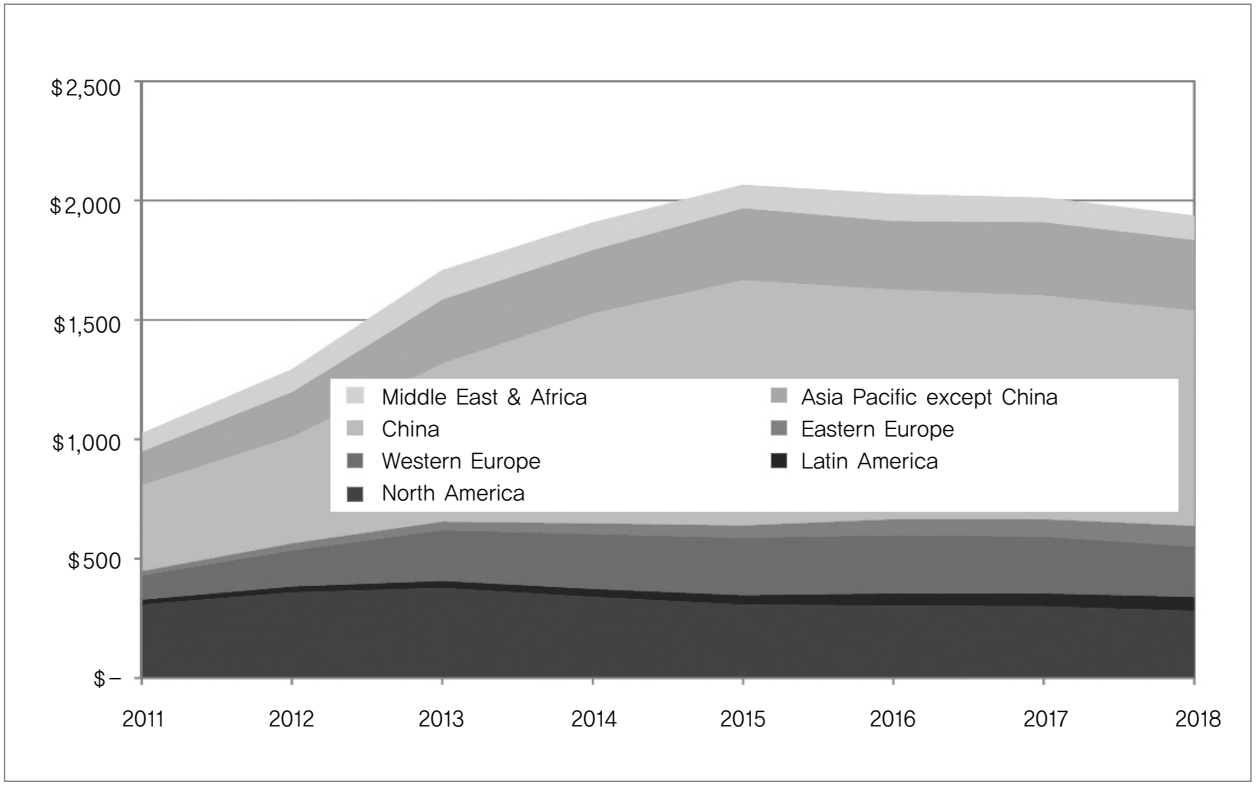
스마트그리드 보안관제 정보체계 구축 동향

김 충 효
한전 전력연구원 선임연구원

1. 개 요

스마트그리드는 '전력망에 정보통신기술을 적용하여 전기의 공급자와 사용자가 실시간으로 정보를 교환하는 등의 방법을 통하여 전기를 공급함으로써 에너지 이용 효율을 극대화하는 전력망' 이라고 관련법(지능형전력망의 구축 및 이용촉진에 관한 법률 제2조)에서 정의하고 있다. DOE, NERC 등 국외의 권위 있는 기관이 규정한 공통의



[그림 1] 스마트그리드 시장규모
(출처: Pike Research, 'Smart Grid Cyber Security 2010, pp. 4)

정의도 '통신 기술 및 정보를 활용하여 공급업체에서 소비자까지 최적으로 송전 및 배전하여 에너지 효율을 향상시키는 체계' 로써 우리와 크게 다르지 않다. 상기 정의를 잘 살펴보면 스마트그리드란 특정한 장치, 소프트웨어, 시스템 등 정적인 개념이 아니라, 기존 기술이 변화하고 새로운 기술이 개발될 때마다 지속적으로 바뀌어 가는 동적인 개념으로 이해되어야 할 것이다.

2. 현 황

대부분 사람들은 LED TV, 스마트 폰으로 각인된 매력적인 정보통신기술이 전력망에 적용되었으니, 뭔가 새로운 기능과 이점이 생겨날 것이라는 희망을 가질 것이다. 정보통신기술은 우리나라의 주력 수출상품이니 전력망을 통한 외화수입도 늘어날 것이고, 더 나아가 정전도 줄어들고 전력공급 상황도 나아질 것이라는 생각을 하는 사람도 있을 것이다.

이처럼 스마트그리드는 전 세계 에너지 효율을 극대화하여 전력분야의 기술을 획기적으로 발전시킬 만병통치약처럼 보일 수 있다. 전송효율을 향상시켜 경제적이며, 자가 복원능력을 보유하여 신뢰성이 향상되고, 실시간 요금체계 적용으로 에너지 절약에도 도움을 줄 수 있다. 이러한 발전은 전력망에 구축된 신기술 및 새로운 차원의 상호연결성은 물론 다양한 기관 간 협력 및 대량의 데이터 분석에 의존한다.

그러나 모든 신기술과 더 쉬워진 에너지 데이터 및 장치 이용으로 인해 악용될 수 있는 새로운 공격요소가 나타

나게 되었다. 보안 담당자들은 신기술, 상호연결성, 데이터 공유 등 새로운 기술과 관련된 환경의 개선은 그에 버금가는 새로운 위험들을 생산한다는 것을 인식할 것이다. 또한, 완전하게 보안성이 보장되는 애플리케이션, 네트워크 등의 환경은 존재하지 않기 때문에 보안 위험에 대한 대비를 스마트그리드 설계단계부터 운영단계까지 고려해야 하며, 이와 관련된 보안 시장 규모는 스마트그리드 시장과 함께 급속히 증가하고 있다.

스마트그리드에 관한 중요한 목표 중 하나가 보안향상[1]이었는데, 보안이 특정한 기능임을 뜻하지 않는다. 보안은 스마트그리드 전반에 통합적으로 적용되어야 효과를 발휘하는데, 주요한 요구사항은 가용성(Availability), 무결성(Integrity), 기밀성(Confidentiality) 순으로 정의할 수 있다.

가용성 보장은 스마트그리드 보안에서 가장 중요한 사안이다. 일순간 감시 및 제어권의 박탈은 전력시스템 전체의 무질서를 초래할 수 있기 때문에, 의도적인 공격이든 우연한 환경적 요인에 의한 공격이든 모든 유형의 DoS[2]를 방지해야 한다. DoS 감시 및 대응에 필요한 정보수집 뿐 아니라, 시스템 및 네트워크 이중화 관리도 가용성 보장의 영역에 포함된다.

데이터 분석은 스마트그리드에서 주된 역할을 하며, 데이터의 정확성이나 무결성은 안정적 운영의 핵심 요소이다. 특히, 전력시스템 운영을 위한 제어명령은 데이터가 훼손되지 않도록 보장되어야 한다. 예를 들면, 부하조절을 위하여 특정 선로를 차단하는 제어명령이 의도하지 않은 다른 선로를 차단한다던가, 소비자의 과금정보가 변형되어 전력소비 통계가 잘못 산출될 경우, 전력망 전체에 그 영향을 미칠 수 있다. 현재 전력망의 시스템 관리를 위한 제어명령은 암호는 물론 무결성에 대한 보장없이 전송되기 때문에, 의도적인 공격 또는 우연한 환경적 요인에 의한 변형의 가능성이 상존한다.

전력회사는 스마트그리드를 통하여 실시간 사용통계 및 전력 가격정보를 소비자에게 제공하고, 소비자의 에너지 사용습관을 바꾸어 이용효율을 높이고자 한다. 이때, 소비자의 전력사용 데이터를 포함한 사적 정보는 암호를 통하여 기밀성을 제공하여야 한다.

대개 금융시장이나 업무망 내의 정보는 정보유출 방지를 위한 기밀성이 가장 중요시 되나, 스마트그리드 환경에서는 정전 방지 또는 확산 억제를 위하여 특정한 시간(수 초~수 분)내에 적절한 제어명령이 도달해야 하기 때문에 보안운영에 있어서 가용성이 가장 우선시 된다.[3]

스마트그리드 보안은 일반적인 IT 시스템의 보안과 그 파급효과 면에서 상당한 차이가 있는데, 정전 발생 시 전력시스템 자체 복구시간보다 사회 · 경제적인 복구시간이 상당하므로 간접적인 피해규모가 훨씬 크다.

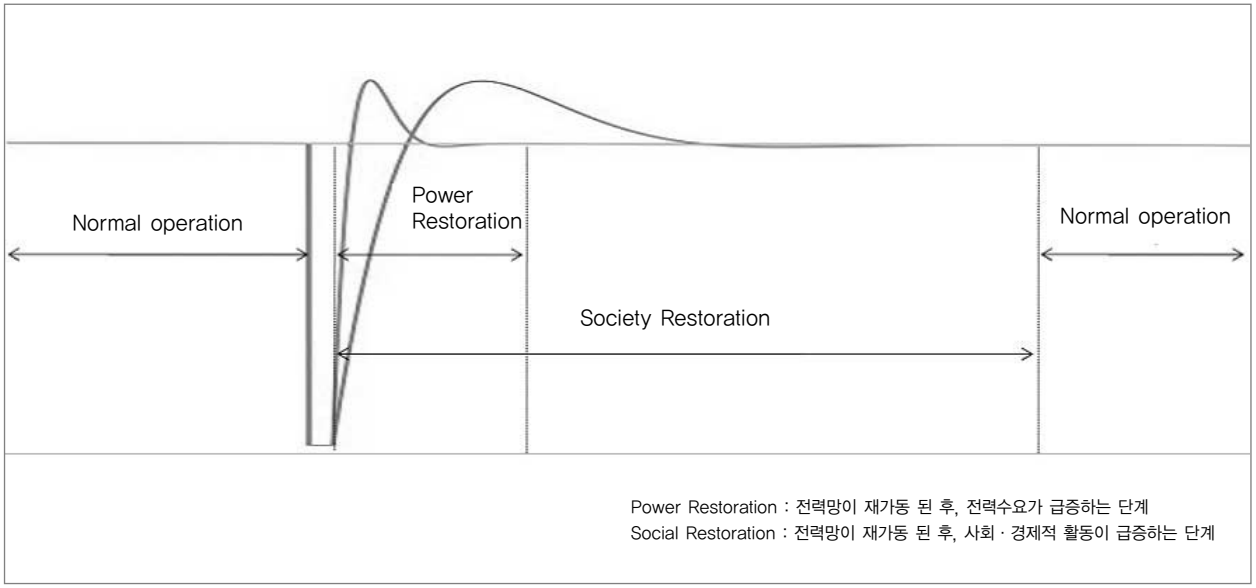
물론 정전의 범위와 시간에 따라 다르겠지만, 대부분 기반시설이 전력을 동력원으로 삼고 있기 때문이다.

---

1) NISTIR 7628, 'Guidelines for Smart Grid Cyber Security Vol. 1', August 2010, pp. viii

2) Denial of Service; 네트워크 상으로 대량의 접속 또는 요청을 유발해 정상적인 시스템 작동을 방해하는 사이버 공격

3) Pike Research, 'Smart Grid Cyber Security', August 2011, pp.20



[그림 2] 정전 후, 전력시스템 및 사회 · 경제적 복구단계 비교
(출처: Viking project, final dissemination workshop, '11.11.30, Rome)

따라서 일반적인 IT 시스템과 다른 요구사항, 대규모 파급효과 등을 고려할 때 별도의 보안체계가 구축되어야 할 필요가 있다.

International Electrotechnical Commission(IEC)에서는 전력 시스템 운영을 위한 네트워크와 시스템 관리(NSM; Network and System Management) 데이터 객체 모델을 정의한다. 이 모델은 Technical Committee 57[4]에 정의한 분야에 적용되며, IEC 62351[5] part 7에 기술규격(TS; Technical Specifications)으로 명시된다. NSM 데이터 객체는 네트워크와 시스템의 건전성을 감시하고, 가능한 보안 침입을 탐지하며, 정보인프라의 성능과 신뢰성을 관리하는데 그 목적을 둔다.

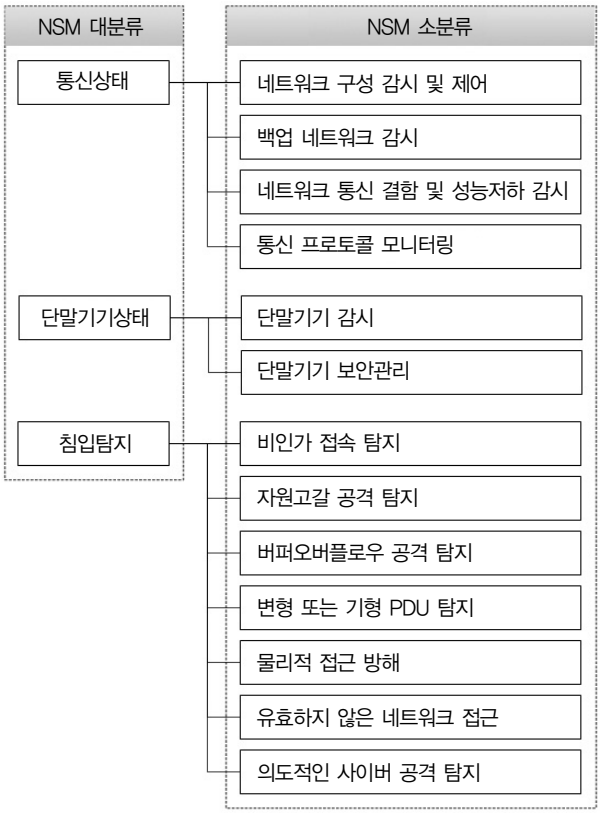
스마트그리드는 10개의 논리적 아키텍처로 구성[6] 되어 있는데, 관련표준이 구체화되고 상용화가 진행된 5개 분야(Grid operation, Distribution, Generation, Transmission, Renewables)는 IEC TC57 표준화 범위에 적용 가능하므로, NSM을 통한 보안적용이 가능하다.

NSM은 크게 3개 대분류, 13개 중분류, 136개 소분류(데이터 객체)로 구성된다. NSM을 보안관제의 주요 데이터로 활용하기 위해서는 모니터링, 탐지, 분석, 대응 및 사후처리/보고서 작성의 보안관제 4단계와 통합되어 적용되어야 한다. 보안관제 각 단계별로 해당 NSM 정보를 분류하면 다음과 같다.

4) Power Systems management and associated information exchange(전력시스템 관리 및 관련 정보교환)
5) Data and Communication Security
6) 스마트그리드 논리 아키텍처[스마트그리드 보안체계 연구 결과('10.12~'12.11)]: Grid operation, Distribution, Generation, Transmission, Renewables, 3rd party service, Electricity service, Market, Customer, Transportation

모니터링

NSM에서는 네트워크와 시스템 감시를 위한 객체들을 지원한다. 위치, 물리적 연결, 타 네트워크 장비와 논리적 상호연결 등을 포함하는 네트워크 설정모델은 표준 영역을 벗어난다. 표준 내에 NSM 데이터 객체는 네트워크 장비가 정보를 전송할 때, 네트워크 내에서 위치와 역할이 이해될 수 있도록 적절한 네트워크 모델이 있다는 가정 하에 정의된다.



NSM 대분류 및 중분류

네트워크 모니터링은 네트워크 구성, 가용성 보장을 위한 백업 네트워크의 상태, 통신 결함 및 성능저하 상태, 프로토콜 감시 등으로 구성되어 있고, 시스템 모니터링은 애플리케이션 상태, 연결 및 상태 정보, 백업장비 상태 및 비인가 된 접속 시도 등을 감시한다. 감시결과는 미리 설정된 값과 비교 · 분석을 통하여 미리 설정된 수신자에게 경고(alarm)로 알리는데, 이는 SNMP의 Trap과 유사한 시스템이다.

모든 보안관제의 시작은 감시와 이상 정보 통지이기 때문에, NSM도 모니터링의 목적을 충실히 달성하기 위하여 중분류 13개 중 5개를 모니터링에 할당하고 있다.

탐 지

침입탐지는 모니터링 결과를 기초로, 발생되고 있는 공격 이벤트의 유효성 판단을 시행한다. NSM은 대부분 미리 설정된 값 또는 메커니즘을 통하여 침입을 탐지해 내는데, 비인가된 접속, 자원고갈 공격(DoS), 버퍼 오버플로우 공격, 변형 PDU, 물리적 접근방해, 유효하지 않은 네트워크 접근, 의도적인 사이버 공격 등에 대한 탐지 기능을 지원한다.

특히, 스마트그리드의 가장 중요한 보안 요구사항인 가용성 보장을 위하여 DoS 공격에 대한 탐지는 대량의 NSM 정보를 활용하고 있다. IEC TC57 내의 네트워크 구성은 수 십개로 제한되어 있기 때문에, 수 천개 이상의 SYN Flooding공격을 대응하는 일반적인 IDS설정과는 달라야 한다. 네트워크 상에 허가된 연결 수 및 실제 연결 수, 동시 접속 수, CPU 로드, 메모리 사용 등 일반적 정보 뿐 아니라 배터리 변화수준 까지 감안하여 공격 탐지에 활용한다.

분 석

모니터링과 탐지를 통해서 발생한 이벤트나 경고는 실제 공격과 구분하는 이벤트 분석과 탐지되지 않은 공격에 대한 사후 로그분석으로 분류될 수 있다.

전력설비의 특성을 반영하지 못한 기존 IPS나 IDS가 공격을 정확히 판단하지 못하는 부분은 이벤트 분석

결과를 NSM에 반영해야 한다. 지속적인 피드백을 통하여 NSM 경고(alarm) 설정 메커니즘의 신뢰도를 향상시켜야 하기 때문이다.

보안관제시스템이 모든 보안 사고를 사전에 방지할 수는 없다. 사후에 공격으로 판단된 경우, 서버점검이나 로그분석을 통하여 전문 CERT[7]의 지원으로 NSM 및 대응체계를 보완하는 피드백 절차가 있어야 한다.

대응, 사후처리 및 보고서 작성

이벤트 분석으로 실제공격이라고 판단될 경우, 공격 IP를 차단하고 미리 계획된 조치사항을 이행해 나간다. 사후 공격으로 판단된 경우, 로그분석을 통하여 어떤 경로로 침입하였는지, 어떤 프로세스가 저장되어 실행 중인지 파악해야 한다.

사후처리는 이벤트나 로그분석을 통한 결과를 NSM 설정치와 시그니처에 반영하고, 보고서 발행 및 조치결과 교육을 통하여 보안담당자의 대응능력을 향상시킨다.

3. 전 망

스마트그리드 보안관제 연구는 필요성이나 중요성에 비하여 현실적 구현방법에 대한 진척이 느린 편이다. 보안관련 표준(IEC 62351) 역시 보안 및 인증을 위한 키관리, 접근제어 등 제정 중인 부분이 많아 증가하는 사이버 위협대응에 부족하다는 우려가 많다. 대안으로 제시된 NSM도 추상적인 데이터 객체로서 구현방법이나 활용성에 대한 구체적인 방안이 없다. 다만, SNMP[8]의 MIB[9]와 같은 형태로써 표준이나 제작사의 응용방법에 따라 확장성이 무한한 규격이기 때문에, 스마트그리드 도입으로 보안관제 시스템 구축이 절실한 유틸리티에서 적극적으로 활용할 필요가 있다. 스마트그리드의 보안 취약으로 발생할 수 있는 파급효과는 단순한 시스템 마비가 아님을 인식하고, 보안사고를 적극적으로 방지하고 대처하려는 각계의 노력이 필요하다. KEA

7) Computer Emergency Response Team(컴퓨터 비상 대응팀)

8) Simple Network Management Protocol; 네트워크 관리 및 네트워크 장치와 그들의 동작을 감시, 통할하는 프로토콜

9) Management Information Base; SNMP를 이용하여 관리할 수 있는 네트워크 관리 객체에 대한 형식적인 규격