정 보 보 호 학 회 지
제24권 제5호, 2014. 10

사물인터넷(IoT) 기반 스마트 그리드 보안 특성 및 쟁점 분석

전 용 희*

요 약

산업제어시스템과 SCADA(Supervisory Control and Data Acquisition) 제어 시스템들이 기존의 고립적이고 폐쇄적인 시스템에서 점차 개방적이고 표준화된 시스템으로 전환되고 있으며, IT 망과의 통합이 이루어지고 있다. 따라서 주요 국가 정보 인프라에 대한 사이버 위협 및 공격에 대한 우려가 증대되고 있다. 산업제어시스템의 정보보호 기술은 일반적인 IT 정보보호 기술과는 특성상 여러 가지 차이점이 존재한다. 국내에서의 산업제어시스템 정보보호 기술에 대한 연구는 아직 미약한 수준이다. 본 논문에서는 국가 주요 정보하부구조를 구성하고 있는 산업제어시스템 중에서 사물인터넷(IoT) 기반 스마트 그리드 시스템의 보안 특성에 대하여 분석하고 보안 쟁점 및 고려사항을 제시하고자 한다.

Ⅰ. 서 론

산업제어시스템(ICS: Industrial Control System)이란 SCADA(Supervisory Control And Data Acquisition) 시스템, DCS(Distributed Control System), PLC (Programmable Logic Controllers), PCS(Process Control System) 등을 포함하는 산업 부문 및 주요 하부구조에서 자주 사용되는 여러 가지 형태의 제어 시스템을 포함하는 일반적인 용어이다. 이 중에서 SCADA 시스템은 중앙 데이터 획득 및 감시 제어를 사용하여 분산된 장치를 제어하기 위하여 일반적으로 사용되며, 스마트 그리드와 같은 전력망의 기반 시스템이 된다 [1-3].

초기에는 ICS가 특별한 하드웨어와 소프트웨어를 사용하여 독점적인(폐쇄적인) 제어 프로토콜을 수행하는 고립 시스템이었기 때문에 전통적인 IT 시스템과는 상당히 구별이 되었다. 근래에 와서, IP(Internet Protocol) 장치가 독점적인 솔루션들을 대체하고 있어, 사이버 보안 취약성 및 사고의 가능성을 증대시키고 있다. 그러나 ICS의 보안 특성은 기존 IT 시스템 보안과는 큰 차이가 존재한다. 예를 들어, 일반적으로 기존 IT 시스템의 3대 보안 목표는 기밀성, 무결성, 가용성(CIA: Confidentiality, Integrity, Availability)의 순서를 따르나, ICS에서는 그 순서가 AIC로 바뀐다. 그러므로 ICS 환경에 적합한 새로운 정보보호 솔루션이 필요하다고 할 수 있다[4-7].

스마트 그리드(Smart Grid)는 사물인터넷(IoT: Internet of Things)의 대표적인 응용 중에서 가장 대규모 IoT 네트워크의 하나로 볼 수 있다. 스마트 그리드는 여러 종류의 유무선 통신 인프라 외에 수많은 스마트 객체, 스마트미터, 센서와 액추에이터 등을 포함할 것이다. ITU-T Y.2060[8]에 의하면 사물인터넷의 정의는 다음과 같다. “기존 및 새로운 상호운용적 정보통신기술을 기반으로 (물리적 및 가상) 사물을 서로 연결함으로써 진보된 서비스를 가능하게 하는, 정보 사회의 글로벌 하부구조”.

[8]에서는 또한 IoT는 식별(identification), 데이터 포획(data capture), 처리 및 통신 능력을 통하여, 모든 종류의 응용들에 대한 서비스를 제공하기 위하여 사물들을 이용하며, 이를 위하여 보안과 프라이버시 요구사항이 충족되어야 함을 기술하고 있다. 여기서 말하는 사물(things)은 물리적 세계(물리적 사물) 혹은 정보 세계(가상 사물)의 객체를 의미하며, 통신망 안에서 식별되고 통합될 수 있다.

본 논문에서는 ICS 중에서 스마트 그리드의 정보보호를 위한 전반적인 개요에 대하여 다루고자 한다. 특

* 대구가톨릭대학교 IT공학부(yhjeon@cu.ac.kr)

히, IoT 기반 스마트 그리드를 대상으로 한 보안 특성을 분석하고 여러 가지 쟁점과 고려사항을 살펴보고자 한다.

국내에서는 2013년 미래창조과학부를 중심으로 인터넷 신산업 육성을 위한 주요 추진 과제로 IoT 서비스 확산을 위한 사물인터넷 기반의 신규 서비스 발굴 및 연구 개발 지원, 시험 환경 인프라 구축 확대 등을 추진하고 있다. IoT 서비스는 스마트 그리드와 같은 국가 전력망, 의료 및 보건 분야, 교육 및 교통 분야와 같은 여러 가지 산업의 응용분야에 적용될 것으로 예상되기 때문에. 이런 서비스의 활성화를 위하여 다양하고 복잡한 보안 문제가 해결되어야 한다[9-11]. IoT 서비스를 위한 보안 시스템을 구축하기 위하여 IoT 환경에서의 보안 위협 분석을 수행하는 것이 필수적인 과정이다. 또한 보안 위협으로 인한 공격 가능성, 보안 공격에 대응하기 위한 보안 요구사항 등이 분석되고 그 대책이 수립되어야 한다.

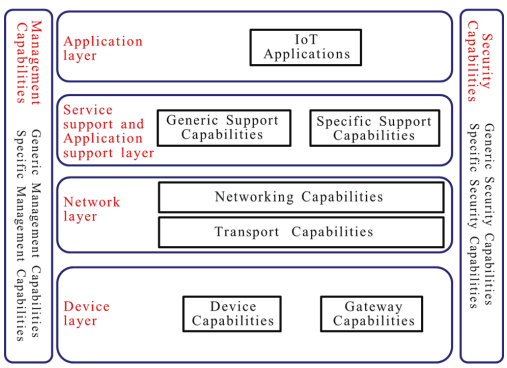
Ⅱ. 사물인터넷과 스마트 그리드

2.1. 사물인터넷(IoT)

그림 1은 IoT 참조 모델을 보여준다[8].

모델은 4계층으로 구성되며, 관리 및 보안 능력이 4 계층과 연관된다. 각 계층에 대한 설명은 아래와 같다[8].

- 응용계층: IoT 응용들을 포함한다.
- 서비스 지원 및 응용 지원 계층: 이 계층은 데이터 처리 혹은 데이터 저장과 같은 일반적 지원 능력과 다양한 응용들의 요구사항에 적합한 특정 능력을 제공하기 위한 특정 지원 능력으로 구성된다.



〔그림 1〕 ITU-T의 IoT 참조 모델[8]

- 네트워크 계층: 이 계층은 접근 및 전송 자원 제어 기능, 이동성 관리 혹은 인증, 권한부여 및 계정과 같은 네트워크 연결성 관련 제어 기능을 제공하는 네트워킹 능력과, IoT 서비스와 IoT 관련 제어 및 관리 정보의 전송을 위한 연결성을 제공하는 전송 능력으로 구성된다.
- 장치 계층: 이 계층은 통신망과의 직접적이고 간접적인 상호작용, 애드 혹 네트워킹 및 에너지를 절약하기 위한 sleeping과 wake-up 능력 등을 포함하는 장치 능력을 포함한다. 그리고 CAN(controller area network) 버스, 지그비, 블루투스 혹은 Wifi 같은 다른 종류의 유무선 기술을 통한 연결된 장치를 지원하는 능력과 공중 교환 전화망(PSTN), 2G 혹은 3G 망, LTE, 이더넷 혹은 DSL과 같은 여러 가지 기술을 통한 통신 능력을 지원한다. 또한 지그비와 3G 사이의 변환과 같은 프로토콜 변환 능력도 포함한다.

보안 능력은 일반적 보안 능력과 특정 보안 능력으로 분류된다. 각 계층에서의 일반적 보안 능력은 아래와 같다.

- 응용 계층: 권한부여, 인증, 응용 데이터 기밀성과 무결성 보호, 프라이버시 보호, 보안 감사와 앤티 바이러스,
- 네트워크 계층: 권한부여, 인증, 사용자 데이터 및 신호 데이터 기밀성, 신호 무결성 보호,
- 장치 계층: 인증, 권한부여, 장치 무결성 검증, 접근 제어, 데이터 기밀성과 무결성 보호.

특정 보안 능력은 응용에 특정적인 요구사항과 밀접하게 연관된다.

IoT 환경에서 객체들이 IPv6, UDP/TCP, HTTP 등과 같은 인터넷-기반 프로토콜을 사용하여 인터넷을 통한 접근과 통신이 이루어진다. 가장 자원-제약적인 장치를 위하여, IETF는 IEEE 802.15.4 표준과 일치하는 다음과 같은 여러 프로토콜을 제안하였다[12]: 6LowPAN (IPv6 over Low Power Wireless Personal Area Networks), RPL(Routing Protocol for Low-Power and Lossy Networks), CoAP(Constrained Application Protocol). 또한 non-IP 스택 프로토콜로써 Zigbee, Z-웨이브 등을 통한 인터넷 연결이 이루어 질 것이다.

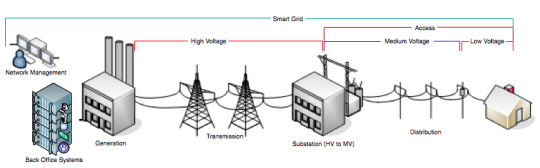
2.2. 스마트 그리드

그림 2는 ITU-T의 스마트 그리드 일반적 모델을 보여준다. 스마트 그리드는 공급자로부터 소비자까지 전력을 공급하는데 있어, 에너지를 절약하고, 비용을 절감하고, 신뢰성과 투명성을 제고하기 위하여 양방향 디지털 통신망을 사용한다[13,14].

통신망은 아래와 같은 요소로 이루어진다.

- WAN(Wide Area Networks): 코어 네트워크/백본과 지역적인 MAN(Metropolitan Area Network)으로 이루어진다. 이 통신망은 SCADA/EMS, 고전압 전송선을 위한 보호 계전기, 발전소 자동화 및 배전 피더 자동화와 같은 전력 회사 하부구조의 안전하고 신뢰적인 운영을 위하여 필요하다.
- 유틸리티 LAN: 전력회사 운영과 기업 LAN들로 구성되며, 유무선 통신망을 통하여 WAN에 연결된다.
- Backhaul: WAN과 last mile 네트워크를 연결하는 통신망이다. 고객의 스마트 그리드 검침 데이터, 변전소 자동화 중요 파라미터 데이터 등을 모아서 전송한다.
- Last mile: 전력 분배 시스템 위에 있는 양방향 유무선 통신망이다. NAN(Neighborhood Area Network) 혹은 AMI(Advanced Metering Infrastructure)라고도 불린다.
- 고객 댁내(Customer Premise): HAN(Home Area Network), BAN(Business/building Area Network) 혹은 IAN(Industrial Area Network) 등으로 구성된다.

스마트 그리드 통신망은 단일 통신망이 아닌, BPL(Broadband over Power Line), WiFi, WiMax, 3G 셀룰라, TDMA/CDMA, VSAT(Very Small Aperture Terminal) 위성과 같은 여러 형태의 무선망 및 고속 인터넷 백본망, 전력선(PLC: Power Line Carrier) 통신, RFID(Radio Frequency IDentification) 통신 같은 통합된 통신 형태가 될 것이다.



〔그림 2〕 스마트 그리드 통신망의 일반 구조

2.3. IoT 기반 스마트 그리드

사물인터넷 기술은 새로운 정보 처리 및 획득 기술로, 지능형 교통망, 환경 감시 및 의료 분야 등에 포괄적으로 사용될 것이다. 그 중에서도 사물인터넷은 스마트 그리드의 개발을 촉진하기 위한 중요한 기술적 수단이 된다[15]. 사물인터넷 기술의 사용은 정보통신망과 전력 시스템의 인프라 자원을 효과적으로 통합하여 주고, 전력 시스템 정보의 수준을 증가시키고 기존 전력 시스템 인프라의 사용 효율성을 개선할 수 있다. 스마트 그리드에서 IoT 기술의 사용으로 발전, 송전, 변전, 배전, 전기사용 및 기타 전력 그리드의 다른 측면에 대한 기술적 지원이 표 1과 같이 효과적으로 제공될 수 있다[15].

〔표 1〕 스마트 그리드에서 사물 인터넷의 응용 분야

구분	대표적 응용
발전	댐 감시, 태양광 패널의 감시, 발전기 감시, 풍력 시스템
송전	스마트 그리드 송전선 감시 및 동적 수용(dynamic capacity), 송전선과 송전탑 및 장비의 상시 보호 플랫폼 구축
변전	송전, 변전 및 배전 지능적 감시 시스템, 지능적 변전소 보조 관리 감시
배전	배전 현장 운영 감독, 지능적 전력 옥외 설비 및 통합 절도-방지 경고 시스템
전기 사용	지능적 정보 수집, 그린 룸, 전기차 충전, 전기 서비스 네트워크 관리, 지능적 전기 서비스 시스템

Ⅲ. 보안 특성 분석

미국의 국가 하부구조 보호 계획(NIPP: National Infrastructure Protection Plan)에 의하면 사이버 보안은 다음과 같이 정의된다[13]:

“기밀성, 무결성 및 가용성을 보증하기 위하여 전자정보 및 통신 시스템과 서비스(그리고 그 속에 포함된 정보)에 대한 손상, 권한이 없는 사용 및 남용을 방지하고, 필요한 경우, 복구까지를 포함 한다”.

스마트 그리드에 대한 위험 요소는 다음과 같다[13]:

- 복잡한 그리드에 따른 취약성이 발생할 수 있고, 잠재적인 공격 노출 및 비고의적 에러를 증가시킬 수 있다.
- 수많은 네트워크가 서로 연결됨에 따라 통상적인

취약성이 도입될 수 있다.

- 악성 소프트웨어 유입의 가능성이 증대됨에 따라, 통신 붕괴에 대한 취약성 및 서비스 거부(DoS: Denial of Service) 공격이나 소프트웨어 및 시스템 무결성이 침해될 수 있다.
- 잠재적인 공격을 위한 진입점과 경로의 수가 증가한다.
- 고객의 비밀성을 포함하여 데이터 기밀성의 침해가 가능하다.

미국 DOE에서도 현대적인 그리드를 도입하는데 해결해야 할 기술적인 장벽 중에 보안 기술을 명시하고 있다. 특히 분산 에너지 자원 소유주, 독립 전력 생산자, 소비자의 수요 대응 및 자동화 검침 프로그램 등에 반드시 보안 기능이 구축되어야 하며, SCADA 및 보호 계전기 시스템의 보안이 보장되어야 함을 명시하고 있다.

스마트 그리드 보안 서비스가 방지하려고 하는 보안 사건의 몇 가지 예는 다음과 같다[13]:

- 스마트 그리드의 안전성 공격
- 그리드의 물리적 재산 손상
- 서비스 거부(DoS)나 붕괴 공격
- 프라이버시 위반
- 장비 제어 하이재킹
- 물리적이고 논리적인 손상
- 운용자가 시스템을 붕괴하도록 하는 치명적 동작을 취하도록 상황 인식 전복
- 자동화 시스템이 허위 경보에 대하여 자원을 허비하도록 원인 제공
- 서비스 하이재킹
- 스마트 그리드 서비스나 지원 통신 메커니즘을 통한 종단 주거 사용자나 산업 네트워크 공격

표 2는 일반적인 정보 시스템과 스마트 그리드 시스템의 보안 특성의 차이점을 요약하여 보여준다[2,3,13].

이와 같이 스마트 그리드 시스템에 대한 위협은 여러 가지 자연적 소스와 같은 다양한 소스로부터 발생할 수 있다. 따라서 자연적 위협뿐만 아니라 악의적인 위협에 대하여 보호하기 위하여, 방어 전략을 세울 필요가 있다. 다음은 스마트 그리드에 대하여 가능한 위협을 보여주는 목록이다[13,14]:

- 스파이웨어/멀웨어의 생성 및 배분 공격
- 좀비를 이용한 봇-넷(Bot-Net) 공격

〔표 2〕 정보 시스템과 스마트 그리드 시스템의 보안 특성 차이점

보안 특성	정보 시스템	스마트 그리드 시스템
앤티바이러스/모바일 코드	통상적 광범위한 사용	비통상적/효과적인 설치가 불가능
패치 응용	정기적 계획됨	드뭄, 비계획적 공급자 특정
변경 관리	정기적 계획됨	고도로 관리되고 복잡함
시간 민감 내용	일반적으로 지연 허용	지연 허용 안 됨
가용성	일반적으로 지연 허용	연속적 사용
보안 인식	개인 및 공공 부문에서 중간 정도	물리적 보안을 제외하고 열악
보안 시험/감사	좋은 보안 프로그램의 부분	정지에 대한 일시적 시험
물리 보안	안전	원격/무인 안전

- 스팸 메일 이용 공격
- 금전적인 이득을 위한 외부 공격
- 내부자 공격
- 피싱(Phishing)
- 기타 산업 스파이 활동 등.

표 3은 스마트 그리드의 응용별 보안 특성을 보여준다[13,14].

Ⅳ. 보안 쟁점과 고려사항

IoT 서비스는 스마트기기, 센서 등 다양한 단말 및 이기종 네트워크, 애플리케이션 등을 활용하기 때문에, 많은 보안 위협이 예상된다[10]. IoT 기반 스마트 그리드는 전통적인 전력 그리드에는 존재하지 않았던 새로운 보안 문제가 발생한다. 주요 보안 문제점은 다음과 같다[12]:

- 위장/신분 가장: 합법적인 사물의 신원을 사용하여 불법적으로 통신을 수행하는 공격이다. 예를 들어 공격자는 다른 스마트미터의 신분을 위장하여 전력 소비에 대한 비용을 지불하게 할 수 있다.
- 도청: IoT 환경에서의 객체 및 장치들은 공중 통신 인프라를 이용하여 통신하기 때문에, 교환되는 데이터에 대한 접근이 가능하다. 어떤 가정의 에너지 소비를 쉽게 도청할 수 있다.
- 데이터 손상: 시간대별 차등 요금이 적용되는 경

〔표 3〕 스마트 그리드의 응용별 보안 특성

응용	통신매체	프로토콜	가용성 (%)	보안 중요도
AMI	PLC, 무선, 광대역망	WiMAX, LTE, 802.15.4, 지그비	99-999.99	높음
전력수송	PLC, 무선	지그비, 802.15.4	99-99.99	비교적 높음
분산그리드관리	광섬유, 무선, 위성, 이동통신	DNP3, IEC 61850, WiMAX, LTE 802.15.4	99-99.999	높음
지역간 통신	전화회선	IP	99.999	높음
분산 에너지 자원 및 저장	광섬유, 무선, 마이크로웨이브, 위성	분산 그리드 관리와 같음	99-99.99	높음

우, 교환되는 전력 사용 데이터를 수정하여 전력 요금이 싼 시간으로 수정하는 공격이 가능하다. 결과적으로 이것은 전력 과소비를 가져와서 전력망의 과부하를 초래할 수 있다.

- 권한부여 및 접근 제어 문제: 스마트 미터 혹은 배전변전소 현장에 설치된 센서와 액추에이터와 같은 장치들이 원격으로 감시되고 구성될 수 있기 때문에, 공격자가 불법적인 접근 권한을 획득하여 조작함으로써, 변압기와 같은 물리적 자산을 손상시켜 정전을 유발할 수 있다.
- 프라이버시 문제: 주거용 가입자들에 대한 스마트 미터와 스마트 장치들의 에너지 소비가 사용자의 프라이버시를 침해할 수 있다. 예를 들어 전력 소비 패턴을 통하여 기상 및 취침 시간, 저녁 시간 등을 알 수 있고, 집에 사람이 있는지 없는지의 여부도 알게 된다.
- 침해 및 악성 코드: 스마트 그리드의 객체들이 물리적 혹은 원격으로 침해의 목표가 될 수 있다. 또한 객체들이 다른 운영체제를 수행함에 따른 다른 종류의 소프트웨어 감염 혹은 악성 코드의 목표가 될 수 있다. 더구나 센서와 같은 자원 제약적인 장치들을 가진 수많이 설치된 장치들이 보통 손상-저항(tamper-resistant) 능력이 없기 때문에 물리적으로 쉬운 침해 대상이 될 수 있다.
- 가용성 및 DoS 문제: IoT 환경에서 대부분의 장치들 상에서 IP 프로토콜이 실행 가능하기 때문에 가용성 및 DoS 공격의 대상이 될 수 있다.
- 공격: 스턱스넷(Stuxnet) 공격과 같은 사이버 공격이 변압기, 회선 차단기(circuit breaker), 스마트 미터, 케이블 등과 같은 물리적 자산을 위태롭게 할 수 있다.

IoT 기반 스마트 그리드의 보안을 위하여 다음과 같은 고려사항들이 제시되었다[12]:

- 확장성: 키 관리와 인증 같은 보안 솔루션에 대한 확장성이 고려되어야 한다.
- 이동성: 이동 장치와 객체들에 대하여 인증과 안전한 통신이 필요하다.
- 설치: 대규모로 넓게 설치된 객체 및 장치들에 대한 손상 시도가 탐지될 수 있어야 한다.
- 리거시(legacy) 시스템: 이미 설치된 보안 능력이 거의 없거나 전혀 없는 기존 시스템들과 IoT 기반 스마트 그리드의 통합이 큰 문제이다.
- 제한된 자원: 제한된 자원 문제로 공개키 암호화와 같은 보안 솔루션의 수용에 제한이 발생할 수 있다.
- 이질성: 스마트 그리드 상의 장치와 객체 자원 그리고 구현된 프로토콜과 통신 스택의 차이로 인하여 안전한 종단간 통신을 하는 것이 어려운 일이다.
- 상호운용성: TCP/IP 스택을 지원하지 않는 전통적 시스템과 장치 및 객체들이 게이트웨이 없이는 IP 기반 시스템과 통신이 불가능하다. 이것이 종단간 안전한 통신을 불가능하게 만든다.
- 부트스트래핑: 스마트 그리드 상의 수많은 장치 및 객체들을 암호 키, 암호 함수/알고리즘과 파라미터와 같은 초기 키 정보를 가지고 어떻게 효율적으로 부팅할 것인가?
- 신뢰 관리: 대규모 네트워크에서 다른 개체들에 의하여 소유되거나 관리되는 객체/장치들 사이의 신뢰관계를 구축하는 것이 도전과제이다.
- 지연/시간 제한: SCADA와 같은 시스템은 전류, 전압, 주파수 값의 변화와 같은 이벤트와 메시지에 대하여 실시간 대응이 필요한데, 이것은 공개키와 같은 시간-소비적 운용은 적합하지 않다.

IoT 기반 스마트 그리드를 위하여 고려되어야 할 주요 보안 서비스는 다음과 같다[12]:

- 인증: 스마트 그리드 내의 모든 통신 장치와 객체들의 신원을 점검 및 보증할 수 있는 능력이 있어야 한다. 예를 들어, 정확한 사용자에 대한 요금 청구를 위하여 스마트 미터가 인증되어야 한다.
- 데이터 무결성: 데이터가 불법적인 방법으로 변경되지 않도록 보증해야 한다.
- 기밀성: 저장 및 전송 데이터는 의도된 수신자에게만 접근이 가능하도록 해야 한다. 예를 들어, 종단 사용자의 에너지 소비는 운영자와 공급자에게만 알려져야 한다.
- 사용자 프라이버시: 사용자와 관련된 데이터는 명확한 승인 없이 획득이 불가능해야 하며, 의도된 목적으로만 사용되어야 한다.
- 권한부여와 접근 제어: 인증된 객체나 사람은 어떤 업무나 자원에 대한 접근이 허용되어야 함을 보장해야 한다.

특히 SCADA 제어 시스템은 인증, 권한부여, 무결성, 가용성과 부인봉쇄와 같은 주요 보안 서비스들을 지원하는 특징들이 필요하다[1].

Ⅴ. 맺음말

산업제어시스템(ICS)은 국가적인 주요 기반시설로 전기, 수도, 수송, 화학, 제지, 자동차, 석유 및 가스와 같은 광범위한 산업에 사용되고 있다. 초기에는 ICS가 특별한 하드웨어와 소프트웨어를 사용하여 독점적인 제어 프로토콜을 수행하는 고립 시스템이었기 때문에 전통적인 IT 시스템과는 상당히 구별이 되었다. 근래에 와서, MS 윈도우, Unix, TCP/IP와 같은 표준 기술 및 프로토콜로 전환되고 있고 IT 망과의 통합이 이루어지고 있어, 정보통신 인프라에 존재하는 사이버 보안 취약성 및 사고의 가능성이 산업제어시스템에도 그대로 재현될 가능성이 증대되고 있다.

스마트 그리드는 여러 종류의 유무선 통신 인프라 외에 수많은 스마트 객체, 스마트미터, 센서와 액추에이터 등을 포함할 것이다. 따라서 스마트 그리드의 효과적인 구축을 위하여 사물인터넷 기술의 사용이 필수적으로 요구된다.

본 논문에서는 ICS 시스템 중의 하나인 스마트 그리드의 보안 특성을 살펴보고, 주요 보안 쟁점 및 고려사항을 제시하였다. 향후 연구로써 보다 자세한 IoT 기반 스마트 그리드정보 보호 기술에 대하여 연구가 수행되어야 할 것이다. 이를 위하여 위협 요소에 대한 분석 및 모델링, 공격 가능성 분석, 요구사항 및 대응책 수립과 같은 보안 모델링에 대한 연구가 필요하다고 사료된다.

참 고 문 헌

[1] Mariana Hentea, “Improving Security for SCADA Systems”, Interdisciplinary Journal of Information, Knowledge, and Management, Vol. 3, pp.73-86, 2008.

[2] Arvid Kjell, Guide to Increased Security in Process Control Systems for Critical Societal Functions, The Swedish forum for information sharing concerning information security-SCADA and Process control systems(FIDI-SC), Swedish Emergency Management Agency, Oct. 2008.

[3] NIST(National Institute of Standards and Technology), U.S. Department of Commerce, Special Pub. 800-82, Final Public Draft, Guide to Industrial Control Systems (ICS) Security, Sep. 2008.

[4] 이철수, “산업제어시스템 정보보안 감리 프레임워크 연구”, 정보보호학회논문지, 제 18권 제 1호, pp.139-148, 한국정보보호학회, 2008년 2월.

[5] 전용희, “산업제어시스템 정보보호: 개요”, 한국정보보호학회 정보보호학회지, 제 19권 제 5호, pp. 52-59, 2009년 10월.

[6] 전용희, “산업제어시스템 보안을 위한 네트워크 설계 및 구조”, 한국정보보호학회 정보보호학회지, 제 19권 제 5호, pp.60-67, 2009년 10월.

[7] 윤정한, 김우년, 서정택 , “제어시스템 네트워크 보안기술 동향”, 한국정보보호학회 정보보호학회지, 제 22권 제 5호, pp.22-27, 2012년 8월.

[8] Recommendation ITU-T Y.2060, Overview of the Internet of things, June 2012.

[9] 서화정, 이동건, 최종석, 김호원, “IoT 보안 기술 동향”, 한국전자파학회지, 제 24권 제 4호, pp.27-35, 2013년 7월.

[10] 김동희, 윤석웅, 이용필, “IoT 서비스를 위한 보안”, 한국통신학회, 정보와 통신, pp.53-59, 2013년 8월.

[11] 김호원, “사물인터넷 환경에서의 보안/프라이버시 이슈”, TTA Journal Vol. 153, pp.35-39, 2014년 5/6월.

[12] Chakib BEKARA, “Security Issues and Challenges for the IoT-based Smart Grid”, Procedia Computer Science 34, pp.532-537, 2014.

[13] 전용희, “지능형 전력망(Smart Grid)과 정보보호”, 한국정보보호학회 정보보호학회지, 제 19권 제 4호, pp.65-71, 2009년 8월.

[14] 전용희, 장종수, “스마트 그리드 통신망의 보안 특성, 고려사항, 구조, 설계 원칙과 연구동향에 대한 고찰”, 한국정보보호학회 정보보호학회지, 제 22권 제 5호, pp.40-53, 2012년 8월.

[15] Liu Hua, Zhang Junguo, and Lin Fantao, “Internet of Things Technology and its Applications in Smart Grid”, TELKOMNIKA Indonesian Journal of Electrical Engineering, Vol.12, No.2, pp.940-946, Feb. 2014.

〈저자소개〉

전 용 희 (Yong-Hee Jeon)
종신회원

1971년 3월~1978년 2월 : 고려대학교 전기전자전파공학부, 학사
1985년 8월~1987년 8월 : 미국 플로리다 공대 대학원 컴퓨터공학과
1987년 8월~1992년 12월 : 미국 노스캐롤라이나주립 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월~1978년 11월 : 삼성중공업(주)
1978년 11월~1985년 7월 : 한국전력기술(주)
1979년 6월~1980년 6월 : 벨기에 벨가톰사 연수
1989년 1월~1989년 6월 : 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월~1992년 9월 : 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992년 10월~1994년 2월 : 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월~현재 : 대구가톨릭대학교 IT공학부 교수
2001년 3월~2003년 2월 : 대구가톨릭대학교 공과대학장
2004년 2월~2005년 2월 : 한국전자통신연구원 정보보호연구단 초빙연구원
2007년 1월~2007년 12월 : 한국정보보호학회 학회지 편집위원장
2008년 1월~현재 : 한국정보보호학회 부회장
<관심분야> 네트워크 보안, IoT보안, 보안 모델링