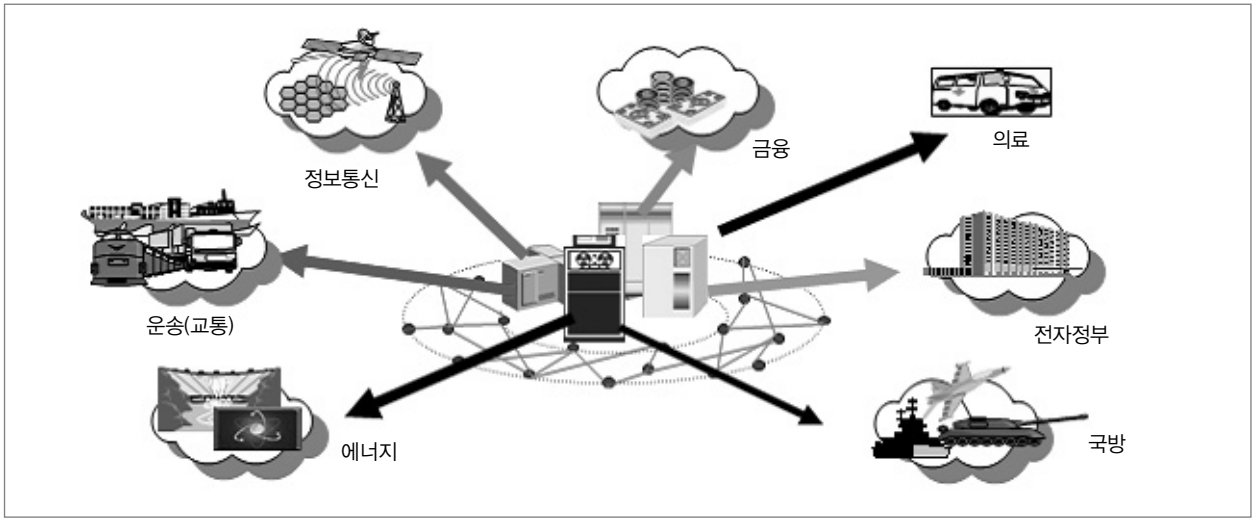
전력망에서의 전력통신과 보안 기술

백 종 목
한전 전력연구원 책임연구원

1. 개 요

저탄소 녹색성장과 신성장 동력창출을 향한 범국가적인 스마트그리드 아젠다에 발맞추어 양방향 통신 인프라 기반의 전력망은 IT기술과의 융합으로 지능화되고 표준화된 프로토콜기반의 개방형 망으로 진화가 전망된다.

전력망에 분산전원이나 전기차 충전인프라 등과 같은 기능별로 분화된 다양한 영역과 연계되고, 이해관계가 얽힌 복수의 사업자가 개입될 때 전기가 흐르는 전력 시스템을 중심으로 물리적인 토폴로지상의 구성은 물론,



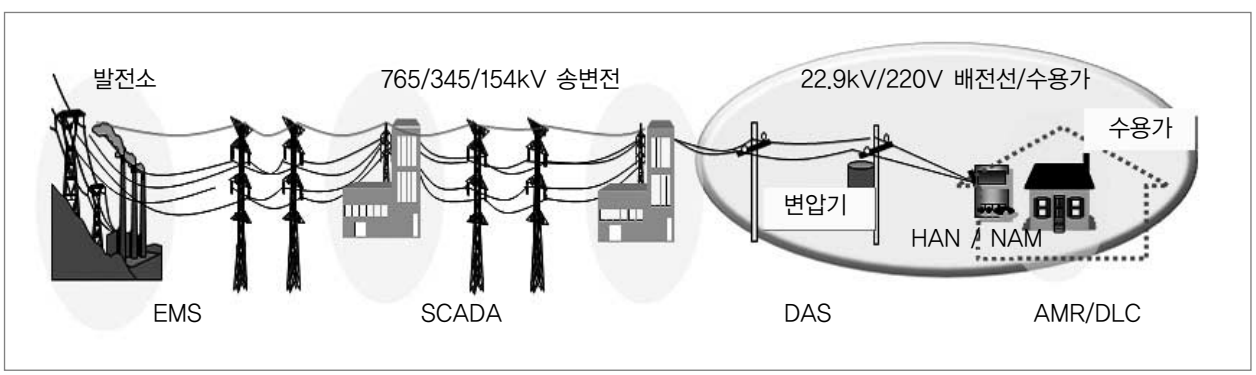
주요 정보통신 기반 시설

논리적으로 복잡한 형태를 가지면서 신뢰성과 기밀성이 요구되는 통신 네트워크의 구성이 필요하게 된다.

더욱이 최근에 해킹기술의 발달과 기업의 무관심으로 발생하는 사이버 해킹사고(2011년 7월 싸이월드 3,500만 명 고객정보유출, 2011년 4월 소니 7,700만 명 고객정보 유출 및 25조 원 손해배상 소송 피소, 농협전산망 및 백업 시스템 파괴로 고객거래정보 손상, 현대캐피탈 175만 명 고객정보 유출 등)로 개인의 피해는 물론 해당기업의 신뢰도에 치명적인 피해를 안겨주었다. 특히 우리나라 주변의 중국과 북한 등 적성국가는 대규모의 해킹부대를 운영하고 있는 것으로 알려져 있고 전 세계적으로 국가 간의 사이버 전쟁이 이미 시작되었음을 보여주는 징후들이 많이 포착되고 있다.

사이버테러의 주요 목표물은 금융망, 댐, 발전소 등 주요 사회기간시설이며, 특히 전력망은 공장과 산업시설에 전기를 공급하는 핵심 인프라로써 사회불안을 노리는 사이버 테러의 주요한 표적이 될 것으로 전망된다.

전력제어망은 인터넷 망과는 분리되어 운영되고 있으나 스턱스넷과 같은 악성코드가 이동형 메모리를 통해 전파된 사례가 있고 농협의 금융망 해킹사례는 전산설비 유지보수 직원의 노트북을 통해 발생한 해킹사고로서 폐쇄된 네트워크 환경에서도 해킹위협으로부터 자유



계층구조 전력망에서의 전력자동화시스템 구성

롭지 못한 단적인 사례이다.

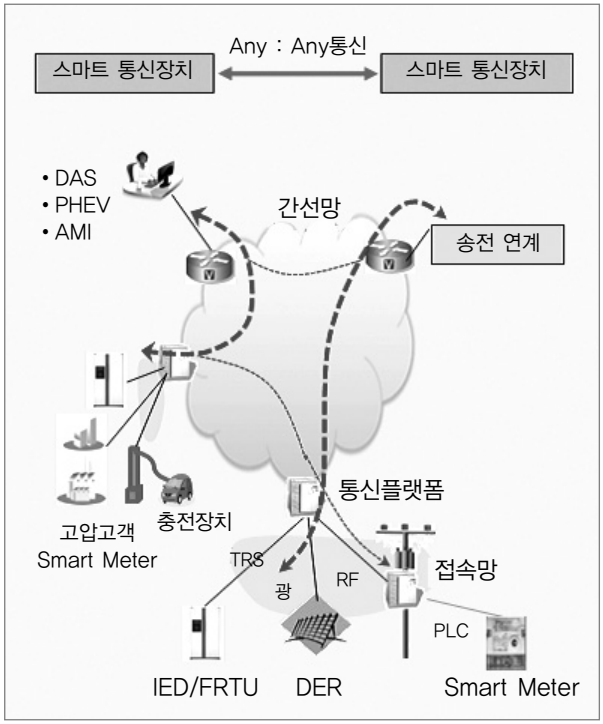
더욱이 전국적인 조직과 설비를 운영하는 전력회사의 경우는 한층 강화된 신중하고 철저한 보안대책 마련이 요구되고 있다. 본고에서는 전력망에서 필요한 통신망과 보안기술에 대해 살펴보고자 한다.

2. 동 향

가. 전력망에서의 전력통신시스템

전력회사에서 필요한 통신망으로서 전력설비를 감시 · 측정 · 제어하는데 필요한 전력제어 통신망(FA망으로 통칭)과 일반 행정 · 요금 · 수금 업무를 위한 업무자동화 통신망(OA망으로 통칭)으로 구분할 수 있다. FA망은 송변전설비 자동화를 위한 SCADA망과 배전설비 자동화를 위한 DAS망 그리고 검침업무 자동화를 위한 AMR망으로 구분된다. 한편, 전력시스템은 계통구조상 계층구조로 되어 있으며, 발전소에서 생산된 전기는 송전선로를 거쳐 인근 변전소에서 배전용 전압으로 변환되어 가정에 공급된다.

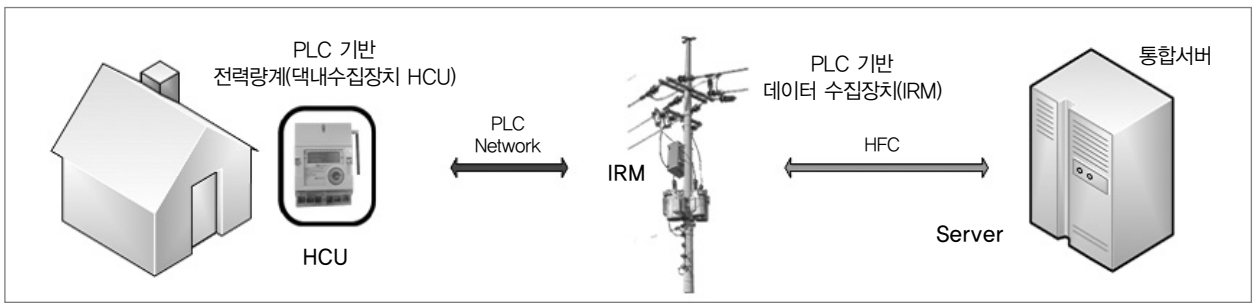
전기가 직접적으로 흐르는 송전선, 변압기, 모선, 차단기 등과 같은 현장의 전력기기를 원격지에서 감시제어하기 위해 전력제어 통신망이 중간에 개입된다. 특히 무인



스마트그리드에서 통신망 개념

변전소의 확대 및 배전센터의 광역화를 위해서는 필연적으로 신뢰성 있는 통신망 구성이 요구된다.

전력수급조절과 전국전력 계통을 운영하는 급전소 EMS[1]시스템, 지역급전소에서 주요계통 운전정보를 제공하며 지역 전력계통을 운영하는 지역급전소 SCADA[2], 무인변전소를 원방 운전하는 급전분소 SCADA, 변전소



전력선통신 기반의 저압원격검침 구성도

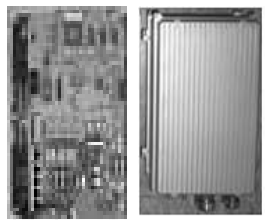
1) EMS : Energy Management System
2) RCC SCADA : Regional Control Center Supervisory Control And Data Acquisition

전력선통신 칩

Wall-Plug모뎀

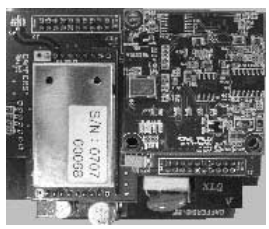
댁내집속장치

광대역 커플러

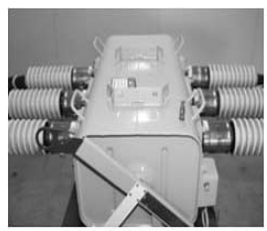


데이터집중장치

비접촉식코어



계량기탑재형 댁내수집장치



커플러내장형 개폐기

커플러내장형 변압기

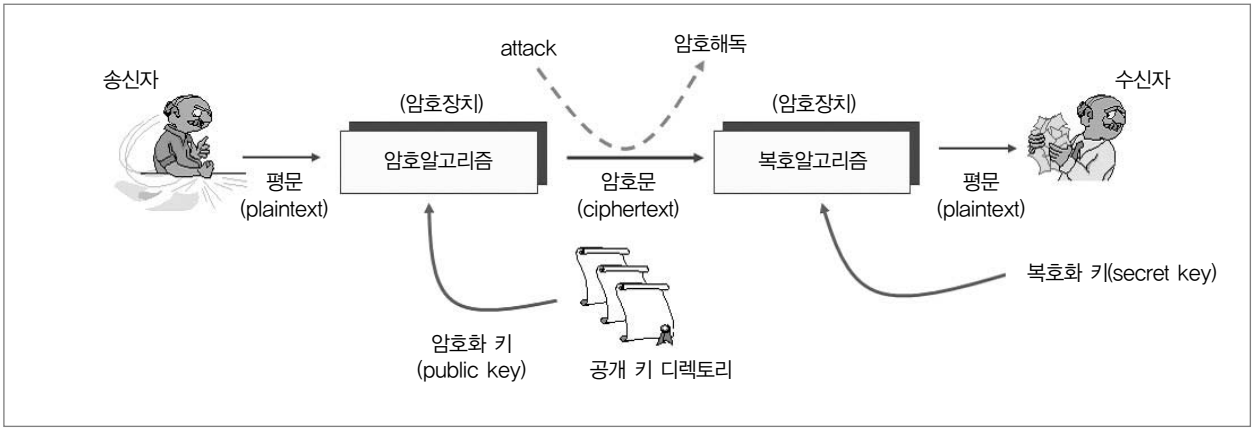
전력선 통신용 장치

에서 변압기 · 차단기 등 전력기기를 직접 측정 · 감시 · 제어하는 원격소장치가 있다. 이와 함께 지역단위의 전력 시스템을 계층화한 제어 시스템체계로 상하위 영역 간 양방향 전력통신망이 연계되어 있다. 송변전계통 전력기기를 원방 감시 제어하는 급전소와 급전분소 제어센터의 영역설비는 이더넷망으로 연결되어있으며, 변전소 원격소 장치와 이더넷망과 일반 통신회선으로 이중화 구성되어 있다. 스마트그리드 환경에서는 현장의 전력설비에서 발생하는 운영상태 및 운전정보를 실시간 양방향으로 기기 간 혹은 도메인 간 전송되어야 하므로 요구하는 전송대역폭 및 신뢰도 등에 따라 다양한 매체의 통신기술을 적용이 요청된다.

나. 전력선 통신기술

스마트그리드환경에서 지능형 계량기가 존재하는 Smart Place영역은 사용자에게 실시간 전기사용량과 전기요금 가격과 같은 전력정보를 양방향 통신망을 통하여 제공함으로써 에너지사용 효율을 극대화하는 RTP, TOU 서비스 제공의 근간이 되는 가장 복잡한 통신망 구간이다.

스마트그리드 정책에 따르면 2020년 까지 전기를 소비하는 1750만 가구에 100%의 스마트계량기를 보급할 계획이 수립되어 있으며, 전기계량기로부터 전력회사 간에 전국규모의 검침네트워크 인프라가 확대 구축 될 예정이다.



데이터의 암복호화 개념도

2005년 6월, 전 세계에서 가장 보급률이 높은 인프라인 전력공급망에 통신신호를 실어서 전송할 수 있는 전력선 통신 기술이 정부지원 하에 전력IT 중대형 전략과제로 5년간 연구가 추진되었고, 상용화 수준으로 개발되었다.

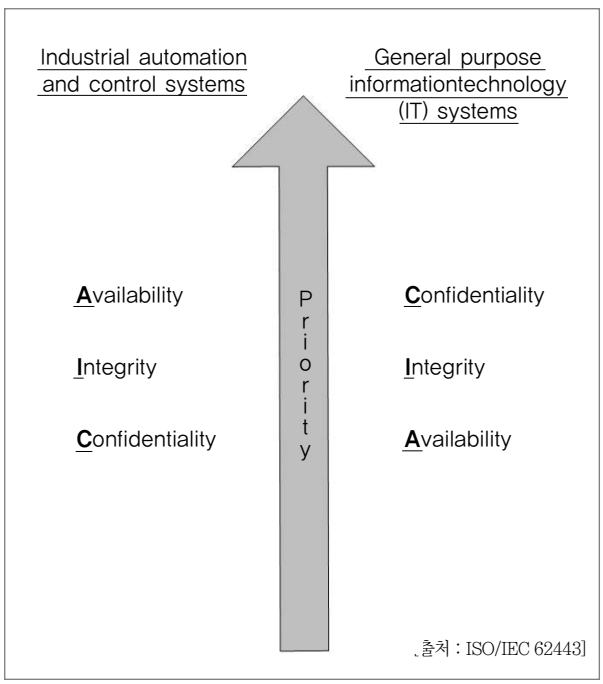
현재 개발된 전력선통신 기술은 2006년에 국가표준 KS X 4600-1규격이 제정되었고, 2009년 ISO/IEC 12139-1의 국제규격으로도 채택되어 국제적으로 한국 전력선 통신기술의 우수성을 인정받았다.

전력선에 전송하기 위한 통신신호를 생성하는 전력선 통신 변복조 장치, 전력선에 통신신호를 삽입하기 위한 신호결합장치, 신호가 분산되거나 접지로 분산되는 것을 방지하는 블로킹 필터, 저압가구에서 수집된 검침데이터를 많게는 100여 호에 가구씩 집속하여 간선망으로 전달하는 데이터집중장치, 댁내에서 수도와 가스계량기와 무선으로 검침데이터를 모아서 전력선 원격검침 인프라에 실어주는 댁내 데이터 집속장치와 같은 디바이스가 개발되었다. 한전에서는 저압 원격검침망의 인프라로 활용하여 2010년 현재 55만호를 구축하였으며 75만가구 보급을 추진 중에 있다.

다. 전력망 보안 기술

우리나라의 2009년 인터넷 보급률은 OECD국가 중 4위이며, 최근 UN공공행정부문 평가에서 1, 2위를 차지하는 등 인터넷 강국의 면모를 보여주고 있다.

특히 표준화된 공개프로토콜의 개방형 망은 전 세계 네트워크를 하나로 묶었으며, 이를 통한 수평적 정보의 흐름은 기존 사회적인 통념을 변화시키고 지식사회를 앞당기는 기반이 되고 있다.



제어와 IT시스템 간 보안 우선순위 비교

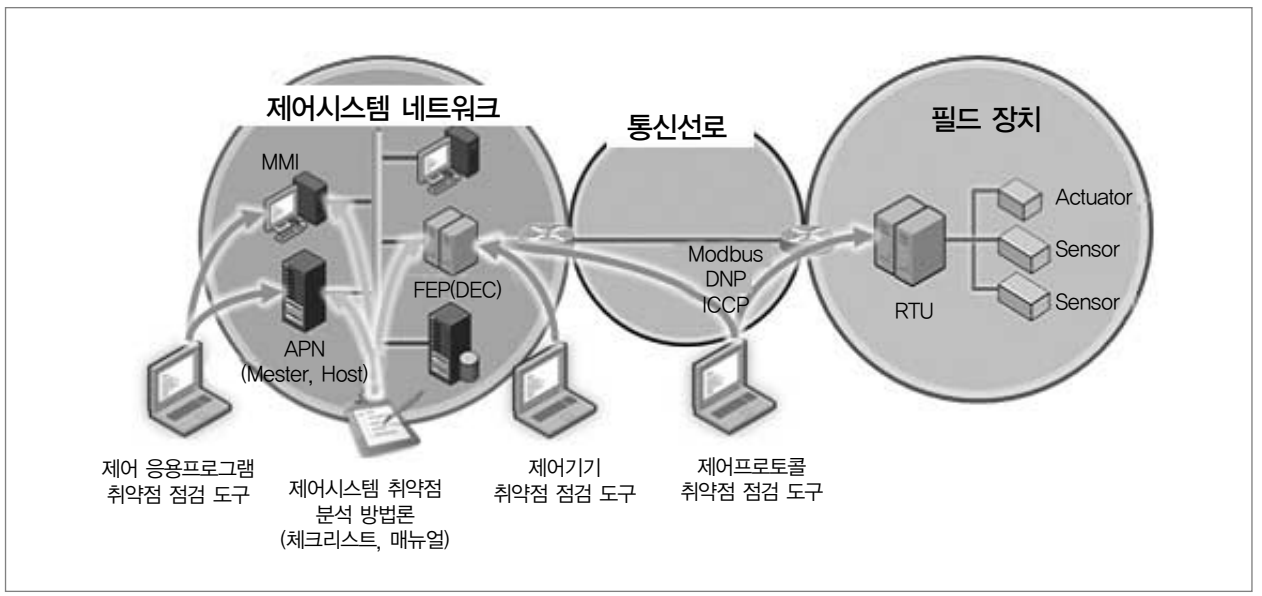
ISO/IEC TC57 WG15 표준화작업

IEC 62351	Definition
Part1	Introduction and Overview
Part2	Glossary of terms
Part3	Profiles Including TCP/IP
Part4	Profiles Including MMS
Part5	Security for IEC 60870-5 and derivates
Part6	Security for IEC 61850
Part7	Network and System Management (NSM) data object models

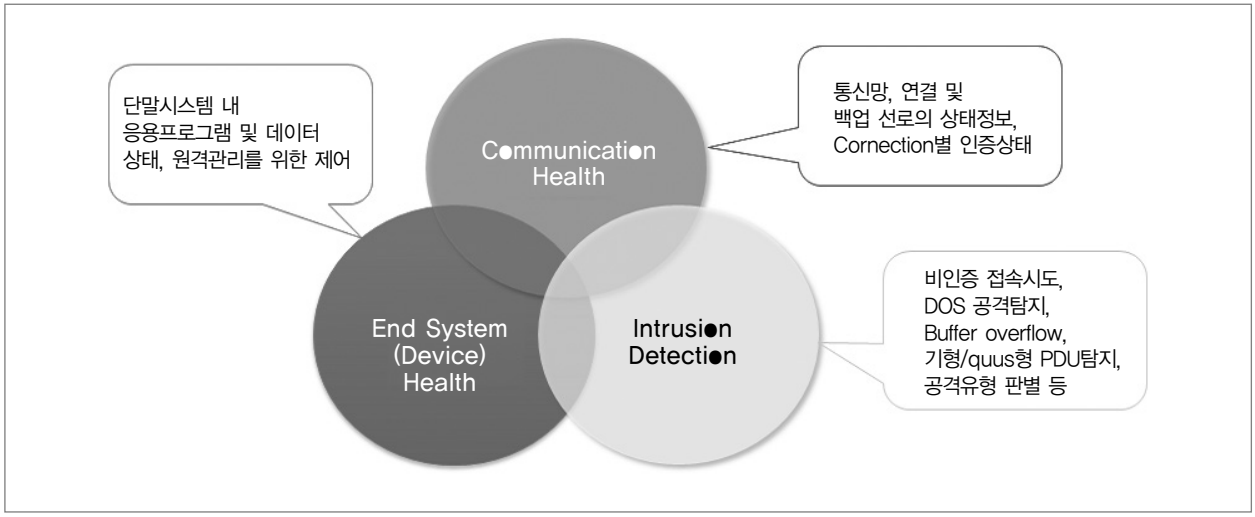
전력분야에서도 설비의 지능화와 함께 IT기술의 융합은 정보통신의 편의성과 뛰어난 확장성을 제공하지만 통신기술 고유의 취약점을 고스란히 내포하기 때문에 외부로부터의 침해나 사이버해킹으로 인한 위험은 더욱 많이 노출되게 되었다. 일반적인 IT망에서 금융거래나 인터넷 쇼핑몰 상품구입과 같은 행위를 보장하기 위해 인터넷망에 적합한 보안기술이 적용되어 왔으며, 대부분의 일반인은 IT분야에서 개발된 보안기술을 그대로 사용하면 되지 않느냐는 생각을 가지고 있지만 전력시스템은 IT시스템과는 사뭇 다른 환경과 보안 요구사항을 가지고 있다.

첫째, IT환경에서 단말장치들은 개인용 컴퓨터나 ATM단말기와 같이 프로세서 능력이 뛰어난 기기로 구성되어 있으므로 복잡한 암호알고리즘 및 인증처리 절차를 수용할 수 있다. 하지만 전력망의 현장단말 기기들은 전력기기 고유의 기능발휘와 운영에 필요한 최소한의 프로세서와 임베디드 운영체계를 가지고 있어 소형 경량형 보안기술 적용이 필요하다.

둘째, IT망에서 단말기기는 금융서버나 쇼핑몰 서버에서 요청하는 정보를 대화형식으로 직접 입력을 통하여 이루어진다. 하지만 전력제어시스템에서는 현장설비 제어를 위한 신호 혹은 현장단말의 장애발생 트랩신호가 실시간 전송되어 허용된 시간내에 처리해야 하는 시간 제약을 가지므로 보안알고리즘 적용 시 시간제약 조건과 보안요구 수준을 동시에 만족할 수 있어야 한다.



제어시스템 취약성 분석기술 내용



IEC 62351-7 NSM data object Modelling 영역

셋째, 전력 제어센터와 현장기기 간에 주기적으로 전송되는 측정 또는 감시데이터나 현장계기에서 검침된 전기사용량 데이터는 해킹으로 인한 위변조 없이 무결성을 보장해야 하므로 메시지 인증과 기기의 자동인증이 적용되어야 한다.

ISO/IEC TC65 WG10 산업통신 네트워크 간 및 시스템 보안 표준을 따르면 제어망에서 보안전략 우선순위로 가용성 · 무결성 순으로 두고 있으며, IT망에서 가장 중요시하는 기밀성은 상대적으로 최하위로 순위를 제시하고 있다.

그리고 ISO/IEC TC57[3] WG15에 의해 전력시스템 관리 및 관련정보 교환에 필요한 데이터 및 통신보안에 관한 표준화[4]를 통하여 광범위한 전력분야의 보안방향을 제시하고 있다. 정보보호 기반법에 의해 주요 정보통신 기반시설로 분류되어 있는 SCADA시스템의 보안수준 향상을 위한 연구개발이 정부지원 연구과제로 2010년 6월 시작하여 3년간 진행되고 있다.

주요 연구 분야는 ▲전력제어망과 일반업무망 간에 물리적인 일방향 자료전달 기술 ▲제어망에서 통신프로토콜 · 기기 및 응용시스템의 취약성분석 기술 ▲해커나 외부의 침입으로 제어망의 이상 징후를 탐지 할 수 있는 이상 징후 탐지 기술 등이며, 국가보안기술 연구소와 공동연구를 시행하고 있다. 현재 급전(분)소와 변전소 원격장치 간에 평문으로 전송하는 통신구간의 명령어 등의 메시지는 보안장치를 통해 전송한다.

또한 연구개발 성과물을 현장에 투입하기 전에 검증 및 시험을 위한 테스트베드 구축이 진행 중이다.

IEC TC57에서는 전력시스템관리 및 관련 데이터 교환을 위한 표준을 개발하고 있으며, WG10 · 17 · 18에서는 수력 · 분산전원분야를 포함하여 변전소 내 통신과

3) Electric Power System Management and associated information exchange
4) ISO/IEC 62351-1 ~ 8

데이터취득을 위한 표준 IEC61850[5]을 제공한다.

그리고 WG15에서는 IEC61850표준을 통하여 데이터 및 통신보안을 제공하고 있으며, 특히 Part7[6] NSM에서는 보안에 대한 요구사항과 데이터 객체를 Communication Health · End System Health · Intrusion Detection System으로 분류하여 제시하고 있어 보안관제를 위한 보안 객체정보의 방향을 제시하고 있다.

또한 WG13의 IEC61970에서 제시하는 공통정보모델을 기반으로 한 4세대 SCADA의 구현도 2012년 풍동변전소를 시작으로 구축될 전망이므로 이에 대한 보안관제 기술 개발이 시급한 상황이다.

3. 전 망

전력산업은 생산 · 변환 · 전송 · 소비에 이르기까지 지정학적으로 전국 규모의 방대한 전력망이 운영되고 소비에 필요한 전력량만큼 실시간으로 발전해야 하는 전기의 특성상 전력자동화를 위한 신뢰성 있는 전력통신망의 중요성은 아무리 강조해도 지나침이 없을 것이다. 전력을 공급하는 전력망이 국토의 동맥이라면 이와 병행하는 전력통신망은 신경망과도 같아 전력설비의 가용성을 보장하기 위해 매순간 동작하여야 한다.

전력망의 선진화와 더불어 IT기술의 융합은 전력망으로 하여금 확장성과 편의성을 확대시키지만 통신 특성 고유의 취약성을 물려받게 되고 무인변전소 확대와 배전센터 광역화, 그리고 스마트그리드 환경 진화 등과 같은 환경변화에 따라 전력망이 해커나 테러의 위협에 노출될 우려가 높아질 전망이다.

이처럼 변화하는 전력산업의 발전에 능동적으로 대응하는 전력통신기술과 전력보안기술의 개발 적용은 첨단고도화되어 지속적으로 이루어져야 할 것이다. KEA

5) Communication networks and systems for utility automation
6) Network and System Management data object models