情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

# 저지연 Legacy SCADA 보안 통신장치 개발*

최 문 석,† 김 충 효,‡ 임 유 석, 주 성 호, 임 용 훈, 전 경 석
한전 전력연구원

# Development of Low Latency Secure Communication Device for Legacy SCADA*

Moon-suk Choi,† Chung-hyo Kim,‡ You-seok Lim, Seong-ho Ju, Yong-hun Lim, Kyung-seok Jeon
Korea Electric Power Corporation Research Institute

요 약

SCADA시스템에 대한 보안 필요성이 대두됨에 따라 최근 제어 프로토콜 보안기술에 대한 연구가 활발히 진행중이다. 그러나 성능, 가격 및 키 관리 등의 문제로 보안 솔루션이 legacy SCADA 시스템에 적용된 사례는 전무하다. 본 논문에서는 이러한 문제점을 해결하기 위해 low latency, 저가의 DNP 보안 솔루션을 제안한다. 본 논문에서 제안한 보안 솔루션은 데이터링크 계층에서 보안기능을 수행하고 보안을 위해 추가되는 데이터량을 최소화하여 전송시간 증가를 최소화하였을 뿐만 아니라 체계적인 키 구조와 키 분배방식을 제공하여 키 관리의 어려움을 해결하고자 노력하였다.

ABSTRACT

As the need for security of SCADA systems is increasing, significant progress has been made in research on security of control protocol. However, very few security solutions were adapted to legacy SCADA system. The reasons for non-adoption are latency, cost and key management problem. We propose a low latency, economic security Solution to solve these issues. The proposed solution performs security function in data link layer and has minimum overhead to minimize latency. Furthermore, we try to solve the key management problem by providing systematic security keys and key distribution method.

**Keywords**: Secure Authentication, DNP, BITW, latency, key management

## I. 서 론

과거의 전력 제어시스템은 제어시스템에 특화된 전용 프로토콜과 인터넷망과 분리된 폐쇄망을 통해 전력정보를 수집하기 때문에 외부로부터 침입이 불가능하며, 제어시스템을 분석하기 어렵기 때문에 사이버 공격으로부터 안전하다는 가정 하에 개발되어 전송 데이터 보호 기술이나 시스템 보호 기술이 적용되지 않았다. 그러나 최근 전력 제어 시스템의 운영 효율성 향상을 위해 제어 통신망과 업무망간의 통신망 연계 접점이 증가하는 추세이고 시스템간 상호 호환성 확보를 위해 표준화된 통신프로토콜과 장비를 사용함에 따라 제어 시스템 분석이 용이해져 사이버 공격 가능성이 증가하고 있다.

DNP(Distributed Network Protocol)은 원격지에 위치한 설비의 정보수집 및 제어에 최적화되어 설계된 제어시스템 전용 프로토콜로 전기, 수도, 가스 등 전 세계 제어시스템에서 가장 보편적으로 사용되고

접수일(2013년 2월 22일), 수정일(2013년 4월 11),
게재확정일(2013년 4월 11일)
* 본 연구는 2010년 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. (No. 20101010300091)
† 주저자, cms96@kepco.co.kr
‡ 교신저자, ch2kim@kepco.co.kr

있다. DNP통신규약은 물리계층, 데이터링크 계층 , 전송계층, 응용계층의 4계층으로 구성되며 보안, 확장성, 상호운영성 등을 보완한 규격이 2010년 7월 IEEE 1815 표준으로 발표되었다[1].

전력 제어시스템에서 사용되고 있는 DNP3 프로토콜 역시 보안상 안전하다는 가정하에 개발되어 에러 검출 메커니즘으로 CRC을 사용할 뿐 메시지 암호, 메시지 인증 등의 보안 메커니즘은 적용되지 않았다. 최근 DNP 제어명령 보호의 필요성이 증가함에 따라 DNP User Group은 기존 DNP3 통신규격에 메시지 인증 메커니즘을 추가한 DNP Secure Authentication 규격을 제정하고 2010년 IEEE 1815 규격으로 발표하여 제어명령 보호에 대한 관한 국제 표준을 완성하였다. 그러나 IEEE1815 국제 규격을 현재 운영중인 제어시스템에 적용하기에는 여러 가지 어려움이 있어 제어시스템에 보안기능을 추가한 사례는 전무한 실정이다.

본 논문에서는 현재 운영 중인 제어시스템 변경을 최소화하면서 보안기능을 추가할 수 있도록 설계된 DNP 통신 규격을 소개한다. 본 논문의 구성은 다음과 같다. 2장에서는 DNP 보안과 관련된 연구 동향을 소개하고, 3장에서는 DNP 보안기술에 대한 요구사항에 대해 살펴본다. 4장에서는 본 논문에 제안한 DNP 보안통신장치의 시스템 구성, 통신규격 및 통신절차를 설명한다. 마지막으로 5장에서 결론 및 향후 연구방향을 언급한다.

## II. DNP 보안 기술 동향

### 2.2 IEC 62351-5

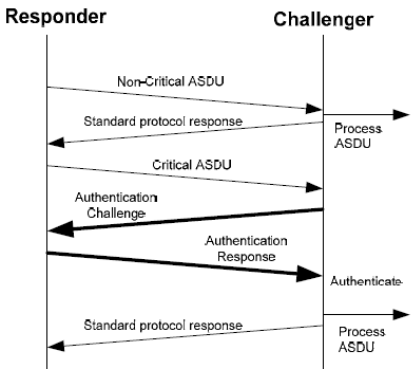
ISO/IEC TC 57 WG15(보안표준 그룹)은 스마트그리드시스템의 보안성 향상을 목표로 하고 있으며 WG15에서 제정한 IEC 62351 표준[2]은 IEC 60870-5, IEC 61850 등 전력자동화 프로토콜의 정보보안을 위한 표준으로 통신보호 규약, 네트워크 및 시스템 관리, 역할기반 접근제어, 인증 및 보안 키 관리 등 스마트그리드 및 연계 정보의 보호방안을 제시하고 있다. IEC 62351-5에서는 IEC 60870-5와 관련된 제어 프로토콜의 보안수준 제고를 위해 제어 프로토콜의 위협이 되는 spoofing, modification, replay, non-repudiation과 같은 공격행위를 명시하고 이에 대응하기 위해 보안 메커니즘을 설계할 때 고려사항, 설계 원칙과 함께 메시지 구조, 통신절차 및 알고리즘 등을 제시하고 있다.

### 2.2 IEEE 1815 DNP Secure Authentication

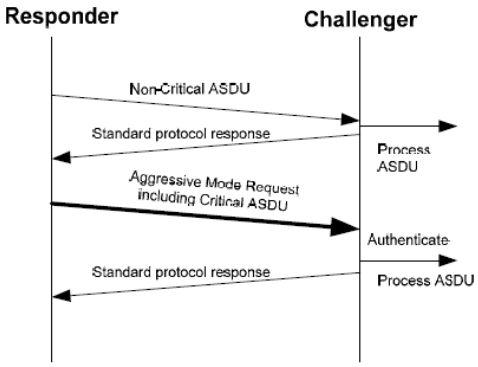
DNP User Group은 IEC 62351-3과 IEC 62351-5에서의 권고사항을 수용하고 이를 실제적으로 구현하기 위한 통신흐름, function code, object group, variation등을 구체화하여 2007년 3월에 DNP Secure Authentication 규격을 처음 발표하였고 2010년에 IEEE 1815 규격으로 발표하였다. IEEE 1815의 Secure Authentication 규격은 기존의 DNP3 규격에 인증과 무결성 보장을 위한 메커니즘을 추가하였다. Secure Authentication의 가장 큰 특징은 기존 DNP3 규격의 응용계층만 변경하여 메시지 인증기능을 제공한다는 점이다. Secure Authentication에서는 메시지 인증을 위해 Challenge-Response와 Aggressive의 두 가지 인증모드를 제공한다.

Challenge-Response 모드는 기본 인증 모드로 대부분의 제어시스템이 저속의 시리얼통신으로 운영된다는 점을 고려하여 전송성능을 보장하기 위해 control, setpoint adjustment, parameter setting 등과 같은 중요한 데이터(critical function code)를 요청하는 경우에만 메시지 인증기능을 수행하도록 설계되었다. 중요 데이터를 요청받은 장비(challenger)는 해당 프로세스를 즉시 수행하지 않고 난수를 포함하는 Authentication Challenge 메시지를 데이터 요청 장비(responder)로 전송하고 Responder로부터 MAC(Message Authentication Code)를 포함하는 Authentication Response를 받는다. Challenger는 Authentication Response 메시지 검증절차를 거친 후 유효한 경우에만, Challenge-Response 절차를 수행하기 전에 Responder가 보낸 명령에 대한 응답을 전송한다.

Secure Authentication에서는 전송효율을 위해 ISO/IEC 9798-4의 단방향 one-pass authentication 메커니즘을 사용하는 Aggressive 모드를 제공한다. Aggressive 모드의 경우 중요 메시지 요청 시 MAC을 첨부하여 전송하기 때문에 Challenge-Response 절차가 따로 수행되지 않는다. Aggressive 모드는 Challenge-Response 모드에서 발생하는 지연과 오버헤드를 제거할 수 있다.




〔그림 1〕 Challenge-Response 모드 인증 절차




〔그림 2〕 Aggressive 모드 인증 절차

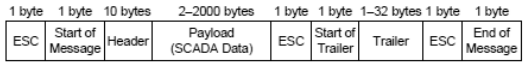
Secure Authentication에서는 메시지 인증을 위해 session key, update key 2종류 키를 사용한다. session key는 데이터의 인증에 사용되고 update key는 session key 교환시 키의 암호화에 사용된다.

## 2.3 IEEE 1711

IEEE 1711[3]은 IEEE 1689와 AGA(American Gas Association) 12-2표준을 기반으로 하고 있다. IEEE 1689와 AGA 12-2는 SCADA 시스템 내 시리얼통신의 보호를 위해 보안 요구사항을 정의하였으며 제어시스템에 이미 설치되어 있는 설비의 변경을 최소화하면서 보안성을 향상시키는 것을 목적으로 한다. IEEE 1711에서는 상호운용성을 위해서 시리얼구간의 데이터를 명확하게 정의하고 있어 다양한 시스템 구조와 연동하기 위한 유연성을 제공하고 있다.

IEEE 1711은 사이버공격에 대응하기 위해 암호 및 메시지인증 기능을 제공하며, 암호 알고리즘으로 AES, HMAC SHA-1 및 HMAC SHA-256을 사용한다. 프로토콜은 세션, 전송, 링크의 3계층으로 구성된다. 세션계층은 다양한 종류의 메시지의 표현, 세션키 협상, 추상적인 데이터 교환을 담당하고 전송계층은 무결성 검사, 암호화, header와 trailer의 추가를 지원한다. 링크계층은 통신채널에 전송을 위한 메시지의 구성을 담당한다.

IEEE 1711의 장점은 시스템 구성의 유연성에 있다. 사용자의 요구사항에 따라 암호를 위한 오버헤드 변경이 가능하고 암호 알고리즘도 선택적으로 사용할 수 있다




〔그림 3〕 IEEE 1711 메시지 구조

## 2.4 DNP 보안 솔루션 개발 현황

기 구축된 제어시스템에 보안기능을 탑재하기 위해서는 기존 시스템 전체를 보안기능이 탑재된 새로운 시스템으로 교체해야 하기 때문에 보안을 위해 많은 구축비용을 필요로 하며 시스템 교체에 따른 전력서비스 공급 중단 문제 등 어려움이 있다. 상기 문제점을 해결하기 위해 BITW[1](Bump-In-The-Wire)와 같은 별도의 보안통신장치를 개발하려는 연구가 활발히 진행되고 있다.

### 2.4.1 SEL(Schweitzer Engineering Laboratory)

SEL은 SCADA 장비간의 시리얼통신 데이터를 보호하기 위해 SEL 3021-1과 SEL 3021-2 두 종류의 BITW 장치를 개발하였다[4]. 또한, DOE의 지원을 받은 Hallmark 프로젝트를 통해 SSCP (Secure SCADA Communication Protocol) 규격에 적합한 보안솔루션으로 3025를 개발하였다. SEL 3021-1은 기밀성만 제공해주는 반면 SEL 3021-2과 SEL 3025는 기본적으로 데이터 무결성을 제공하지만 선택적으로 데이터 기밀성을 제공할 수 있다.

1) 통신보호를 위해 보안기능을 별도의 하드웨어로 구현하는 방식

#### 2.4.2 Cisco Systems

Cisco Systems는 제어시스템 내 시리얼통신(전송속도: 300~115200 bps) 구간에 데이터 무결성을 보장하기 위해 IEEE 1711에서 제시한 SCM(SCADA Cryptographic Module)을 BITW(Bump-In-The-Wire)형태로 구현하였다.

#### 2.4.3 PNNL(Pacific Northwest National Laboratory)

PNNL은 SCADA 메시지를 보호하기 위해 SCADA 메시지를 authenticator와 고유 식별자로 감싸는 형태인 PNNL의 SSCP(Secure SCADA Communication Protocol)로 변환하는 보안솔루션을 BITW와 임베디드 두가지 방식으로 구현하였다.

## III. DNP 보안 솔루션 개발시 고려사항

2.4절에서 살펴본 바와 같이 SCADA 메시지를 보호하기 위해 다양한 보안 솔루션이 개발되었으나 다음과 같은 이유로 운영중인 SCADA 시스템에 적용된 사례는 전무하다.

### 3.1 전송성능

최근 보고서에 따르면 SCADA시스템 운영자들은 보안솔루션을 도입함으로 인해 polling 효율이 20% 이상 저하되는 것을 원치 않는다[5]. PNNL의 시험 보고서에 따르면 1200bps 전송속도에서 AGA-12의 BITW 솔루션은 polling 효율이 70%까지 저하된다[6]. PNNL의 SSCP BITW 솔루션 역시 AGA-12의 솔루션과 크게 차이가 나지 않는다[7].

### 3.2 키관리

NIST의 Guide to SCADA and Industrial Control System Security에서는 키관리와 보안정책 결정에 숙련된 경험자들 위주로 보안전담팀을 운영할 것을 전력회사들에게 권고하고 있다. 키관리만을 위한 보안전담팀 운영은 전력회사에게 상당한 부담이 된다. 또한, CA(Certificate Authority)와 같은 상용 키관리시스템 운영은 상당한 비용을 요구하며 폐쇄망에 적합지 않다.

### 3.3 경제성

SEL 3021-1와 SEL 3021-2의 가격은 $540이고, SEL 3025의 가격은 $900로 BITW솔루션은 장비 한 대당 $500이상의 비용을 소모하며 시리얼 통신 한 회선을 보호하기 위해서는 한쌍의 장비를 필요로 한다. SCADA 시스템은 가용성 확보를 위해 회선 이중화, 장비 이중화 등의 메커니즘을 적용하고 있다는 점을 고려한다면 하나의 변전소에 여러 대의 BITW 솔루션을 필요로 한다. 또한 별도의 키관리시스템 구축 비용과 키관리 인력에 대한 교육 비용 및 인건비까지 고려한다면 보안비용 부담이 상당해진다.

## IV. DNP 보안 솔루션

본 논문에서는 DNP기반의 SCADA시스템 제어명령 보안을 위해 low latency, 저가의 DNP 보안솔루션을 제안하고자한다. 우리가 제안한 보안솔루션은 사용자의 키관리 부담을 줄일 수 있도록 자동화된 키 분배 기능을 지원한다.

DNP 보안솔루션은 키관리시스템(KMS : Key Management System), SSIO(Secure Serial Input Output module) 및 BITW 세 가지 장비로 구성되어 있다. KMS는 개인키와 업데이트 키 관리 및 보안통신장치의 관리기능을 수행한다. SSIO 장비는 제어센터에 설치되는 랙마운트 타입의 보안통신장치로 16채널의 시리얼 DNP 데이터 보호기능과 세션키 분배기능을 수행하며 키관리시스템과의 통신을 담당한다. BITW 장비는 변전소에 설치되는 보안통신장치로 8 채널의 시리얼 DNP 데이터 보호와 필드 장치에 대한 원격 사용자 인증기능을 담당한다.

[그림 4] DNP 보안장치(SSIO/BITW) 시작품 사진

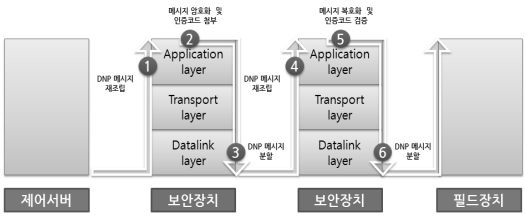
### 4.1 Low latency

SEL 3021-1 장비는 5 byte-times[2]의 낮은 전송시간 증가를 보장하지만 데이터 무결성 기능을 제공하지 않는다는 단점이 있고, SEL 3021-2 장비는

2) byte-time : 1바이트를 전송하는데 소요되는 시간

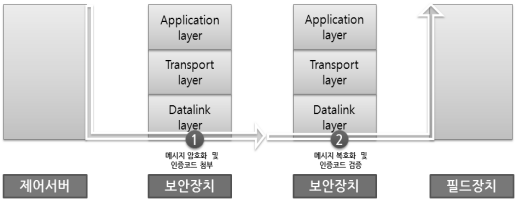
데이터 무결성 기능을 제공하지만 낮은 전송시간 증가를 보장하지 못한다.

IEEE 1815 Secure Authentication 규격은 응용계층만 변경하여 메시지 무결성 기능을 제공하고 체계적인 키 구조를 가지고 있어 키 관리의 어려움을 해결할 수 있다는 장점이 있지만 보안비용을 고려해서 BITW 형태의 보안 솔루션으로 구현할 경우에는 DNP 메시지 생성주체와 보안기능 수행주체가 다르기 때문에 메시지 재조립 및 분할과정이 부가적으로 발생하게 되고 이로 인해 전송시간 지연이 발생하게 된다.




〔그림 5〕 DNP 보안 흐름(IEEE 1815)

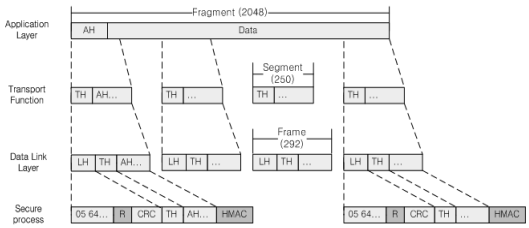
이러한 문제점을 해결하기 위해 본 논문에서 제안하는 DNP 보안 솔루션은 DNP 메시지 보호를 위해 BITW 장비가 데이터 링크 계층에서 보안기능을 제공하는 방법으로 설계하여 응용계층에서 보안기능을 수행함으로 인해 발생하는 전송시간 증가를 해결하고자 한다.




〔그림 6〕 DNP 보안 흐름(제안 방법)

### 4.1.1 데이터링크 계층에서의 보안기능 수행

본 논문에서 제안하는 보안솔루션은 4가지의 통신 방식을 지원한다. 보안기능을 제공하지 않은 장비와 통신을 위해 DNP 메시지를 그대로 전송하는 바이패스 모드(DNP)와 IEEE 1815 Secure Authentication 규격을 지원하는 인증모드(DNP-AUTH)모드를 지원한다. 두가지 통신모드이외에 전송시간 증가를 최소화하기 위해 데이터링크에서 보안기능을 제공하는 KEPCO-AUTH 모드와 KEPCO-SEC 모드를 지원한다. KEPCO-AUTH 모드는 데이터 무결성만 지원하는 인증모드이고 KEPCO-SEC 모드는 데이터 무결성과 기밀성을 모두 지원하는 암호모드이다. 〔그림7〕에 데이터 링크계층에서의 보안기능 제공방법을 나타내었다. 제어서버의 응용계층 메시지는 여러 개의 데이터링크 프레임으로 분할되어 전송되고 BITW 솔루션은 제어서버로부터 수신한 DNP프레임마다 보안기능 수행한다. 〔그림7〕에서 노란색 부분으로 표시된 필드는 보안기능을 위해 추가된 필드로 데이터링크 헤더(LH)의 CRC 필드 앞에 random data(R) 필드가 삽입되고, frame 끝에 메시지 인증데이터(HMAC)가 추가된다. 인증모드는 random 필드부터 어플리케이션 데이터까지 데이터를 대상으로 메시지 인증코드를 생성한다. 암호모드의 경우 인증영역 데이터에 대해 메시지 인증 코드 생성하고 메시지 암호화도 수행한다.




〔그림 7〕 데이터링크 계층에서의 DNP 보안기능

### 4.1.2 DNP 보안 메시지 구조

본 논문에서 제안하는 보안솔루션은 보안기능을 위해 키분배 메시지와 DNP 보안메시지의 두가지 메시지 구조를 제공한다. 키분배메시지는 DNP 보안메시지의 암호화에 사용되는 보안키를 분배할 때 사용되는 메시지로 IEEE 1815 규격에서 제공하는 reserved function code와 object를 이용하여 구현하였다. DNP 보안메시지는 보안기능 수행으로 인한 전송시간 증가를 최소화하기 위해 보안기능을 위해 추가되는 데이터량을 최소화하였다. 본 논문에서 제안한 보안솔루션은 보안기능을 위해 Random 필드와 메시지 인증코드만 추가된다. 상세한 메시지 구조를 〔그림8〕에 표현하였다.

random data 필드는 1바이트의 count와 4바이트의 random 값으로 구성된다. count 값은 송신측 BITW가 생성하여 전송하며 수신측 BITW가 수신한 메시지의 보안모드를 구분하는데 사용된다. random 값은 replay

| Data Link Layer | | | | | | | Transport function | Application Layer | Authentication field |
|---|---|---|---|---|---|---|---|---|---|
| Header | Len | Ctrl | Dest | Source | Random data | CRC | Transport Header | Application data | HMAC value |
| | | | | | 인증 영역 | | | | |
| | | | | | 암호화 영역 | | | | |
| 2 byte | 1 byte | 1 byte | 2 byte | 2 byte | 5 byte | 2 byte | 1 byte | 0~249 byte | N byte |

〔그림 8〕 DNP 보안 메시지 구조

공격 방지하는데 사용된다. 암호모드(KEPCO-SEC)의 경우 random data 필드가 암호문 랜덤화 기능에 사용된다. 〔그림9〕에 random data 필드의 구조를 나타내었다.

| Random data | |
|---|---|
| count | random |
| 1 byte | 4 byte |

〔그림 9〕 Random 필드 구조

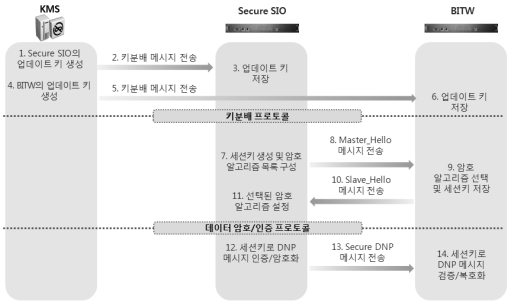
### 4.2 키관리 방안

본 논문에서 제안하는 키 구조는 IEEE 1815의 키 구조와 유사하다. IEEE1815에서는 DNP 메시지 인증에 사용하는 세션키와 세션키 분배시 세션키의 암호화에 사용하는 업데이트키의 두 가지 키를 제공하고 있지만 업데이트 키의 분배절차는 제시하지 않고 있다. 본 논문에서는 업데이트키 분배 문제를 해결하기 위해 비대칭키 방식인 개인키를 이용하여 업데이트키를 암호화하여 전송하는 방법을 제안한다. 보안키의 종류와 기능을 〔표1〕에 나타내었다.

〔표 1〕 DNP 보안키 종류와 기능

| 키 | 키 생성 주체 | 키 분배 대상 | 용도 |
|---|---|---|---|
| 개인키 (비대칭키) | KMS | SSIO BITW | 개인키 분배 업데이트키분배 |
| 업데이트키 (대칭키) | KMS | SSIO BITW | 세션키분배 |
| 세션키 (대칭키) | SSIO | BITW | 메시지 암호화 메시지 인증 |

〔그림 10〕에 보안키 분배 절차와 DNP 메시지 암호/인증 절차에 대해 나타내었다. 전력제어시스템의 특성상 전력 설비가 광범위한 지역에서 운영이 되며 원격지에 위치해 키 갱신을 위해 사용자가 현장에서 키 생성을 위한 비밀값을 입력하기 어렵다. 또한, 키 분배 절차에 인력이 개입할 경우 키 노출 위험이 존재한다. 이러한 문제를 해결하기 위해 본 논문에서는 비밀키 유출을 최소화하기 위해 키 생성은 장비내에서




〔그림 9〕 키 분배 및 데이터 암호 절차

실시하도록 설계하였다. KMS는 SSIO와 BITW장비의 개인키, 업데이트키의 생성, 분배 및 갱신을 담당한다. 세션키의 생성 및 분배는 SSIO가 담당한다. 또한, 사용자 개입을 최소화하기 위해 최초 장비 설치시 개인키만 입력하면 설정된 갱신주기에 맞춰 KMS가 개인키와 업데이트키를 자동으로 분배하고 갱신이력만 관리하도록 설계하였고 세션키는 SSIO와 BITW에만 보관되어 제어시스템 운영자도 현재 DNP 보안을 위해 사용되는 세션키를 확인할 수 없도록 하였다.

### 4.3 경제성

SCADA시스템은 제어서버와 필드장치로 구성된다. 제어서버는 필드장치를 관리하는 장치로 필드장치에서 전송되는 계측 정보를 수집하고 분석하며 필드장치로 제어명령을 전송하는 기능을 담당한다. 필드장치는 원격지에 위치해 대상 시스템의 계측정보를 제어서버로 전송하는 장비이다〔8〕.

통상적으로 제어서버는 다수의 필드장치를 관리하며 통신 가용성을 보장하기 위해 네트워크 이중화 및 장비 이중화 기법을 적용하고 있다. 하나의 제어서버가 16대의 필드장치를 관리하고 네트워크 이중화를 적용한 경우를 가정한다면 SEL 3021장비는 총 64대가 필요한 반면, 본 논문에서 제안한 솔루션은 SSIO 2대와 BITW 장비 16대가 필요하다. 네트워크 이중화뿐만 아니라 장비 이중화와 상위 연계시스템까지 고려한다면 SEL장비의 규모는 더욱 증가하게 된다.

본 논문에서 제안한 SSIO와 BITW 장비는 각각 16채널, 8채널의 데이터 보호가 가능하므로 SEL 사의 보안 솔루션에 비해 네트워크 이중화 및 장비 이중화가 구현된 SCADA 시스템에 적용하기 용이하다.

〔표 2〕 DNP 보안 솔루션 경제성 비교

| 구분 | 개소 | 설명 | SEL 솔루션 | 제안 솔루션 |
|---|---|---|---|---|
| 제어서버 | 1 | - 16대 필드장치 관리<br>- 네트워크 이중화 | 32 대 | SSIO 2대 |
| 필드장치 | 16 | - 네트워크 이중화 | 32 대 | BITW 16대 |

## V. 결 론

본 논문에서는 DNP 보안기술 개발 동향을 조사하고 DNP 보안 솔루션 개발시 고려해야할 사항으로 전송성능, 키관리, 경제성에 대해 살펴보았다. 본 논문에서는 IEEE 1815 Secure Authentication에서 제공하는 보안기능을 별도 보안장치로 구현할 경우 응용계층에서 보안기능 수행을 위해 발생하는 메시지 재조립 문제를 해결하기 위해 데이터링크 계층에서의 보안기능 제공방법을 제안하였으며 키관리의 어려움을 해소하기 위해 키 자동 분배방식을 제안하였다. 또한, legacy SCADA 시스템에 경제적으로 적용하기 위해 가능하도록 네트워크 이중화 및 장비 이중화시에도 하나의 장비로 지원이 가능하도록 개발하였다. 논문에서 제안한 보안 솔루션은 전력연구원에 설치된 SCADA 보안테스트베드와 연동하여 성능시험을 수행하고 있다. 향후에는 테스트베드 연동시험 결과를 바탕으로 IEEE 1815 Secure Authentication 방식과 본 논문에서 제안한 보안 솔루션의 전송 성능을 비교하여 전송성능 개선방안을 모색할 예정이다.

## 참고문헌


〔1〕 IEEE 1815, "Distributed Network Protocol(DNP3)," 2010

〔2〕 IEC 62351-5, "Security for IEC 60870-5 and derivatives," 2009

〔3〕 IEEE 1711, "Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links," 2007

〔4〕 A. Risley and K. Carson, "Low-or No-Cost Cybersecurity Solutions for Defending the Electric Power System Against Electronic Intrusions," Schweitzer Engineering Laboratories, Inc, 2008

〔5〕 P.P. Tsang and S.W. Smith, "YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems," Proceedings of the IFIP TC 11 23rd International Information Security Conference, pp. 445-459, Sep. 2008.

〔6〕 M.D. Hadley, K.A. Huston, and T.W. Edgar, "AGA-12, Part 2 Performance Test Results," Pacific Northwest National Laboratories, Aug. 2007.

〔7〕 M.D. Hadley and K.A. Huston, "Secure SCADA Communication Protocol Performance Test Results," Pacific Northwest National Laboratories, Aug. 2007.

〔8〕 김영진, 이정현, 임종인, "SCADA 시스템의 안정성 확보방안에 관한 연구," 정보보호학회논문지, 19(6), pp. 145-152, 2009년 12월.

## 〈著者紹介〉

최 문 석 (Moon-Suk Choi) 정회원
2002년 8월: 충남대학교 전파공학과 졸업
2005년 2월: 한국과학기술원(KAIST) 전기전자공학과 석사
2005년 2월~현재: 한국전력공사 전력연구원 근무
〈관심분야〉 제어시스템, 스마트그리드, 정보보호

김 충 효 (Chung-Hyo Kimi) 정회원
2003년 2월: 고려대학교 전기전자전파공학부 졸업
2005년 2월: 한국과학기술원(KAIST) 전기전자공학과 석사
2005년 2월~현재: 한국전력공사 전력연구원 근무
〈관심분야〉 스마트그리드, 보안관제, 정보모델

임 유 석 (You-seok Lim) 정회원
2004년 2월: 인하대학교 전자공학과 졸업
2009년 2월: 인하대학교 정보통신대학원 석사
2009년 12월~현재: 한국전력공사 전력연구원 근무
〈관심분야〉 정보보호, 무선통신, 전기자동차 충전인프라

주 성 호 (Seong-ho Ju) 정회원
2001년 2월: 연세대학교 전기공학과 졸업
2004년 2월: 서울대학교 전기컴퓨터공학부 석사
2004년 2월~현재: 한국전력공사 전력연구원 근무
〈관심분야〉 스마트그리드, 보안관제, AMI

임 용 훈 (Yong-hum Lim) 정회원
1996년 2월: 건국대학교 전자공학과 졸업
1998년 2월: 건국대학교 전자공학과 석사
1996년 2월~현재: 한국전력공사 근무
〈관심분야〉 정보보호, 스마트그리드, 보안관제

전 경 석 (Kyung-seok Jeon) 정회원
1986년 2월: 한양대학교 전자공학과 졸업
1994년 2월: 고려대학교 정보통신공학과 석사
1987년 2월~현재: 한국전력공사 근무
〈관심분야〉 정보보호, 전력제어, 스마트그리드