정 보 보 호 학 회 지
제 30 권 제5호, 2020. 10

전력제어분야 사이버 보안기술 개발동향

김 진 철*, 박 택 근*, 이 규 철*

요 약

최근 전력제어분야 사이버 보안에 대한 관심이 지속적으로 증가하면서 전력제어분야에 특화된 보안 표준화 논의를 지속적으로 진행 중이며, 국내외 보안기업에서 제어시스템 보안 솔루션을 출시하고 있다. 본 논문에서는 전력제어분야 보안기술 표준화 동향을 살펴보고, 스카다, 배전자동화시스템, AMI와 같은 전력제어시스템에 적용되는 사이버 보안기술 개발동향을 소개한다.

Ⅰ. 서 론

최근 제어시스템 취약점을 이용한 사이버 공격들은 갈수록 고도화·지능화되고 있는 추세이다. 대표적인 제어시스템 대상의 APT(Advanced Persistent Threat) 공격으로는 지난 2010년에 등장한 스턱스넷(Stuxnet)을 비롯하여 듀큐(Duqu), 플레임(Flame), 샤문(Shamoon) 등 다수의 제로데이 (zero-day) 취약점을 이용한 제어시스템 보안 위협 사례들이 있었다.

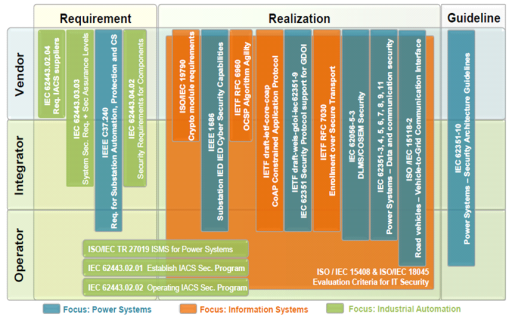
과거에는 전력분야 제어시스템 보안기술은 국내외적으로 주로 국가연구기관에서 테스트베드에서 연구단계로 실증을 수행한 수준이었지만, 최근 제어시스템 사이버보안에 대한 관심이 지속적으로 증가하면서 글로벌 보안기업과 신기술을 보유한 벤처기업에서 제어시스템 보안 솔루션을 출시하고 있으며, 시장조사 기관의 발표에 따르면, 글로벌 제어시스템 보안시장은 연평균성장률(CAGR) 6%의 높은 성장세로 2024년까지 140억 달러까지 성장할 것으로 예측하고 있다.[1]

본 논문에서는 전력제어분야 보안표준화 동향을 살펴보고, 스카다, 배전자동화시스템, AMI(Advanced Metering Infrastructure)와 같은 전력제어시스템에 적용되는 사이버 보안기술 개발 동향을 소개한다.

Ⅱ. 전력제어분야 보안기술 표준화 동향

전력제어분야 고유한 특성상 기존 정보시스템과 산업용 자동화 시스템의 보안 표준을 전력제어분야에 그대로 적용하는 것을 무리가 있기 때문에 전력제어분야 보안의 중요성이 높아지면서 IEC, IEEE, IETF 등 국제표준화 기구에서 전력제어분야에 특화된 보안 표준 제정을 위하여 지속적으로 표준화 논의가 진행 중에 있다. 그림 1과 같이 전력제어분야의 보안표준을 사용목적에 따라 보안 요구사항을 도출할 때 고려해야 할 표준, 실제 보안 시스템을 구현할 때 고려해야 할 표준, 보안적용 방안에 대한 가이드라인을 제공하는 표준으로 분류할 수 있으며, 보안표준 사용자에 따라 제조사(Vender), 사업자(Integrator), 운영자(Operator)에게 필요한 표준 등으로 분류할 수 있다.[2]

특히, IEC 62351 표준은 EMS(Energy Management System), 스카다(SCADA), 배전자동화 및 원격 제어시스템 등을 포함하는 전력시스템에서의 정보교환을 위한 표준으로 IEC의 TC57의 WG15에서 표준화를 수행하



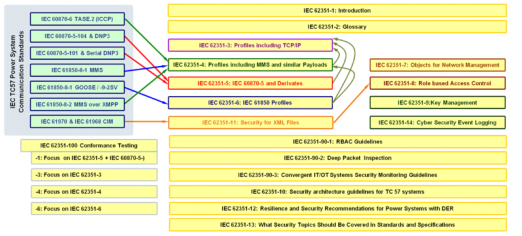
출처 : CEN-CENELEC -ETSI

〔그림 1〕 전력제어분야 보안표준

* 한전KDN(주) (부장, shine_1991@kdn.com / 차장, reply_1997@kdn.com / 처장, 52bright-plum@kdn.com)

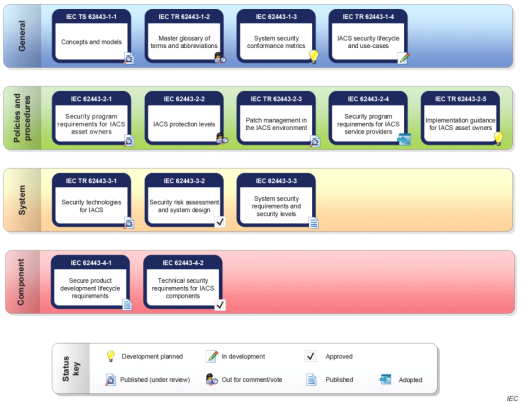
고 있다. TC57에서 표준화하여 전력계통에서 많이 사용되는 DNP, ICCP, MMS, GOOSE와 같은 프로토콜에 대한 보안적용 표준뿐만 아니라 보안관제, 접근제어, PKI, XML보안, DER(Distribution Energy Resource) 전력계통 연계, 전력계통 보안적용 가이드라인 등과 같이 전력계통의 패러다임의 변화에 따른 새로운 보안 표준을 추가적으로 진행하고 있다. 그림 2와 같이 IEC 62351 표준은 보안 이벤트 로그, 보안 모니터링 가이드라인 등에 대한 표준화가 진행 중이다.[3]

IEC 62443은 산업제어시스템 사이버보안을 견고하게 하기 위한 표준으로 미국 ISA 99 위원회에서 작성한 ISA 62443을 기반으로 작성되었으며, IEC TC65 WG10의 주관으로 관리되고 있다. 본 표준에서의 산업제어시스템은 스마트팩토리, 전력제어시스템, 생산제어시스템 등 전반적인 산업제어시스템을 대상으로 하며, 특정 대상을 구분하지 않는다. 또한, 하드웨어, 소프트웨어, 통신 네트워크, 사용자를 포함하는 산업제어시스템 보안 프로세스를 구축하는 것을 목표로 하고 있



출처 : NOZOMI

〔그림 2〕 IEC TC57의 IEC 62351 표준



출처 : IEC

〔그림 3〕 IEC TC65의 IEC 62443 표준

다.[4]

그림 3과 같이 IEC 62443은 용어, 개념 및 모델을 설명하는 일반(General)분야, 산업제어시스템을 보유하는 조직의 보안 정책 및 관리시스템 요구사항을 기술하는 정책 및 절차(Policy &Procedure) 분야, 산업제어시스템에 대한 보안 요구사항을 다루는 시스템(System) 분야, 산업제어시스템 구성요소를 다루는 업체에 대한 요구사항을 다루는 구성요소 (Component) 분야로 구성된다. 모두 4개의 분야로 나뉘어 있으며, 각 분야는 모듈 방식의 세부 사항으로 구성된다.

Ⅲ. 전력제어분야 보안 기술 개발동향

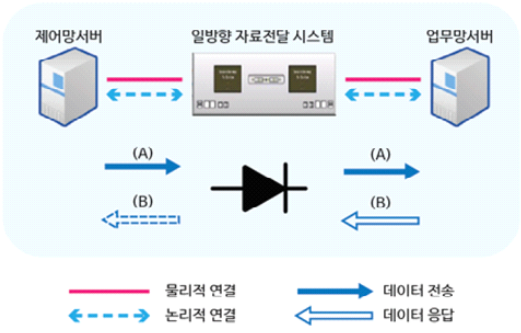
3.1. 스카다(SCADA) 보안

스카다(SCADA)에서는 국가 정보보안 기본지침과 전자제어시스템 보안가이드라인에 따라 물리적 일방향 자료전달 시스템, 이상징후 감시시스템, Secure DNP 통신시스템, HMI 인증 및 감시시스템 등의 보안솔루션이 연구개발되어 활용되고 있다.

국가 정보보안 기본지침 3장2절 제53조2에는 교통·에너지·원전 등 국가안보상 중요한 제어시스템을 운용할 경우 인터넷 및 일반 사무용 내부망과 분리·구축하도록 하고 있으며, 부득이하게 기관 인터넷망과 연동할 필요가 있는 경우 연동 구간에 일방향 전송장비와 같은 안전한 망연동 수단을 설치·운용하도록 하고 있다.[5]

물리적 일방향 자료전달 시스템은 전력 제어망과 업무망을 물리적으로 일방향으로만 연계하여 제어망에서 업무망으로 감시 · 상태정보를 단방향으로 전송하는 시스템이다. 이는 업무망에서 제어망으로 물리적인 연결 자체가 없기 때문에 악성코드나 해킹 침입경로를 원천적으로 제공하지 않아 제어망을 안전하게 보호할 수 있다. 물리적 일방향 자료전달 시스템은 OPC, PI, DB, FTP, TCP/UDP 등과 같은 기존 제어망과 제어망 외부 서비스에 대한 안정적이고 신뢰성 높은 일방향 자료전달이 가능해야 한다. 그림 4는 물리적 일방향 자료전달 시스템을 통한 제어망에서 내부 업무망으로 물리적 일방향 통신경로를 제공한 예시로써 SCADA뿐 만 아니라 발전소 제어망, DAS에 물리적 일방향 자료전달 기술이 적용되어 운영 중에 있다.[6]

Secure DNP 통신시스템은 IEC 62351-5에 따라 급



출처 : 한전KDN

〔그림 4〕 물리적 일방향 자료전달 시스템

전(분)소의 자료수집 처리장치(FEP, Front End Processor)와 현장 원격제어장치(RTU, Remote Terminal Unit)간의 시리얼 통신에 대한 메시지 인증 및 송수신 메시지에 암복호화 기능을 제공한다. Secure DNP 통신시스템은 기존에 구축된 SCADA시스템에 Add-in 형태로 추가된 암복호화 통신장비로 DNP 보안 마스터 통신장치 SSIO(Secure SIO)와 슬레이브 통신장치 BITW(Bumper In The Wire), DNP 보안 키관리시스템(KMS)로 구성하여 제어명령 및 감시정보의 위·변조를 방지하여 통신 데이터의 무결성을 제공한다.

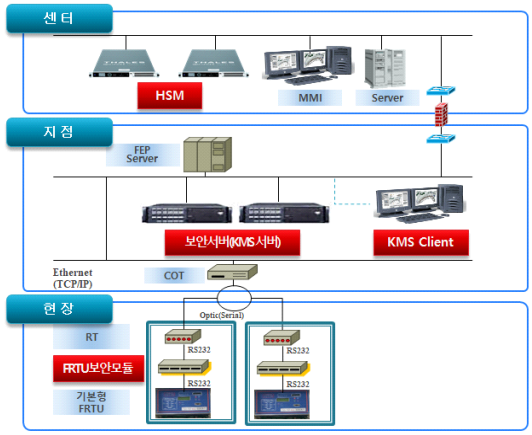
HMI 인증 및 감시시스템은 급전(분)소의 SCADA를 감시·제어를 할 수 있는 HMI시스템에 대하여 허가된 사용자를 인증하고, 권한에 따른 HMI시스템을 사용제한과 인증된 사용자가 작업한 행위에 대한 화면, 키입력, 명령어 등의 로그 기록, 이상 작업에 대한 추적 기능을 제공하는 접근제어 시스템이다. 허가된 사용자 인증은 패스워드, 등록된 스마트카드 인증과 추가 선택적인 지문과 같은 생체 인증 등 다양한 다중 인증을 통하여 접근제어 서비스를 제공한다.

출처 : 한전KDN

〔그림 5〕 Secure DNP 통신시스템

3.2. 배전자동화시스템(DAS) 보안

DAS 주장치와 현장 단말장치간의 통신에서 사용하는 DNP3 프로토콜은 자체 보안 기능이 부재하여 다양한 방법의 악의적인 공격으로 시스템 교란이 가능하다. 이러한 취약점은 FEP과 FRTU에서 송·수신되는 메시지를 암호화 및 인증으로 보완할 수 있다. 현재 시스템의 수정 없이 보안시스템을 구성하는 방안으로 그림 6과 같이 보안 서버와 보안모듈을 별도의 장치로 구성할 수 있다. 보안서버는 FEP과 FRTU에서 사용하는 DNP Standard Protocol 메시지가 송·수신 될 경우 Secure DNP3.0 Protocol과 IEC 62351-5를 이용하여 메시지에 대한 보안 및 메시지가 발생한 장비를 인증하여 악의적으로 발생하는 위협을 방지할 수 있다.



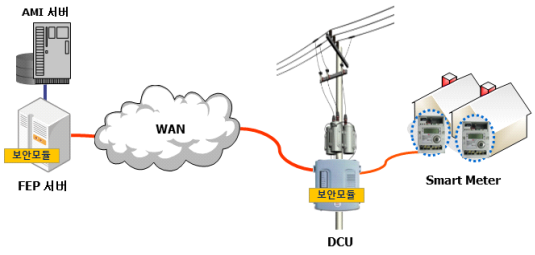
출처 : 한전KDN

〔그림 6〕 배전자동화시스템 보안

3.3. AMI 보안

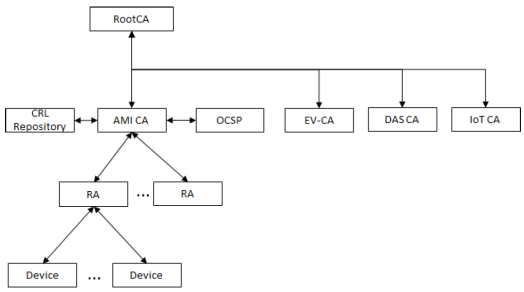
AMI에서는 AMI 기기 상호인증, 암호화 저장 및 암호화 통신을 수행한다. AMI에서 보안기술이 적용되는 대상 기기는 그림 7과 같이 수용가 측에 설치된 스마트미터, 변대주 (변압기가 설치된 전주)에 설치된 DCU(Data Concentration Unit), 검침센터에 설치된 FEP서버를 그 대상으로 하며, 각각의 대상에 보안 모듈을 적용하여 상호 간 인증, 암호화 저장 및 암호화통신을 수행한다.

AMI 기기의 상호인증을 위한 PKI 기반의 기기인증 시스템은, 최상위 인증서 발급 시스템(RootCA), 인증서 발급 시스템(CA), 인증서 등록 시스템(RA), 키관리 시스템(KMS), 실시간 유효성 검증시스템(OCSP)으로 구성된다.



출처 : 한전KDN

〔그림 7〕 AMI 보안



출처 : 한전KDN

〔그림 8〕 기기 인증서 발급 인증시스템

최상위 인증서 발급시스템(RootCA)의 개인키와 공개키는 HSM(Hardware Security Module)을 통해 생성된다. 또한 인증서에 대한 생성 및 암호화 필요시 HSM을 통한 전자서명과 암·복호화를 수행하며, 생성된 개인키와 공개키는 HSM 외부로 추출이 불가능해야 한다. 인증서 발급 시스템(CA)는 전력 기기의 용도별 인증서의 정책을 설정하여 인증서 용도에 맞는 인증서를 생성한다. 인증서의 정책 설정 내용은 RFC 5280 인증서 프로파일을 따른다. 생성되는 인증서는 HSM(Hardware Security Module)에 저장된 인증서 발급 시스템(CA)의 개인키를 통해 인증서에 전자서명을 수행하게 된다. 이때 생성되는 인증서의 전자서명 알고리즘은 저사양 기기를 고려한 ECDSA 전자서명 알고리즘을 사용하여, SHA-256 해쉬를 사용한다. 인증서 등록 시스템(RA)은 대량의 기기 인증서의 효율적인 운영관리를 위하여, 인증서 발급시스템(CA)으로부터 권한을 부여받은 관리자가 발급된 기기 인증서에 대한 운영관리가 가능하도록 구성한다. 실시간 유효성 검증 시스템(OCSP)은 주요 서버 기반의 서비스에 적용하여 실시간으로 상태 검증이 가능하도록 구성하며, 키 관리 시스템(KMS)은 생성되는 기기의 개인키 보호를 위해 개인키를 암호화하는 용도로 구성된다.

3.4. 이기종 프로토콜 연계 보안

전력망이 전력회사와 마이크로그리드, 신재생에너지, 분산형 전원, 전기자동차 충전 인프라와 같은 다양한 이해당사자 간에 연동되기 위해서는 이기종 프로토콜 연계가 필요하고 이에 대한 보안기술 적용이 필요하다. 이기종 전력제어 프로토콜 보안 연계는 이기종 프로토콜을 사용하는 전력제어 시스템 간에 국제 표준방식의 이기종 프로토콜 맵핑과 이기종 보안 프로토콜의 고속 처리 수행이 가능해야 한다.

이기종 프로토콜 보안 게이트웨이는 SCADA 시스템과 디지털 변전소의 IED간의 연계를 위해 국제표준인 IEEE 1815.1에 따라 DNP 프로토콜과 IEC 61850의 MMS 프로토콜의 맵핑을 수행한다. 또한, DNP 프로토콜 구간인 SCADA 시스템과 이기종 프로토콜 보안 게이트웨이 간에는 DNP SA(Secure Authentication) 표준에 따라 제어명령의 무결성을 확인하는 메시지 인증과 암복호화가 이루어지고, MMS 프로토콜 구간인 이기종 프로토콜 보안 게이트웨이와 디지털 변전소 IED 간에는 TLS(Transport Layer Security) 표준에 따라 PKI 인증서 기반으로 기기 간 상호인증, 암호화 방식 확정, 확정한 암호화 방식에 따른 데이터 암복호화가 이루어진다.[7]

Ⅳ. 결 론

최근 제어시스템 취약점을 이용한 사이버 공격들은 갈수록 고도화·지능화되면서, 전력제어분야 사이버 보안에 대한 관심이 지속적으로 증가하고 있다. 이에 따라 국내외 표준화 단체에서는 전력제어분야에 특화된 보안 표준화 논의를 지속적으로 진행 중이며, 시장조사기관에서는 글로벌 제어시스템 보안시장이 높은 성장세를 예측하고 있으며, 국내외 글로벌 보안기업과 신규 벤처회사에서는 제어시스템 보안 솔루션을 빠르게 출시하고 있다.

본 논문에서는 전력제어분야 보안표준화 동향을 살펴봄으로써, 전력제어 분야에 특화된 보안 표준화 동향을 분석하였다. 특히, IEC에서는 TC57과 TC65에서 전력제어 분야에 특화된 표준화 활동을 활발하게 전개하

고 있다. 초기에는 전력제어 분야 표준 프로토콜에 대한 인증 및 암복호화를 중심으로 진행이 되었으나 최근에는 전력제어 보안시스템 설치 및 운영, 적정성 시험, 로그 분석, 이상징후 탐지, 전력제어 보안 모니터링 등에 대한 표준화가 진행되고 있다.

또한, 본 논문에서는 스카다, 배전자동화시스템, AMI(Advanced Metering Infrastructure)와 같은 전력제어시스템에 적용되는 사이버 보안기술 개발 동향을 소개하였다. 전력제어시스템에 특화된 보안 솔루션은 아직 초기 단계로 표준 프로토콜을 사용하는 제어망 중심으로 적용되고 있지만, 제어시스템 제조사와 협력을 통하여 점차 확대될 것으로 예상된다.

참 고 문 헌

[1] Visiongain, Utilities Infrastructure Security Market Forecast(2014-2024), 2014.

[2] CEN-CENELEC-ETSI, Smart Energy Grid Coordination Group Cyber Security and Privacy, 2016.

[3] IEC TC57, Power Systems Management and Associated Information Exchange - Data and Communication Security - All Parts.

[4] IEC TC65, Security for Industrial Automation and Control Systems - All Parts.

[5] 국가정보원, 국가 정보보안 기본지침, 2020.

[6] 한전KDN, 전력ICT원론(Ver4.0), 2019.

[7] 김진철, “전력 분야 보안기술 동향”, *주간기술동향* 통권 1790호 pp. 2-14, 2017.

〈저 자 소 개〉

김 진 철 (Kim Jin Cheol)

종신회원

1995년 2월 : 광운대학교 전자통신공학과 졸업

1997년 2월 : 광운대학교 전자통신공학과 석사

2006년 8월 : 광운대학교 전자통신공학 박사

1996년 12월~현재 : 한전KDN 부장

<관심분야> 정보보호, 융합보안

박 택 근 (Park Teak Geun)

1997년~현재 : 한전KDN 차장

<관심분야> 정보보호, 융합보안

이 규 철 (Lee Kyu Cheol)

1994년~현재 : 한전KDN 처장

<관심분야> 정보보호, 융합보안