Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.5, Oct. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1201

IEEE 1815.1 기반 이기종 프로토콜 변환 게이트웨이 기술 연구*

이 석 준,[1†] 권 성 문,[1] 손 태 식,[2‡] 박 성 완[3]
[1]아주대학교 컴퓨터공학과, [2]아주대학교 사이버보안학과, [3]한전KDN

Research on Protocol Conversion Gateway based on IEEE1815.1*

Seokjun Lee,[1†] Sungmoon Kwon,[1] Taeshik Shon,[2‡] Sungwan Park[3]
[1]Department of Computer Engineering, Ajou University
[2]Department of Cyber Security, Ajou University,
[3]KEPCO KDN

요 약

기존의 전력망이 스마트그리드로 진화하면서, 수많은 컴포넌트간의 상호운용을 위해 각종 통신 표준과 기술들이 사용되고 있다. 이러한 실정에, 운영센터에서 외부와의 연계를 위한 다양한 프로토콜 연계방안의 필요성이 대두되었다. 본 논문에서는 국내에 자동화 변전소가 급증하는 실정에 따라, 기존제어센터와 자동화 변전소의 프로토콜 연계인 DNP3와 IEC 61850의 프로토콜 연계 게이트웨이에 대해 연구하였다. 프로토콜 매핑을 위해 IEEE 1815.1 표준을 분석하였으며, 게이트웨이의 개발 방향을 제시하고 프로토타입을 개발해 실현가능성을 검증하였다. 이에 더불어, 발생 가능 한 보안 문제를 제기하고 보안기술을 제시한다.

ABSTRACT

While the legacy electric grid evolving into the smart grid, various communication standards have been used for interoperability between many components. In this situation, the needs emerged for protocol conversion and mapping method for connecting the outside components to the operation center. In this paper, according to the surge of IEC 61850-based substation automation, we studied the protocol conversion gateway for linking legacy DNP3-based control center and IEC 61850-based substation automation. This paper is based on the IEEE 1815.1 standard for the protocol mapping. We suggested the direction of development the gateway and developed prototype for evaluate the proposed gateway. Also, we bring up a security problem and give a solution.

Keywords: DNP3, IEC 61850, IEEE1815.1, Mapping, Protocol conversion gateway, Substation Automation

I. 서 론

스마트그리드는 발전-송·변전-배전에 이르는 지능형 전력 시스템으로, 수많은 구성 컴포넌트들 간의 연계를 위해 각종 통신 표준과 기술들을 사용하고 있다. 스마트그리드 운영센터는 외부 시스템과 연계를 위해 IEC61970/61968의 CIM(Common Interface Model)을 사용하고 있으며, 변전소 등 하위 시스템에서는 간 직접적인 매핑을 통한 프로토콜 연계 방안이 요구되기도 한다. 이러한 실정에, 국내 전력망 운

Received(05. 30. 2016), Modified(09. 01. 2016), Accepted(09. 09. 2016)
* 이 논문은 2013년 산업통상자원부 재원으로 에너지기술평가원의 지원을 받아 수행된 연구임 (과제번호 : 20131020400660)
† 주저자, wadeco@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

영 면에서는 CIM, OPC UA(Open Platform Communications Unified Architecture) 등을 이용한 중앙 SCADA, K-EMS (Energy Management System), 차세대 EMS, 그리고 자동화 변전소 등 주요 전력 IT 시스템의 연계를 고려하고 있다.

특히 자동화 변전소는 2010년 풍동변전소를 시작으로, 2016년 현재까지 약 10여개의 변전소를 자동화변전소로 구축하였고, 2018년까지 60곳 이상의 자동화 변전소가 구축될 예정에 있다. 새로 구축되는 자동화 변전소와 기존 제어센터 간에 이기종 프로토콜이 사용되는 구간이 생기면서 프로토콜 변환 게이트웨이가 요구된다.

해외에서는 Newton-Evans Research의 통계자료[1]에 의하면 변전소 내부 네트워크 프로토콜은 2014년 북미 전력 유틸리티 중 76%가 DNP3-Serial을 사용하고 있고, 47%는 DNP3 LAN을 사용하였으며, 2016년까지의 전망으로는 IEC61850의 급부상과 DNP3 over TCP/IP의 꾸준한 활용을 예상하고 있다. 변전소의 외부 연계도 마찬가지로 DNP3가 35%로 가장 높은 비율을 차지하고 있어 변전소의 연계구간에서 DNP3-IEC61850 프로토콜 변환 게이트웨이가 개발되고, 보안기술이 개발된다면 국내뿐 아니라 국외의 산업기반시설에 보안기술을 보급할 수 있을 것이다.

DNP3와 IEC61850간에 통신을 수행하기 위해서는 프로토콜 매핑기술이 필요하며, 현재 도처에서 DNP3-IEC61850 프로토콜 변환 게이트웨이는 각 제조사나 사용기관별로 프로토콜을 매핑하며 별다른 표준 없이 사용되고 있다. 하지만 2011년부터 IEEE 표준 개발이 시작되어 현재 IEEE Approved Draft Standard인 IEEE1815.1-2015가 2016년 1월에 발표되었다.

본 논문은 변전소와 제어센터에서 DNP3 프로토콜[2]과 IEC61850 프로토콜[3]을 사용하게 되는 환경에서 IEEE1815.1의 표준[4]에 정의된 내용을 기반으로 프로토콜 매핑을 수행하고, 이 때, 발생할 수 있는 보안 문제를 제기하고자 한다. 본 논문에서는 DNP3 모듈로는 TurnerTech의 DNP3 protocol[5]을 이용하였으며, IEC61850 모듈로는 SISCO사의 MMS-EASE lite[6]를 사용하였고, Ubuntu14.04기반[7]에서 실험하였다.

논문의 구성은 2장에서 국내 현황 및 IEEE1815.1를 논하고, 3장에서는 국내 환경에 적용되어야 할 이기종 변환 게이트웨이를 제안하고 보안을 확보할 수 있는 방안을 제시한다. 4장에서는 논문에서 제시한 이기종 변환 게이트웨이의 구현 방향을 제안하고 이에 대한 타당성을 검증하였고, 마지막 5장이 향후연구방향과 논문의 결론이다.

II. 관련연구

2.1 국내 SCADA와 발전소 연계 현황

Fig. 1.은 기존의 레거시 변전소일 때 SCADA와의 통신과, 자동화변전소 도입 시 SCADA와의 통신을 간단히 비교한 것이며 변전소 내부 네트워크의 구성이 변화하고, ICT 기술적용이 가능하도록 IEC61850 프로토콜이 적용되었다는 큰 차이가 있다. 이제까지의 국내 대부분의 변전소들은 필드 디바이스 각각으로부터 센서가 측정한 값을 각 값 하나하나 코퍼 케이블을 통해 리포트 하였으며, RTU(Remote Terminal Unit)에서 이를 취합하여 SCADA(Supervisory Control And Data Acquisition)의 FEP(Front End Processor)에 DNP3 프로토콜을 통해 전달하는 방식을 사용해 왔다. 하지만 스마트그리드 시대가 도래하면서 국내 변전소도 ICT기술이 적용되기 시작하였고. 2010년 풍동 자동화변전소를 시작으로, 2013년 농소 등 10여곳에 자동화 변전소를 도입했고 향후 2018년까지 60곳 이상의 자동화 변전소를 구축할 예정에 있다.

국내 변전소의 형태가 변화함에 따라 DNP3와 IEC61850의 연계구간이 발생하게 되었고, 연계구간에서는 게이트웨이에 프로토콜 변환 기능을 포함함으로써 SCADA 내부의 다른 컴포넌트들에 영향을 최소화 하면서 자동화 변전소로 교체를 할 수 있다. 물론 변전소의 교체 뿐 아니라 신규 자동화변전소를 구축할 때도 프로토콜 변환 게이트웨이가 필수적으로 동반되어야 한다.

2.2 IEEE1815.1 표준의 배경

전력제어시스템에서는 기존에 OPC UA라는 통합 아키텍처를 사용하여 이기종 장비 통신의 미들웨어로 활용하여 다양한 프로토콜 간 통합된 데이터 모델을 사용하는 네트워크를 구성한 뒤에야 프로토콜 매핑이 가능했다. OPC UA의 장점은 DNP3, IEC61850, DLMS/COSEM, IEC61870 등 보다 다양한 프로

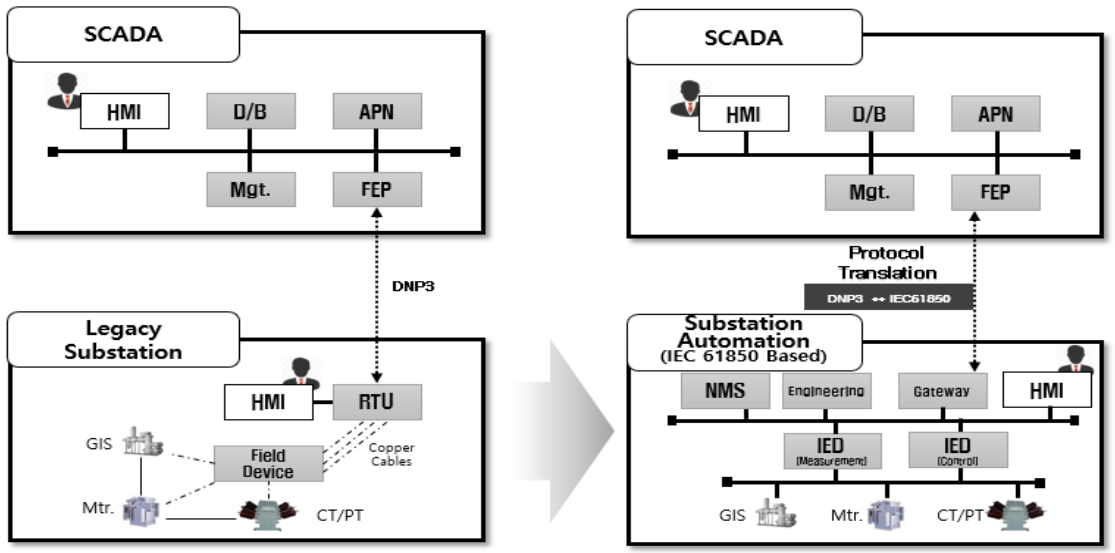

Fig. 1. Differences with S/S and S/A

토콜이 혼재되어 있는 네트워크에서 통합된 데이터 모델을 사용하기 때문에 통신뿐 아니라 데이터 통합 관리 측면에서도 용이하다. 하지만, OPC UA를 사용하기 위해서는 제어센터 측 네트워크 자체가 OPC UA로 구성되어야하기 때문에, 현재 운영 중인 제어센터에 적용하기 위해서는 모든 장비에 대규모 개선 작업을 수행해야 한다.

이러한 실정에 2011년부터 개발되어온 표준 IEEE1815.1은 DNP3와 IEC61850을 직접 매핑하는 방식으로 표준을 제정하였고, 이를 활용하면 운영 중인 제어센터에 직접적으로 통신할 기기만 개선하고 프로토콜 변환 게이트웨이를 설치하면 새로 구축되는 자동화변전소를 운영할 수 있다. 이는 OPC UA보다 경제적일 뿐 아니라, 변전소와 제어센터간에 부하 및 속도면에서 유리할 수 있다.

2.3 IEEE1815.1 관련 기술 및 표준 현황

스마트그리드가 도입됨에 따라 변전소 네트워크는 IEC61850기반 디지털 변전소로 변화되고 있으나 변전소 및 변전소 연계구간에서 사용되는 DNP3 프로토콜의 경우 IEC61850 표준에서 사용되는 구조체/데이터이름표현 등 IEC61850 기반의 기능을 모두 제공하지 못하기 때문에, 두 프로토콜을 연계·사용하기 위해서는 프로토콜이 제공하는 서비스와 데이터를 매핑하는 룰이 필요하다. 국내에서는 송병권 외 1인의 "DNP3.0과 IEC61850 게이트웨이 기능 설계"[8]에서 DNP3와 IEC61850의 프로토콜 변환 기능이 포함된 게이트웨이를 설계하였고, 이는 프로토콜 변환 게이트웨이를 설계하는 일반적인 접근 방식을 두 프로토콜에 적용하여 매핑 가능한 데이터 오브젝트와 서비스를 추출하고 이를 상호 변환 시킬 수 있는 게이트웨이를 설계하였다. 하지만 위 논문에서는 매핑하는 방식을 자체적으로 설계하였고, 본 논문에서는 국제표준인 IEEE 1815.1의 절차를 따른다. 마찬가지로, 일찍이 미국, 유럽 등지에서는 제조사별로 제각각인 룰을 이용해 매핑게이트웨이를 설계하였고, 2011년에 NIST가 후원하는 SGIP(Smart Grid Interoperability Panel)에서 DNP3와 IEC61850의 상호운용을 위한 매핑 가이드라인 개발을 시작으로 IEEE1815.1표준이 등장하였다.

한편, 자동화변전소에 사용되는 통신프로토콜인 IEC 61850은 DNP3 프로토콜 외에도 기존의 다양한 프로토콜을 수용하기 위해 Table 1.과 같이 IEC 61850의 서브표준으로 매핑 및 변환과 관련한 표준을 제정해나가고 있다. 이 중, IEC61850-80-2 표준이 DNP와 IEC61850의 매핑에 대한 표준이며, 이는 IEEE1815.1과 함께 Dual Logo로 출판될 예정이므로 사실상 DNP3와 IEC61850의 매핑 표준은 IEEE1815.1이 유일하다. IEEE1815.1은 2015년 10월 19일에 Draft 8.00버전이 공개되었고, 2016년 1월에 이 버전을 IEEE1815.1-2015로 명명하여

Table 1. Mapping Related Standards of IEC61850

Standard Parts	Title
IEC 61850-80-1	Guideline to exchange information from a CDC based data model using IEC 60870-5-101/104
IEC 61850-80-2	Mapping DNP3 to IEC 61850 (will be published with IEEE1815.1 as Dual Logo)
IEC 61850-80-3	Mapping to Web protocols - Requirements and Technical choices
IEC 61850-80-4	Translation from the COSEM object model (IEC 62056) to the IEC 61850 data model
IEC 61850-80-5	Guideline for mapping information between IEC 61850 and IEC 61158-6 (ModBus)

Approved Draft Standard로써 출판하였다.

III. 국내 환경에 적합한 IEEE1815.1 기반 이기종 변환 게이트웨이

본 장에서는 IEEE1815.1에서 기술하고 있는 DNP3와 IEC61850 매핑의 유즈케이스와 매핑기술을 파악하고 국내환경에 적용가능 한 이기종 프로토콜 변환 게이트웨이 모델을 제안한다. 이와 더불어 보안성 제공을 위해 필요한 기술을 제안한다.

3.1 IEEE1815.1 Use Cases

IEEE1815.1에서 DNP3와 IEC61850 연계는 우선 Use case(a)와 Use case(b)의 두 유즈 케이스로 나뉜다. 두 유즈 케이스는 매핑 자체를 수행하기 위한 기본 요소는 유사하나 그 의미와 입출력 데이터에 차이가 있다. 가장 큰 의미상의 차이는 Use case(a)는 제어센터와 변전소간 통신에서 제어센터가 DNP3 프로토콜을 유지하고, 변전소가 IEC61850기반으로 교체되거나 새로 구축되는 경우이며, Use case(b)는 제어센터가 IEC61850기반으로 교체되는 경우 기존에 DNP3 기반으로 동작하던 변전소를 수용하는 경우를 뜻한다.

본 논문에서 제안하고자 하는 구조는 Fig. 2.의 Use case(a)의 형태이다. 국내 SCADA와 변전소의 통신구조에서 국내흐름은 변전소가 우선 IEC61850 기반으로 운영되는 Use case(a)의 형태이기 때문에, 우선적으로 Use case(a)와 같은 상황에서 동작하는 이기종 변환 게이트웨이를 구축해야 한다.

3.2 IEEE1815.1 Greenfield Model

앞 절에서 설명한 IEEE1815.1의 Use case(a)는 세부적으로 Use case(a1):Greenfield와 Use Case(a2):Retrofit의 두 가지로 구분되어 있다. Greenfield 형태는 기존의 DNP3 기반 제어센터를 그대로 운영하면서 새로운 IEC 61850 기반 자동화 변전소를 도입하는 경우이다. 이때는 제어센터의 DNP3 프로토콜의 데이터 리스트인 Point list를 새로 구축할 자동화 변전소로부터 IEC 61850 데이터를 기준으로 설정하게 된다. Retrofit의 경우, 기존의 DNP3 기반 제어센터를 그대로 운영하면서 기존에 운영 중인 변전소를 자동화변전소로 변환하는 경우를 말하며, 이때는 기존에 변전소와 제어센터 간에 사용되고 있던 DNP3 Point list는 수정이 불가하기 때문에 기존의 요구사항과 신규로 추가되는 데이터에 대한 설정이 복잡하다. IEC61850 기반의 변전소로 변환하면서, 기존 DNP3의 데이터 중 일부 매핑이 명확하지 않은 경우는 이를 리포팅하기 위해서 개발자가 임의로 생성해야 할 수 있어야 한다. 단, 이 부분은 표준에 정의되어 있지 않다.

본 논문에서는 신규 디지털 변전소가 구축되고 있는 국내 운영 현황에 적합한 IEEE1815.1 매핑 모델인 Use case(a1): Greenfield 모델을 우선적으

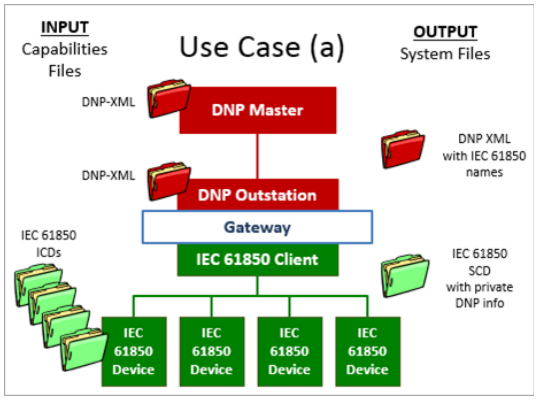

Fig. 2. IEEE1815.1 Use cases (a) : DNP3 Control Center & IEC61850 Substation[4]

Table 2. A Part of Leaf Level Data Mapping Rules between IEC61850 and DNP3 DataType

Spec Order	Leaf Data Attribute Name (s)	DataType	FC	First Ref CDC	Rule Name	BI	DBBU	BO	AI	AIFP	AIDB	AO	AOFP	CTR	FRZCTR	OCT	Profile	Const
1	stVal, general, transInd	BOOLEAN	ST	SPS	BOOLEAN_TO_BI	1												
2	q	Quality	ST	DPS	QUALITY_TO_BIN_FLAG	n												
2	q	Quality	MX	MV	QUALITY_TO_ANA_FLAG				n									
3	t	TimeStamp	ST, MX	SPS	TIME_TO_TIME	n	n	n	n	n		n	n	n	n	n		
4	subEna	BOOLEAN	SV	SPS	BOOLEAN_TO_BO			1										

로 반영할 것이다.

3.3 매핑 프로세스

본 논문에서 제안하는 바는 Use case (a1)인 Greenfield의 프로토콜 변환 게이트웨이를 개발하기 위해서는 우선 새로운 자동화변전소를 설정하고, 기존에 사용하던 DNP3 프로토콜의 Capabilities를 확보한다. 위 과정의 방법론은 표준에 정의되어있지는 않고, 프로토콜 매핑을 위해서 필수로 수반되어야 하는 과정이다. 프로토콜의 매핑은 IEEE1815.1 표준에서 정하고 있는 매핑 룰들을 따라야 하며, 크게 서비스의 매핑과 데이터모델을 매핑하는 것으로 나뉜다. 서비스의 매핑은 Solicited Read Request/Response, Unsolicited Respond(Report) 등의 서비스에서 프로토콜 변환 게이트웨이는 어떤 흐름으로 메시지를 전달하게 되는지를 표준에 제시한 것이다. 데이터모델의 매핑은 IEC61850에서 제공하고 있는 데이터 변수를 DNP3의 어떤 데이터타입에 매핑하는 것을 권장하는지, 혹은 매핑이 불가능한지를 중점으로 표준화한 부분이다. 특정 타입 간에는 1:1로 상대 프로토콜의 정해진 타입으로 변환시켜야 하는 반면, 한쪽 프로토콜의 값이 상대 프로토콜로 매핑될 때는 데이터타입을 여러 가지 중 하나로 매핑시키는 경우도 있다. Table 2는 IEEE1815.1표준의 매핑테이블의 일부를 발췌한 것이다. Spec Order 2의 경우 IEC61850의 Quality값인 q항목은 FC(Functional Constraint)와 First Ref CDC에 따라 DNP3의 BI(Binary Input) 혹은 AI(Analog Input)에도 매핑할 수 있다. (실제 IEEE1815.1 표준에서 Quality의 매핑 룰은 10가지를 제시하고 있다) Spec Order 3의 Leaf Data Attribute Name이 t인 항목을 보면, IEC61850에서 TimeStamp를 의미하는 t 어트리뷰트의 경우에는 DNP3의 BI, DBBI, BO, AI 등 10가지의 타입 중 한 가지에 매핑시킬 수 있다는 의미이다. Quality의 매핑 룰이 여러 가지로 표현된 것과 달리 DNP3에서 TIME값으로 쓰이는 데이터타입에 매핑한다는 의미로 매핑룰은 TIME_TO_TIME으로 일괄 표현된다. 마지막으로 Spec Order 4의 subEna의 경우는 무조건 DNP3의 BO(Binary Output)으로 매핑해야 된다는 의미로 매핑 데이터타입이 1:1로 지정된 경우도 있다. IEEE1815.1 표준의 'Leaf Level Mapping Rules and

```
<!--2) IEC61850 Object Mappings-->
<iec61850DeviceMapping>
  <iec61850RuleMapping note="TIMESTAMP MAPPING TEST">
    <rule>TIME_TO_TIME</rule>
    <dnp3XPath>DNP3DeviceProfileDocument/referenceDevice/dataPointsList/binaryInputPoints/dataPoints/binaryInput[0]/dnpData/timestamp</dnp3XPath>
    <iec61850Path>IEDRelay1/LLN0.Mod.t</iec61850Path>
  </iec61850RuleMapping>
</iec61850DeviceMapping>
```

Fig. 3. A Part of DNP3-XML with Mapping Information

Conformance Table'에서 IEC61850과 DNP3의 Leaf 레벨의 데이터 매핑 106가지를 제시하고 이를 57가지 매핑 룰로 분류하고 있다.

IEEE1815.1에서는 use case(a)의 경우 게이트웨이에 매핑정보가 포함된 DNP3-XML이 산출물로 도출되며, 매핑과 관련된 정보는 Fig. 3.과 같은 XML 형태로 기록된다. 이는 IEC61850의 오브젝트인 IED/Relay1/LLN0.Mod.t의 Timestamp 값을 DNP3 point list의 BI(Binary Input)의 하나의 값과 매핑한 예시이다. 매핑이 필요한 모든 변수를 매핑하면, 게이트웨이와 DNP3 Master에 다시 설정하여, 실제 통신이 가능하도록 한다.

3.4 이기종 프로토콜 변환 게이트웨이 보안 기술

이기종 프로토콜 변환 게이트웨이는 양 측 디바이스 간에 End-to-End 보안을 제공할 수 있는지가 보안 측면에서 가장 큰 문제점으로 대두된다. 이는 End-to-End 보안의 본질인 종단 간 프로토콜의 변화가 없으며, 보안처리 된 부분은 그대로 전송되어야 한다는 원칙 자체를 지키기 어렵기 때문이다. 프로토콜 변환 모듈을 설계함에 있어서 입력프로토콜과 출력프로토콜이 다르고, 이 구간에서 만약 프로토콜 간 공통된 보안기술이 없는 경우엔 변환 과정에서 데이터 구조 및 데이터 값이 노출될 수밖에 없다. 이러한 실정에서 게이트웨이 모듈이 포함되는 기기를 물리적으로 철저히 관리하여 신뢰성을 최대한 높여야하며, 양측 프로토콜에서 제공하는 보안 기술을 게이트웨이의 각 통신 모듈에서 지원할 수 있도록 개발되어야 한다. IEEE 1815.1에서는 DNP3, IEC61850 각 구간에서의 보안이 동일한 수준으로 구현되어야 한다고 표현하고 있으며, IEC61850 기기와 게이트웨이 IEC61850 Module에서는 IEC62351의 TLS/SSL기반으로 보안을 구축하고 DNP3 기기와 게이트웨이의 DNP3 Module의 통신에서도 TLS/SSL을 추가적으로 적용하여 동일한 수준의 보안을 유지할 수 있다. 물론 이렇게 양측에 보안기능을 추가하는 경우엔 게이트웨이 내부 프로세스가 안전하다고 가정하여 게이트웨이 기기 자체에 대한 신뢰성이 기반이 되어야 한다. 따라서 게이트웨이 내부적으로 처리되는 데이터 및 매핑룰 등에 대한 자체적인 보안 기술도 동반되어야 한다. 결과적으로는 양단의 네트워크에 대한 보안 및 게이트웨이 기기보안을 통해 DNP3기기로부터 IEC61850기기까지의 네트워크 측면에서 End-to-End와 유사한 수준의 보안이 성립될 수 있도록 구성해야한다.

IV. 구현 방안 및 검증

본 논문에서는 국내 환경에 적합한 IEC61850-DNP3 간 프로토콜 변환 게이트웨이 전체적인 시스템 아키텍처를 Fig. 4.와 같이 정의하고, 이를 바탕으로 제어메시지 매핑 게이트웨이의 이기종 간 메시지 송수신에 대해 통신기능이 정상적으로 동작할 수 있는지를 검증하기 위한 모듈을 연구하였다. 게이트웨이를 구현함에 있어서 IEEE1815.1에서는 게이트웨이의 기능적 범위를 3가지 모델로 제시하고 있다. 첫 번째는 사전에 매핑이 완료된 상태에서 프로토콜 변환 프로세스만 제공하는 경우, 두 번째는 변환 프로세스 뿐 아니라 게이트웨이의 Polling정보, Priority(Control, Queueing) 등의 통신 구성을 설정하는 도구를 제공하는 경우, 마지막으로 변환프로세스, 게이트웨이 설정과 함께 사전매핑의 기능까지 게이트웨이에서 제공하는 것이다.

본 논문에서는 게이트웨이의 역할 및 현실성을 고려하여 매핑과 게이트웨이 설정은 사전에 수행하고,

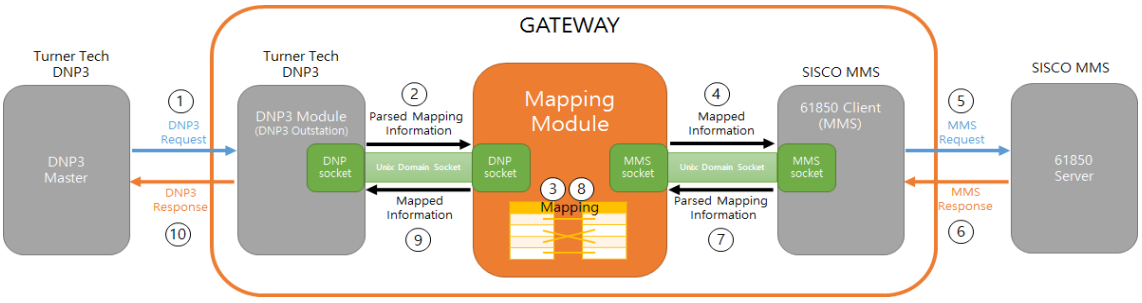

Fig. 4. Protocol Conversion Gateway Architecture

Table 3. DNP3 to IEC 61850 Protocol Conversion Flow

#	Actor	Role
1	DNP3 master	DNP3 master sends 'DNP3 Request' message to gateway (DNP3 Secure Authentication recommended)
2	DNP3 module of gateway	DNP3 module parses information for mapping such as Function code, Object Group, Variation, Number of Data from received message and sends these information to mapping module via IPC
3	Mapping module(internal)	Mapping module maps requested DNP3 objects to IEC61850 objects based on DNP3-XML having mapping rules(Mapping rules based on IEEE 1815.1)
4	Mapping module	Mapping module sends the mapped information to IEC61850 module via IPC
5	IEC61850 module of gateway	IEC61850 module generates 'MMS Request' message with mapped information, and sends message to IEC61850 IED (TLS/SSL recommended)
6	IEC61850 IED	IEC61850 IED sends 'MMS Reponse' to gateway
7	IEC61850 module of gateway	IEC61850 module parses information for mapping such as MMS Opcode, Object Type, Variable Name, Variable value from received message and sends this information to mapping module via IPC
8	Mapping module(internal)	Mapping module maps responsed IEC61850 objects to DNP3 objects based on DNP3-XML having mapping rules(Mapping rules based on IEEE 1815.1)
9	Mapping module	Mapping module sends the mapped information to DNP3 module via IPC
10	DNP3 module of gateway	DNP3 module generates 'DNP3 Response' message with mapped information, and sends message to DNP3 master (DNP3 Secure Authentication recommended)

게이트웨이는 DNP3, IEC61850통신을 제공하면서 프로토콜 변환을 수행할 수 있는 게이트웨이로 구성하였다. 게이트웨이의 동작은 기능별로인 DNP3통신모듈, IEC61850 통신모듈, 매핑 모듈을 각각 별개의 프로세스로 구성하는 방안을 선택하고, IPC(프로세스 간 통신)을 이용하여 필요한 정보를 주고받을 수 있도록 구성하였다. DNP3는 Turner Tech의 라이브러리를 사용했고, IEC61850은 SISCO의 MMS-EASE lite를 사용해 검증하였다. 이는 세 PC를 사용해 구축하였으며, DNP3 Master, 게이트웨이, IEC61850 Server를 각각 구현하였으며, 이들은 모두 Ubuntu 14.04 32bit 기반으로 검증하였다.

전체 시스템의 흐름은 Table 3.과 같다.

게이트웨이 구조에서 핵심부인 매핑모듈은 IEEE1815.1 표준을 근거로 하여 DNP3 Analog Input 형태의 데이터와 IEC61850의 하나의 변수를 1:1 매핑하였으며, 구현된 게이트웨이 검증을 위해 DNP3 로부터 Read Request를 받아 IEC61850이 구현된 MMS 모듈로부터 Read Response를 받을 수 있도록 설계하였다. 결과적으로 Fig. 5.와 같이 DNP3 Request 패킷을 받고 변환하여 MMS(IEC61850) 패킷을 전달하고, 다시 Response를 받아 매핑 후 DNP3 디바이스에 정상적으로 전달되었음을 보였다.

V. 결 론

본 논문에서는 국내 제어센터와 자동화 변전소 간 통신에서 IEEE1815.1 표준을 기반으로 DNP3와 IEC61850 간 이기종 프로토콜 변환 게이트웨이 구조를 제안하고, 검증 단계 수준에서 프로토콜 변환 게이트웨이를 구현하였다. DNP3와 IEC61850를 라이브러리를 활용해 동작시키고, 그 사이에서 실제 DNP3메시지와 IEC61850의 MMS메시지 간 데이터가 성공적으로 전송되는 것을 확인하였고, IEEE 1815.1 표준을 기반으로, 프로토콜 변환 게이트웨이로써 정상적으로 동작할 수 있음을 보였다. 더불어

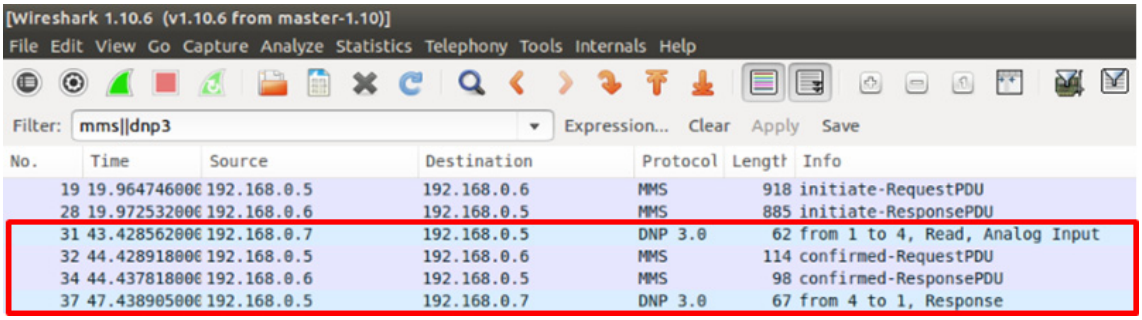

Fig. 5. Read Request & Response packet of Protocol Conversion Gateway

이러한 프로토콜 변환 게이트웨이의 보안 요구사항을 제시하였다. 향후에는 게이트웨이 양측 보안이 제공되는 경우 뿐 아니라 게이트웨이 자체적으로 보안성을 높일 수 있는 방법을 연구하여 DNP3 기기와 IEC61850 기기 간 End-to-End와 유사 수준의 보안을 제공해야 보다 안전한 연계 운용을 할 수 있을 것이다.

References

〔1〕 The World Market for Substation Automation and Integration Programs in Electric Utilities 2005-2007, Newton-Evans Research Company, Sep. 2005.

〔2〕 IEEE1815-2012(DNP3), IEEE Standard Association, https://standards.ieee.org/findstds/standard/1815-2012.html, Oct. 2012

〔3〕 IEC61850 Series (Part7-3:2010), International Electrotechnical Commission, http://www.iec.ch/smartgrid/standards/, Dec. 2010

〔4〕 IEEE1815.1-2015 Standard, IEEE Standards Association, http://standards.ieee.org/findstds/standard/1815.1-2015.html, May. 2016

〔5〕 DNP3 protocol, TurnerTech(sparky1194), https://sourceforge.net/projects/dnp/, Apr. 2013

〔6〕 MMS LITE-EASE, SISCO, http://www.sisconet.com/products/mms-lite/

〔7〕 Ubuntu 14.04, http://releases.ubuntu.com/14.04/, Feb. 2016

〔8〕 Byung-Kwen Song, Geonung Kim, "Design of the Gateway Function for DNP3.0 and IEC61850", Journal of IKEEE, 12(3), pp.151-157, Sep. 2008

〈저 자 소 개〉

이 석 준 (Seokjun Lee) 학생회원
2011년 2월: 아주대학교 정보및컴퓨터공학부 공학사
2011년 3월~현재: 아주대학교 대학원 컴퓨터공학과 석박사통합과정
〈관심분야〉 제어시스템 보안, 비정상행위탐지, 디지털 포렌식

권 성 문 (Sungmoon Kwon) 학생회원
2013년 2월: 아주대학교 정보및컴퓨터공학부 공학사
2013년 3월~현재: 아주대학교 대학원 컴퓨터공학과 석박사통합과정
〈관심분야〉 제어시스템 보안, 비정상행위탐지

손 태 식 (Taeshik Shon) 종신회원
2000년 2월: 아주대학교 정보컴퓨터공학부 공학사
2002년 2월: 아주대학교 정보통신전문대학원 공학석사
2005년 8월: 고려대학교 정보보호학과 공학박사
2004년 2월~2005년 2월: Research Scholar, University of Minnesota
2005년 8월~2011년 2월: 삼성전자 통신/DMC 연구소 책임연구원
2011년 3월~현재: 아주대학교 정보통신대학 사이버보안학과 부교수
〈관심분야〉 산업제어시스템 보안, 비정상행위탐지, 디지털 포렌식

박 성 완 (Sungwan Park) 정회원
1998년 2월: 연세대학교 전산학과 학사 졸업
2001년 2월: 연세대학교 전산학과 석사 졸업
2015년 3월~현재: 충남대학교 컴퓨터공학과 박사과정
2001년 3월~현재: 한전KDN 전력IT연구원 근무
〈관심분야〉 컴퓨터공학, 네트워크보안 정보보호, 전력제어보안