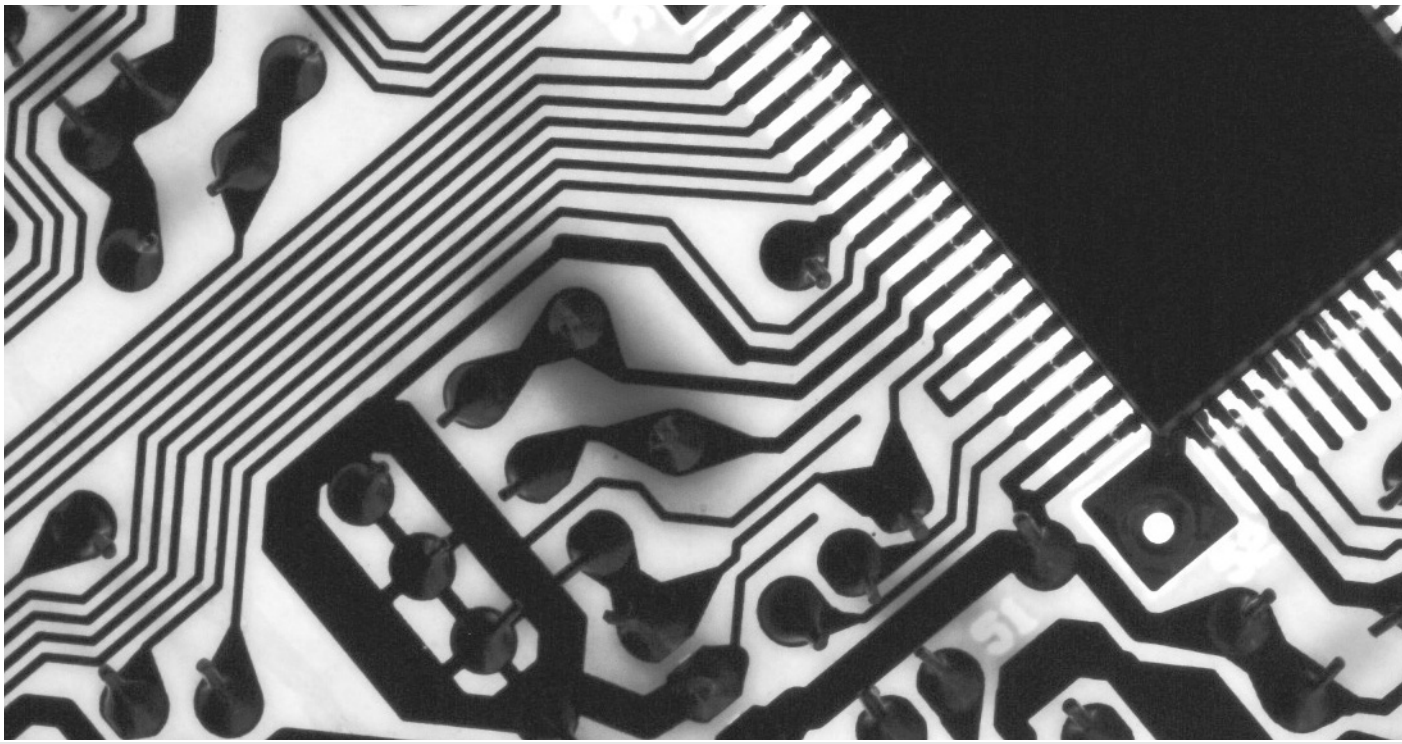


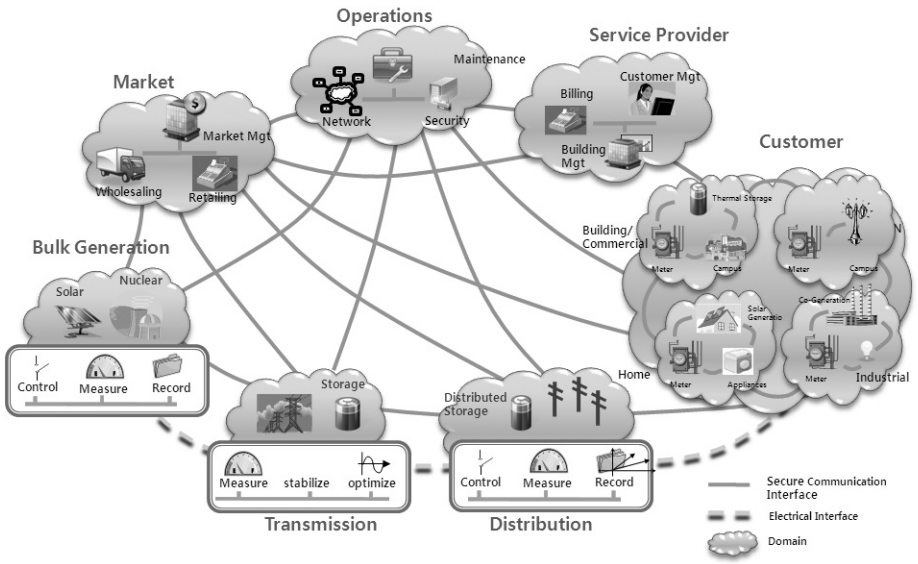
스마트 그리드 보안기술

김진철
한전KDN 전력IT연구원

1. 스마트 그리드의 개념과 보안기술 필요성

스마트 그리드는 IT 기반의 미래형 차세대 전력망으로 센서 · 통신 네트워크 · 자동제어 등의 IT 기술을 전력망에 도입하여 전력 인프라의 상호 호환성 · 보안성 · 신뢰성 · 효율성 · 안전성 등을 향상시키고, 전력회사 · 소비자 · 다양한 이해 당사자 간의 양방향 통신을 가능하게 하여 소비자의 전력 선택 범위를 넓히고, 이를 통하여 전력 인프라 시스템의 효율성을 향상시키는 친환경적인 디지털 시대를 위한 지능형 전력망이다.

[그림1]은 IEEE에서 제안한 스마트 그리드의 개념적인 정의이다. 그림에서 보이는 것처럼 전력의 흐름은 기존 전력망과 같이 발전 · 송전 · 배전 · 소비자로 흐르지만, 각 Domain간 Full Mesh 형태로 연결되어 있음을 알 수 있다.



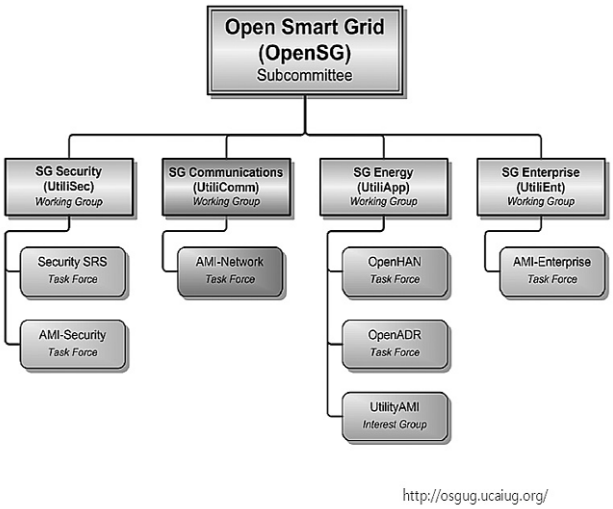
[그림1] 스마트 그리드의 개념적인 정의 (출처 : IEEE, 2009)

물론 국내 전력망은 해외 전력망과 체계가 다르기는 하지만 국내 전력망도 스마트 그리드로 진화되면 이에 참여하는 전력회사와 다양한 이해 당사자간 실시간 · 양방향으로 전력정보를 교환하게 되면서 사이버 공격이 가능한 새로운 경로들이 생성될 수 있으므로, 국내 스마트 그리드에서도 보안이 철저하게 유지되는 통신 네트워크로 연결되어야 한다.

현재까지 전력망은 폐쇄형 단독망 운영관리로 보안이 크게 문제되지 않았다. 하지만 스마트 그리드에서는 IT가 결합됨에 따라 정보통신 네트워크 기기에서 발생하고 있는 보안문제가 나타날 수 있는 우려가 높다. 더욱이 고객의 프라이버시 노출, 정보 도용, 사용요금 조작은 물론, 전력시스템의 마비까지 기존 전력망에서 나타나지 않았던 보안문제까지도 고려하는 보안기술이 개발되어야 한다.

2. 국외 스마트 그리드 보안기술 표준화 동향

미국의 스마트 그리드 표준화는 'Energy Independence and Security Act of 2007 '에 따라 NIST(National Institute of Standards and Technology)가 주도하고 있다. NIST의 CSCTG(Cyber Security Coordination Task Group)는 스마트 그리드 사이버 보안 표준제정을 위하여 보안 위협에 대한 시나리오를 선정 · 분석하고 취약점과 위협에 대한 위험 평가를 수행하고 있으며, "NIST Framework and Roadmap for Smart Grid Interoperability Standards"와 "Smart Grid cyber Security Strategy and Requirements"를 발표하였다. NIST는 AMI와 HAN을 스마트 그리드 실현을 위한 표준화 선결 추진 대상의 일부로 지정하여 관련 주요 표준 및 가이드라인을 권고하였고, IPv6에 기반한 AMI의 종단간 통신을 위한 관련 표준의 개정 작업을 PAP(Priority Action Plans)의 하나(PAP-01)로 진행중이다.

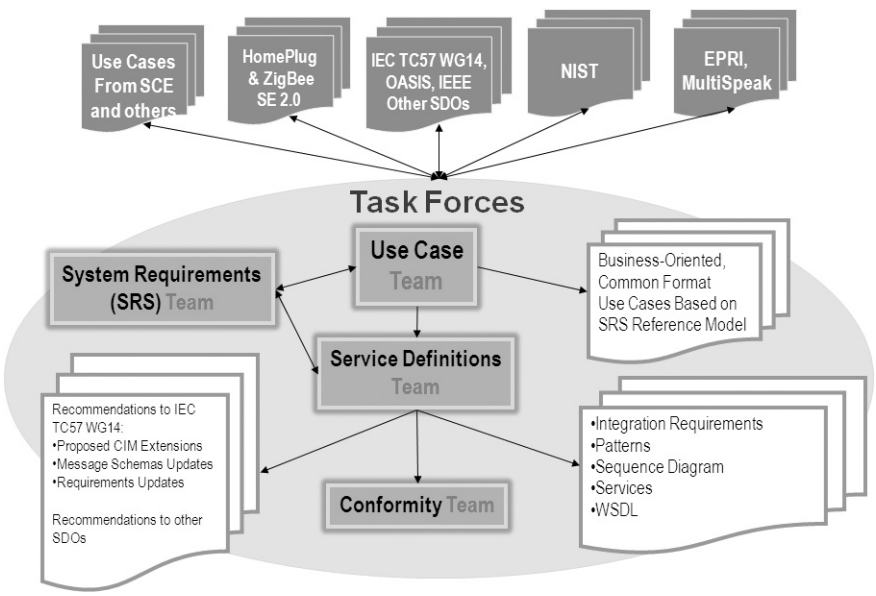


[그림2] Open Smart Grid User Group 조직도 (출처 : OpenSG, 2009)

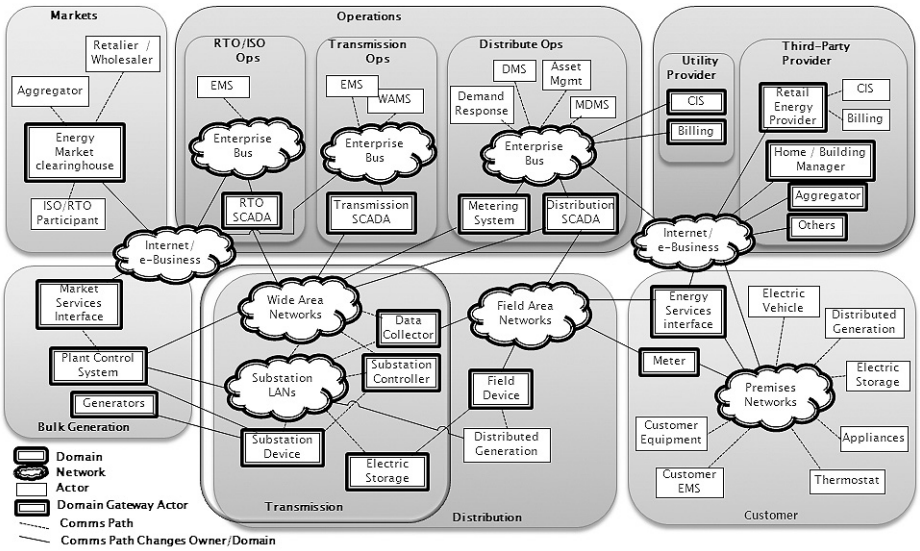
이러한 NIST의 스마트 그리드 표준제정은 실무적으로 **[그림2]**와 같이 Open Smart Grid Users Group(Open Smart Grid Subcommittee)에서 담당하고 있다. UCA International User Group의 Subcommittee인 Open Smart Grid Users Group은 AMI-SEC Task Force를 신설하여 AMI에 대한 사이버 보안 연구를 진행 중이다.

AMI-SEC Task Force에서는 AMI 보안 위협 모델을 연구하고 AMI 보안 요구사항을 작성하여 배포하였다. AMI-SEC Task Force은 **[그림3]**과 같이 Use Case Team, SRS Team, Service Definition Team, Confirmity Team으로 구성하여 SCE와 같은 전력회사, HomePlug, ZigBee Alliance, IEC TC 57, OASIS, IEEE, NIST, EPRI, MiltiSpeak 등의 표준단체와 연구결과를 공유하고 있다.

EU는 European Technology Platform Smart Grids를 설립하여 스마트 그리드의 비전과 연구개발에 대한 전략을 수립하였다. 2006년에는 비전에 대한 문서를 발표하였고 2007년에는 기술개발에 대한 전략을 수립하였으며, 2008년에 이르러 배치 전략을 수립하는 드래프트들을 각각 발표하였다. 총 5개 부문의 19개 세부 과제를 선정하고 스마트 그리드의 장애 및 외부 공



[그림 3] AMI-SEC TF 표준화 활동체계 (출처 : OpenSG, 2009)



[그림 4] 스마트그리드의 개념적인 레퍼런스 다이어그램 (출처 : NIST, 2009)

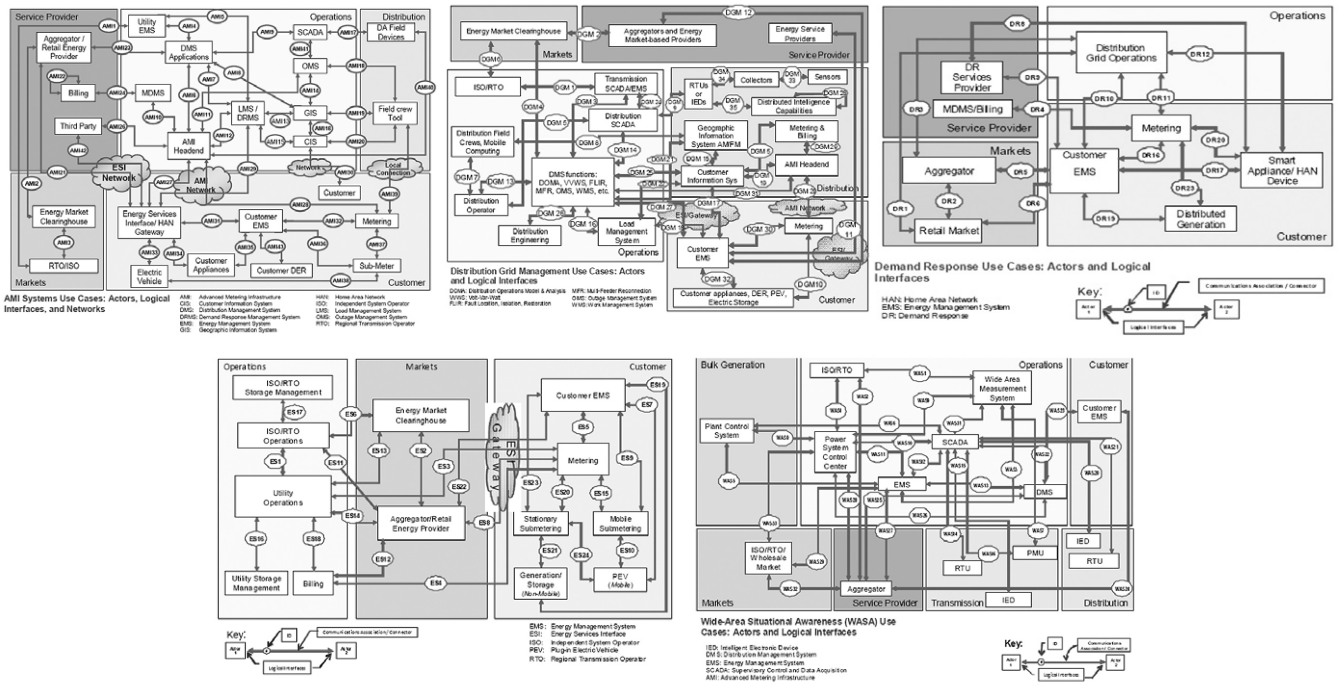
격에 대한 대응방안, 송 · 배전 시스템의 사이버 보안 및 복구능력 향상을 위한 방법론 등을 중점으로 하고 있다. EU의 19개 전력회사가 모여 진행 중인 스마트 미터 표준화 프로젝트인 Open meter Consortium에서는 보안을 비롯한 AMI의 구성요소 각각에 대한 기능, 유지관리, 통신, 보안 측면에서의 요구조건을 식별한 Requirements of AMI version 1.0을 2009년에 발표하였다.

3. 스마트 그리드 보안을 위한 기술개발

스마트 그리드 보안을 위해서는 먼저, 스마트 그리드 보안 아키텍처 정립이 최우선이다. 미국과 EU는 현재의 전력망을 실시간 · 양방향의 다양한 서비스가 가능한 스마트 그리드로 진화시키기 위해서 **[그림 4]**와 같이 Domain, Actor, Use Case, Interface 등을 정의하고, 이를 위한 Requirement를 도출하는 스마트 그리드 아키텍처와 스마트 그리드 보안 아키텍처를 거의 동시에 정립하였다. 이는 스마트 그리드 아키텍처와 스마트 그리드 보안 아키텍처는 서로 불가분의 밀접한 관계가 있고 일단 보안이 취약한 스마트 그리드 서비스와 이를 위한 아키텍처가 고정되면 종단간 보안이 되도록 수정하는 것이 어려울 수도 있기 때문이다.

스마트 그리드의 보안 아키텍처가 명확하게 정립되기 위해서는 **[그림 5]**와 같이 스마트 그리드 서비스와 이에 대한 Actor간의 Interface가 도출되어야 한다. 스마트 그리드 기기의 Computing Power가 크지 않기 때문에 모든 서비스의 과정마다 보안을 적용하는 것은 현실적으로 불가능하다. 서비스와 인터페이스에 따라 별도의 보안 수준이 적용되어야 할 것이다.

스마트 그리드 기기에 적합한 암호 · 인증 기술이 또한 개발되어야 한다. Computing Power가 작은 스마트 그리드 기기에 적합한 암호기술이 개발되어야 하고 기



[그림 5] 스마트그리드의 개념적인 레퍼런스 다이어그램 (출처 : NIST, 2009)

기 인증이 가능한 인증 체계도 개발되어야 할 것이다.

현재 스마트 그리드 보안 관련 법률이 준비 중에 있다. 스마트 그리드가 활성화되기 위해서는 보안이 필수적임에도 다양한 이해 당사자간 보안에 대한 부정적이고 낮은 인식으로 많은 걸림돌이 예상된다.

선진국들이 국가 안보 차원과 국제 스마트 그리드 시장을 선점하기 위해서 기술개발과 표준화를 서두르고 있는 상황에서 이해 당사자간 현명한 대처가 필요한 시점이다. KEA