정 보 보 호 학 회 지
제25권 제5호, 2015. 10

한국형 계통운영시스템 간 보안을 고려한 ICCP/TASE.2 개발

박 성 완*, 김 진 철**, 김 상 태***, 이 승 원****

요 약

한국형 계통운영시스템인 전력거래소(KPX)의 EMS(Energy Management System)와 한국전력공사(이하 한전)의 급전소 SCADA시스템은 서로 ICCP(Inter-Control Center Protocol)를 통한 데이터 교환을 하고 있다. 현재의 ICCP는 데이터 교환에 있어서 보안 기능이 고려되어 있지 않기 때문에 본 논문에서는 안전하고 신뢰성 있는 계통운영시스템 간 데이터 교환을 위한 ICCP/TASE.2의 보안 통신 기능 개발을 소개하고자 한다.

Ⅰ. 서 론

현재의 전력 계통운영시스템으로 전력거래소의 EMS(Energy Management System)와 한전의 급전소 SCADA(Supervisory Control and Data Acquisition)이 WAN(Wide Area Network) 상에서 실시간 데이터처리와 데이터베이스 프로그램을 사용하여 많은 계통정보를 효과적으로 교환하고 있다.

두 계통운영시스템 간 실시간 데이터 교환은 1990년대 초 EPRI(Electric Power Research Institute)의 주도하에 UCA(Utility Communication Architecture) 프로젝트를 시작하여 물, 가스, 전기 등의 기반 산업에 대한 응용프로토콜 표준으로 제안된 ICCP(Inter- control Center Communication Protocol)[1]를 통하여 운영되고 있다.

기존의 3세대 SCADA와 EMS는 보안이 고려되지 않은 ICCP를 사용하여 데이터 교환을 하였으나, 최근 보안에 대한 요구사항이 급증하여, 차세대 시스템부터는 보안이 고려된 ICCP를 요구하고 있다. 한전은 2013년부터 차세대 SCADA 구축에 대한 준비를 하여 2015년 운영예정이고, 전력거래소는 2014년 10월부터 차세대 EMS 운영을 시작 하여, 보안이 고려된 ICCP 적용이 매우 중요한 시점이다. 현재 본 연구과제에서 개발된 보안모듈이 고려된 ICCP/TASE.2 결과물이 차세대 EMS에 적용되어 운용 중에 있다.

1.1. 한국형 계통운영시스템

한국형 계통운영시스템은 전력거래소의 EMS와 한전의 변전소 원방감시시스템(SCADA), 배전자동화시스템(Distribution Automation System, 이하 DAS)의 3계층 구조로 구분할 수 있으며 제어망 내에서 계통별 분산처리를 통한 데이터 수집 및 원격제어를 수행하고 있다[2]. EMS는 변전소 및 발전소의 유/무효 전력, 전압, 변압기 TAP 위치 등에 관한 아날로그(Analog) 데이터와 디지털(Digital) 신호인 차단기의 상태에 대한 데이터 수집 및 원격제어를 통한 경제급전, 자동발전제어, 수요예측, 급전계획, 적정 전력예비율 유지, 전력계통운용 등의 기능을 수행하고 있으며, SCADA 시스템은 송변전 계통설비의 정보를 수집 처리하고 감시, 제어하는 시스템으로 지선전력 계통운용, 송변전설비 운용, 관내 휴전계획 및 사고복구 등의 기능을 수행하고 있다. 그리고, 배전자동화시스템은 배전선로의 운전상태 감시 및 설비의 운전 조작을 원방에서 감시, 제어하는 시스템이다[2].

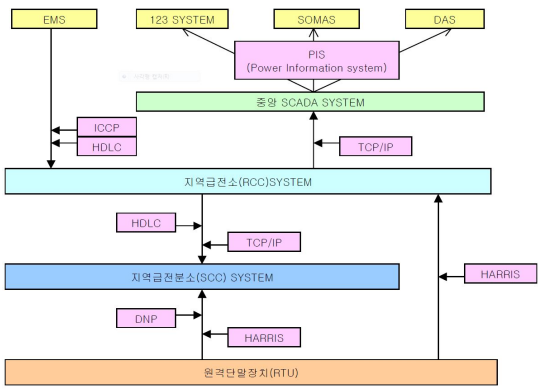
국내 전력계통은 발전-송전-변전-배전 등의 계통이

* 한전KDN(주) 전력IT연구원 (adonis@kdn.com)
** 한전KDN(주) 전력IT연구원 (kjc@kdn.com)
*** 한전KDN(주) 전력IT연구원 (jesteka@kdn.com)
**** 한전KDN(주) 전력IT연구원 (swlee@kdn.com)

서로 유기적으로 연결되어 있고, 상위 계통에 의한 조작정보는 하위 계통에 중요한 영향을 초래한다. 그러므로 각 계통간의 정보에 대한 연계는 반드시 필요하며 현재 전력거래소의 EMS와 한전의 SCADA는 ICCP를 통하여 연계되어 운용되고 있다. 그림 1은 전력 계통 계층별, 시스템간 연계 운용을 위한 사용 중인 프로토콜을 나타내고 있다[2].

많은 전력 계통에 사용되는 제어시스템 프로토콜들은 상호운용성, 확장성 등을 고려하여 점진적으로 국제 표준 프로토콜과 규약을 따라 적용되고 있다. 이렇게 국제 표준 프로토콜이 공개되면서 제어시스템의 프로토콜의 보안 취약점도 노출되고 있다.

제어시스템 프로토콜에 대한 취약점 [3] 은 프로토콜 명세상의 취약점(Design Vulnerability)과 프로토콜 구현 및 설정상의의 취약점(Implementation & Configuration Vulnerability)으로 분류할 수 있다. 프로토콜 구현과 설정상의 취약점은 상용제어시스템마다 프로토콜 명세를 따르지 않거나 구현하지 않을 수 있으며, 제어시스템을 설정하는 환경이 다르기 때문에 제어시스템 운영 기관마다 다른 취약점을 가지고 있다. 그러나, 제어시스템 프로토콜 명세상의 취약점은 프로토콜 명세를 따르는 모든 제어시스템과 네트워크에서 일반적으로 가능하다. 제어시스템 프로토콜인 ICCP 역시, 제어시스템 프로토콜 설계 상에 인증(Authenticity), 무결성(Integrity), 기밀성 (Confidentiality), 가용성(Availability) 확인 기능이 없거나 약한 취약점을 내제하고 있다. 본 논문에서는 ICCP의 보안 취약점을 제거하고, 보안을 강화한 한국형 계통운영시스템 간 안전하고 신뢰성 있는 데이터 연계 및 교환을 위한 ICCP/TASE.2 보안 기능 개발을 소개하고자 한다.



〔그림 1〕 전력 계통 계층 및 시스템간 프로토콜

Ⅱ. TASE.2 Service and Protocol

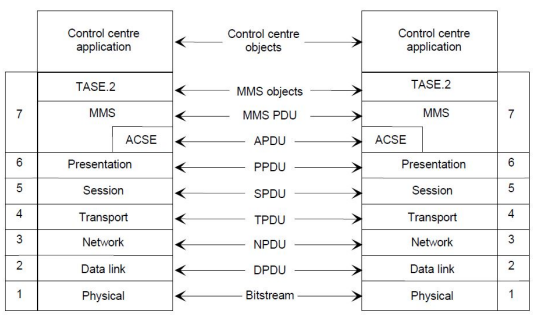
2.1. ICCP 프로토콜 구조

ICCP는 국제 표준 IEC 60870-6-503(Ed3, 2014.07)의 Telecontrol Application Service Element(TASE.2)의 Service and Protocol로써 표준화 되어 기술된다.

서로 다른 제어센터(SCADA, EMS, DMS 등) 간에 응답시간의 중요성을 갖는 실시간 데이터 연계를 위한 데이터 교환 메커니즘을 정의한다.

ICCP는 장치제어, 일반적인 메시지, 원격 제어 센터의 프로그램 제어 등에 대하여 지원한다. 그림 3에서 보는 바와 같이 OSI의 7계층 중 응용계층(Application Layer)에서 데이터 교환을 구현하기 위하여 ISO 9506 MMS(Manufacturing Message Specification) 서비스를 이용하여 표준화된 방법을 정의하고 있다.

ICCP는 OSI의 7계층 모든 계층들을 최대한 활용하고 있다. ICCP와 MMS는 각기 다른 Vendor에 의해 개발되었지만, ICCP에 API(Application Program Interface)를 적용함으로써 데이터 분배, 장치제어, 정보 Message의 출력 또는 원격 프로그램의 정의와 실행을 상호 운용할 수 있다. 또한 ICCP는 7계층의 ACSE(Application Control Service Element)의 서비스를 이용함으로써 네트워크 간의 논리적인 결합과 연결을 유지하고 만들 수 있다.



〔그림 2〕 ICCP 프로토콜 관계

2.2. MMS

MMS는 서로 다른 제조회사의 서로 다른 단위제어

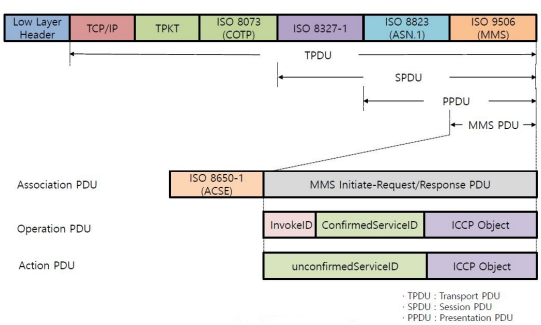
기기 기간에 메시지 교환을 위한 OSI 참조 모델 중 응용계층에 속하는 프로토콜로 ISO/IEC 9506-1과 ISO/IEC 9506-2 문서로써 국제 표준이다.

ISO/IEC 9506-1은 가상제조기기(VMD, Virtual Manufacturing Device), 네트워크 상에서 교환되는 메시지 정의, VMD에 관련된 속성과 파라미터에 대해 기술한다. ISO/IEC 9506-2는 프로토콜의 사양을 표현계층(Presentation Layer)의 추상구문표현 ASN.1 (Abstract Syntax Notation 1)로 기술되어 있다. MMS의 이점은 통합의 편리성, 설치비용과 유지보수 비용 감소, 응용프로그램 이식 등 많이 있지만, 무엇보다도 다른 제조사 기기 간 서로 다른 프로토콜을 사용하는 기기들 간의 통신을 가능하게 하는 상호운용성에 있다.

MMS는 가상제조기기로서 각각의 디바이스를 표현하며, 가상제조기기는 속성과 동작으로 나누어져 디바이스의 모든 자원들을 나타낸다. 서로 다른 기기들을 가상제조기기로 표현함으로써 통신을 할 수 있는 환경을 제공한다. 이 통신 규약은 클라이언트-서버 모델을 기본으로 하고 있으며, 그림 3에서와 같이 클라이언트 시스템과 서버 시스템은 구조화된 데이터 블록인 PDU(Protocol Data Unit)를 이용하여 통신한다.

MMS는 Context, VMD, Variable, Domain, Program Invocation, Semaphore, Event, Journal 등 8개의 객체로 이루어져 있고, 객체들에 대해서 정의된 서비스는 86개를 제공한다. 이들 객체와 서비스들의 일부분이 ICCP의 객체와 서비스들로 매핑되어서 사용된다.

ICCP는 실제 데이터 센터를 나타내기 위해서 가상제어센터(VCC, Virtual Control Center)라는 추상적인 개념을 사용한다. 이는 MMS의 가상제조기기(VMD) 개념의 확대이며 실제 계통운영센터의 모든 데이터들을 추상화하여 나타낸다.

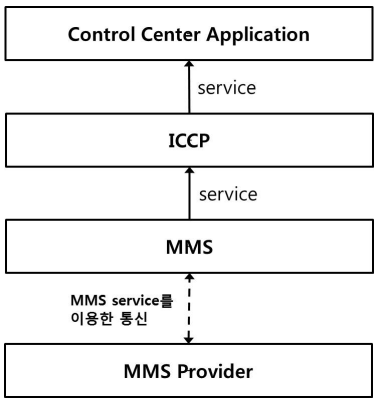


〔그림 3〕 PDU 구조

2.3. ICCP와 MMS의 관계

그림 4는 MMS와 ICCP의 관계를 나타내며 기본적으로 MMS의 서비스를 통하여 ICCP로 제공되고, ICCP의 서비스는 제어센터 응용어플리케이션으로 서비스를 제공한다. ICCP는 MMS 상에서 동작하며 MMS의 서비스와 프로토콜, 그리고 기능을 이용하는 표준화된 응용프로토콜이다. 이것은 MMS 객체에 매핑되어 있는 구조화된 데이터를 표현하고, 그것에 대해 특정 의미를 지정함으로써 MMS의 기능을 향상시킬 수 있다.

실제적인 MMS 서비스의 예로서, MMS는 원거리 시스템에서 데이터를 읽고 쓰는 것이 가능하며 이 데이터는 어떠한 조건없이 응답한다. 만일 특정 조건 하에서 데이터를 읽어야 할 경우, ICCP는 MMS에서 제공되지 않는 서비스를 제공한다. 이러한 것들을 수행하기 위해 ICCP는 제어센터의 요구조건을 충족시키는 CBB(Conformance Building Block)를 정의함으로써 최적화되고 효과적인 구현을 할 수 있다. ICCP와 MMS는 둘 다 사용자에게 서비스를 제공한다는 점에서는 같지만, ICCP는 제어센터 간에 메시지교환을 위해 최적화 되었다는 점에서 다르다[4].



〔그림 4〕 MMS와 ICCP 관계

Ⅲ. Secure ICCP와 IEC 62351 보안표준

3.1. Secure ICCP의 고려사항 및 권장사항

현재 계통운영시스템 간 실시간 데이터 교환을 하는 ICCP에는 전혀 보안을 고려하지 않고 보안 취약점을

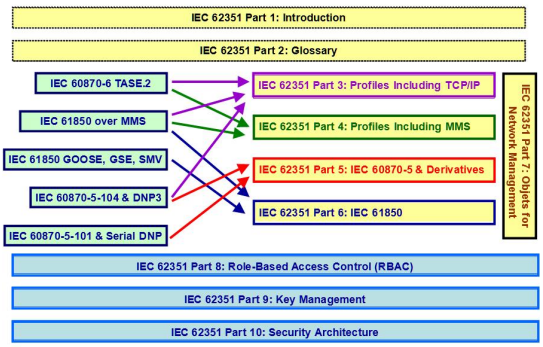
가지고 운용되고 있다. 보안 취약점을 제거하고, Secure ICCP의 IA(Information Assurance)를확보하기 위하여 데이터 가용성, 기밀성, 신뢰성과 인증 등 보안을 고려한 설계와 구현 가이드라인을 제시되고 있다[5].

네트워크 상에서의 통신 및 프로토콜에서의 가용성을 위하여 ICCP는 SSL(Secure Socket Layer)과 TLS(Transport Layer Security)을 구현함으로써 데이터 암호화하여 통신 데이터의 인가된 사용자 이외 접근을 차단해야 한다. 데이터가 통신하는 중간에 데이터가 변조되지 않도록 개인키로 암호화고 해쉬나 MAC(Message Authentication Code)를 이용하여 무결성을 보증해야 한다. 계통운영시스템 간 상호 인증(Authentication)을 위하여 PKI(Public Key Infrastructure) 기반 공개키 암호 메커니즘이 제공되어야 한다. 공개키 기반 인증서를 사용함으로써 SSL(Secure Socket Layer) 프로토콜과 Secure ICCP의 보안 기능을 확보하여야 한다[5].

3.2. IEC 62351 보안 표준

IEC 62351은 그림 5와 같이 IEC 60870-5와 60870-6, IEC 61850, IEC 61970, IEC 61968 시리즈의 보안 표준을 기술한다.

특히, Secure ICCP/TASE.2 보안과 관련하여 IEC 62351-3에서는 암호화를 위한 TLS 사용을 규정하고 있다. IEC 62351-4는 그림 6과 같이 ACSE (Association Control Service Element)의 인증을 정의하고 있어 MMS 기반 프로파일(Profile)로 응용계층에서의 상호인증을 규정한다.



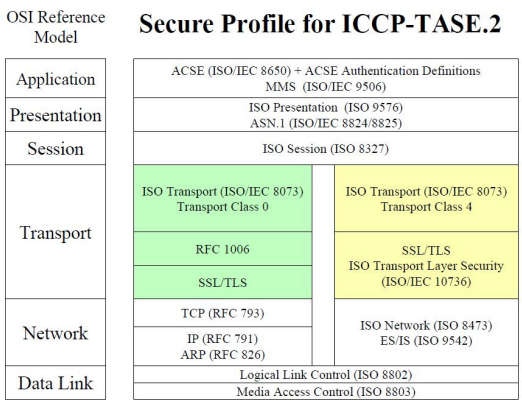
〔그림 5〕 IEC 62351 Security Standard

Ⅳ. Secure ICCP/TASE.2 개발

4.1. 개발환경

현재 EMS와 SCADA의 ICCP 모듈 및 데이터 분석을 통해 차세대 EMS와 차세대 SCADA의 요구사항에 맞는 개발환경을 적용하였다. 차세대 EMS는 HP-UX 11.31이고, 차세대 SCADA는 Linux 커널 2.6버전의 OS 환경이다.

본 논문에서는 계통운영시스템 간 Secure ICCP/TASE.2 개발에 대하여 소개하는 개발은 크게 두 부분으로 나눌 수 있다. 첫 번째는 Secure ICCP 보안모듈로 SISCO 사의 Secure ICCP Software Toolkit을 이용하여 국제 표준인 IEC 62351-4를 준수하는 것이고, 두 번째는 차세대 EMS와 차세대 SCADA의 OS 환경에 대한 국가정보원의 KCMVP (Korea Cryptographic Module Validation Program) 인증을 취득한 국가 표준 ARIA 암호알고리즘을 적용하는 것이다.

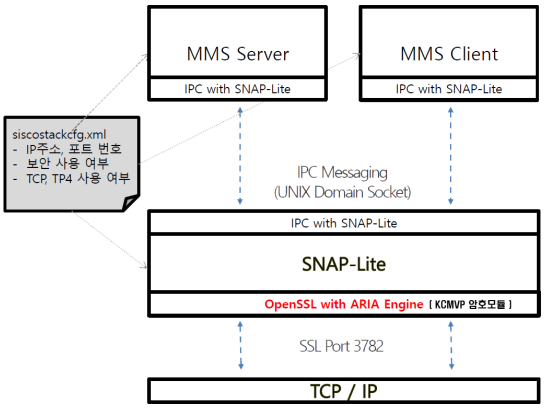


〔그림 6〕 Secure Profile for ICCP-TASE.2

4.2. Secure ICCP 보안모듈

Secure ICCP Software Toolkit은 MMS 및 SNAP(Secure Network Access Provider) 보안 모듈을 제공한다. 그림 7에서는 SNAP과 MMS의 관계를 도식화 하였다. MMS 서버는 한전 급전소의 차세대 SCADA이고, MMS 클라이언트는 차세대 EMS가 된다. SNAP은 MMS와 IPC(Inter-process Communication) 통신을 하여 보안 기능을 제공한다.

SNAP은 SSL/TLS 보안 기능 지원을 위하여 OpenSSL을 기본적으로 탑재되어 보안 기능을 제공하는 API를 제공한다. 그러나 SNAP은 API의 함수의 입력 파라미터와 출력에 대한 정의만 되어 있고, 실제 소스코드는 구현되어 있지 않다. 그래서 보안 기능이 적용되는 시스템에 맞는 보안프로토콜과 암호모듈을 사용할 수 있도록 구현하였다. 그리고 두 제어센터 각각의 인증서는 OpenSSL에서 제공되는 툴을 이용하여 인증서를 생성한 후 공개키와 전자서명 등에 적용하였다.



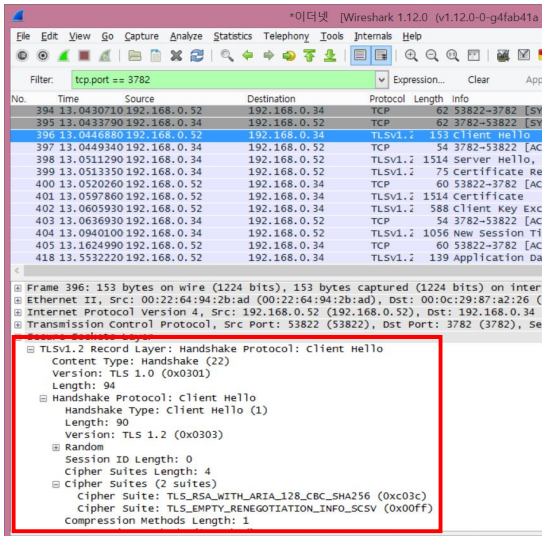
〔그림 7〕 SNAP과 MMS 아키텍처

4.3. KCMVP 암호모듈

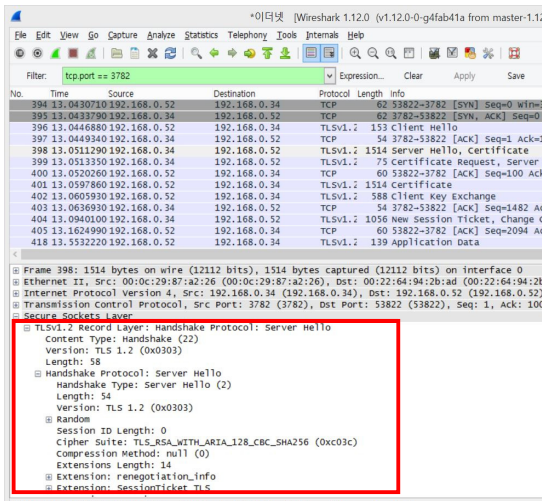
국정원에서는 국가 및 공공기관 정보통신망의 정보를 보호하기 위해서 사용되는 암호모듈은 KCMVP 통해 안정성과 구현적합성 검증된 암호모듈을 사용하도록 규정하고, 또한 국가 표준 ARIA 암호알고리즘을 사용하도록 규정하고 있다. 국가 표준을 준수하여 SNAP 보안 모듈 내 OpenSSL에 KCMVP 암호모듈을 추가하여 ARIA 암호알고리즘을 지원하였다. 그림 8은 차세대 EMS가 MMS 클라이언트로써 SSL/TLS 보안 통신을 하는 화면이다.

화면 상단에는 TLS v1.2 버전으로 client hello 핸드쉐이크 프로토콜 통신을 보여준다. 화면 하단은 보다 상세한 통신 내용을 확인할 수 있다. 즉, 핸드쉐이크 프로토콜의Cipher Suite로 TLS에서 ARIA 128 CBC모드와 SHA256으로 RSA 암호알고리즘 사용을 알 수 있다.

그림 9는 차세대 SCADA가 MMS 서버로써 SSL/TLS 보안 통신을 하는 화면이다. 마찬가지로 차



〔그림 8〕 차세대 EMS 보안프로토콜

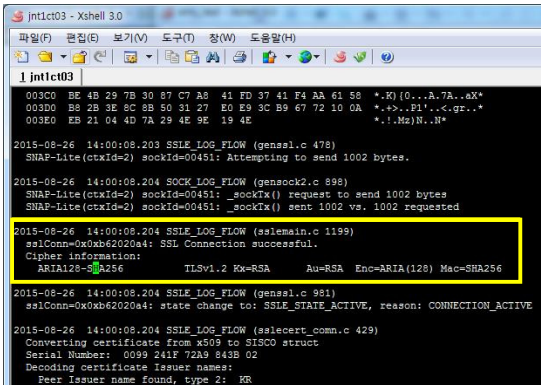


〔그림 9〕 차세대 SCADA 보안프로토콜

세대 SCADA도 Server Hello 핸드쉐이크 프로토콜의 Cipher Suite로 TLS에서 ARIA 128 CBC와 SHA256으로 RSA 암호알고리즘 사용을 알 수 있다.

차세대 EMS와 차세대 SCADA의 Cipher Suit는 데이터 암·복호화 알고리즘으로 ARIA 128 CBC 모드를 사용하고, 전자서명은 RSA 2048 사용한다. 해쉬알고리즘은 SHA256을 사용한다.

그림 10은 차세대 EMS에서 SNAP의 통신 로그화일을 실시간으로 캡처한 것이다. 차세대 EMS와 차세대 SCADA 가 국제 보안 표준과 국가 보안 지침을 준수



〔그림 10〕 Secure ICCP 통신 로그

하는 한국형 계통운영시스템 간 Secure ICCP/ TASE.2 보안 기술이 적용되어 두 계통운영시스템간 안전한 실시간 데이터 교환을 보여주고 있다.

Ⅴ. 결 론

본 논문에서 소개한 Secure ICCP/TASE.2 개발은 응용계층의 ACSE에 PKI 인증서 기반 전자서명 데이터 추가하여 국제 보안 표준인 IEC 62351 및 제어시스템 보안 규정을 준수함으로써 인증과 부인방지, 무결성 기능을 제공하고, 전송계층(Transport Layer)에서는 KCMVP 보안적합성 인증을 받은 SSL/TLS 보안 모듈을 이용하여 데이터 기밀성과 가용성에 대한 암호화 기능을 제공함으로써 제어센터 간 실시간 데이터 교환의 안전성과 신뢰성을 제공하였다.

참 고 문 헌

[1] ICCP Inter-control Center Communication Protocol; *Section 870-6-503:2014; TASE.2 Services and Protocol*, pp.10-15, (2014.07)

[2] 김명수, 임용훈, 현덕화, 김충환 “전력자동화용 통신프로토콜 현황 및 분석”, *대한전기학회 하계학술대회 논문집*, (2003.7)

[3] 장문수, 이건희, 김신규, 민병길, 김우년, 서정택, “DNP3 제어시스템 프로토콜 취약점 실험”, *보안공학연구논문지, 제7권 제1호*, (2010.2)

[4] 장경수, 장병욱, 한경덕, 신동렬, “ICCP를 사용한 전력센터간의 통신 프로토콜 구현”, *한국정보처리학회 논문지* 제7권 제12호, (2000.12)

[5] Secure ICCP Integration Consideration and Recommendations, http://energy. gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

〈저 자 소 개〉

박 성 완 (Sung-wan Park)
정회원

1998년 2월 : 연세대학교 전산학과 졸업
2001년 2월 : 연세대학교 전산학과 석사
2015년 3월~현재 : 충남대학교 컴퓨터공학과 박사과정
2001년 3월~현재 : 한전KDN 전력IT연구원 근무
관심분야 : 컴퓨터공학, 통신공학, 정보보호

김 진 철 (KIM Jincheol)
정회원

2006년 8월 : 광운대학교 대학원 박사 졸업
1996년 12월~현재 : 한전KDN 전력IT연구원 근무
관심분야 : 암호알고리즘, 통신공학, 정보보호

김 상 태 (KIM Sangtae)
정회원

1995년 2월 : 명지대학교 전기공학과 졸업
1998년 2월 : 명지대학교 전기공학과(석사)
2003년 2월 : 명지대학교 전기공학과(박사)
2003년 3월~2005년 1월 : 현대엔지니어링 근무
2005년 1월~현재 : 한전KDN 전력IT연구원 근무
관심분야 : SCADA, EMS, WAMPAC, 신호처리

이 승 원 (LEE Seungwon)
정회원

1990년 8월 : 고려대학교 대학원 석사
2013년 2월 : 서울벤처대학교 박사
1992년 1월~현재 : 한전 KDN 전력IT연구원 근무
관심분야 : 컴퓨터공학, 암호알고리즘, 정보보호