

Design of the Gateway Function for DNP3.0 and IEC61850

DNP 3.0과 IEC 61850 게이트웨이 기능 설계

Byung-Kwen Song*, Geonung Kim**★

송 병 권*, 김 건 응**

Abstract

The DNP3.0 and the IEC61850 are the most important standards in the SCADA systems for the power. Each standard has strength and weakness, so they will coexist for a while. This paper presents a design of the gateway function between DNP3.0 and IEC61850. Both standards use object-oriented modelling methods, so, they have some similarities. However, the DNP3.0 objects are described by object number and index, and the IEC61850 objects are described by name. So there should be mapping function between the object number and index of DNP3.0 objects and the object name of IEC61850 objects. We analyse the communication profiles of both standards, and shows the service-primitive mapping table and the procedure of the gateway function.

요 약

전력 설비를 감시하고자 하는 SCADA 시스템 표준으로 대표적인 프로토콜이 DNP3.0과 IEC61850이다. 두 표준은 각각의 특성과 장단점을 가지고 있으며, 따라서 상당 기간 두 표준이 공존할 것으로 예상된다. 본 논문은 두 프로토콜 간 변환 기능을 제공하는 게이트웨이 기능을 설계한 내용을 소개한다. 두 표준 모두 객체지향 모델링을 이용하여 유사점이 많지만, DNP3.0 객체는 객체 번호와 인덱스로 묘사되고, IEC61850 객체는 이름으로 묘사된다. 따라서 이들을 변환시켜주는 기능이 필요하다. 또한 각 표준의 통신 프리미티브를 분석하여 변환 가능한 프리미티브를 표로 정리하고, 게이트웨이 기능의 처리 절차를 제안하였다.

Key words : SCADA, DNP3.0, IEC61850, gateway function

1. 서론

전력 설비를 감시하고 제어하기 위한 SCADA (Supervisory Control And Data Acquisition)용 프로토콜 중 대표적인 것이 DNP(Distributed Network Protocol) 3.0[1][2][3]과 IEC61850[4-18][19]이다.

DNP 3.0은 1990년 IEC875-5에 기초하여 DNP1.0/2.0이 개발되었고, 1993년 DNP3 Basic 4 문

* 서경대학교 정보통신공학과

★ 교신저자(Corresponding author)

목포해양대학교 해양전자통신공학부

※ 본 연구는 서울시 산학연 협력사업(과제번호 : NT070064) 연구비로 수행되었음

接受日:2008年 8月 10日, 修正完了日: 2008年9月 29日

서가 발표되면서, DNP User Group이 결성되었으며, 현재 산업계의 사실상의 표준으로서 전기, 석유, 가스 분야에서 널리 사용되고 있다. 특히 DNP3.0은 북미 시장에서의 점유율이 높다. 이에 반해 IEC61850은 유럽에서 IEC TC57 WG10, 11, 12를 발족 한 후 IEC 60870, UCA 2.0 기술자들을 모아 개발한 프로토콜로서 북미를 제외한 다른 국가들에서 도입을 위한 고려가 가장 많이 되고 있는 프로토콜이다[20]. 국내에서는 DNP3.0과 IEC61850이 공존하는 환경이 예상되며, 따라서 이들 이기중 SCADA 시스템간 정보를 교환할 수 있는 기능이 요구된다.

본 논문은 현재 SCADA 시스템중 가장 높은 지지를 받고 있는 두 표준의 통신 기능을 비교 분석하고, 이를 통해 두 시스템간 정보 교환이 가능하도록 하는

게이트웨이 기능을 도출한다. 두 표준의 적용 대상이 동일하더라도 각 표준의 철학이나 특성이 상이하여 완전한 일대일 대응은 불가능하며, 따라서 서로간의 매핑이 가능한 기능 영역의 한계를 명확히 하는데 중점을 두었다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 DNP3.0과 IEC61850의 데이터 모델링을 비교하고, 다음 3장에서는 두 프로토콜의 통신 기능을 비교한다. 다음 4장에서는 정보 교환이 가능한 기능들을 정리하고, 변환 방안을 제시한 후 5장에서 결론을 맺는다.

II. 데이터 모델링 비교

1. DNP3.0의 데이터 모델링

DNP3.0의 응용계층의 APDU는 다음과 같다. 여기서 객체 헤더는 DUI(Data Unit Identifier)로서 뒤따라오는 데이터 객체를 식별하기 위한 헤더이며, 데이터에는 객체 헤더에서 규정된 형태의 IO(Information Object)들이 포함된다 [1][2].

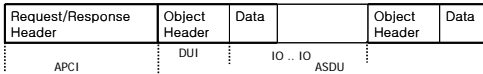


Fig. 1. Format of APDU of DNP3.0
그림 1. DNP3.0의 APDU 형식 [1]

DNP3.0 객체 헤더의 DUI는 객체 그룹(Object Group), 객체 변화(Object Variation), 한정값(Qualifier), 범위(Range)로 구성되는데, 여기서 객체 그룹은 일반적인 데이터 클래스를 의미한다. 객체 변화는 요청을 보낼 때는 0으로 설정되며, 응답시 특정한 타입에 따라 그것을 표현하게 된다. 예를 들면 요청에서는 Analog Input 으로 변화가 0으로 설정되어 전달되면, 응답에서는 16bits Analog Input으로 구체적인 형식에 대한 변화 값이 돌려진다. 한정값은 뒤에 나오는 범위 값의 의미를 구분하며, 범위에서는 인덱스의 시작값과 종료값을 가지고 있다.

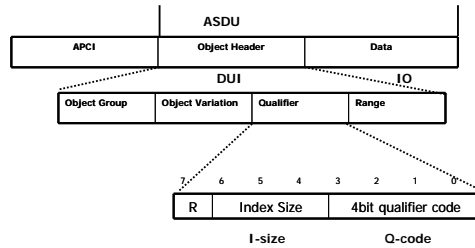


Fig. 2. Format of DNP3.0's Object Header
그림 2. DNP3.0의 Object Header 형식 [1]

DNP3.0에서의 객체 그룹은 서로 유사한 데이터 타입의 집합으로 볼 수 있다. 일반적으로 외부 스테이션 구현 시 동일한 타입을 갖는 데이터들을 배열 형태로 모아서 관리하고, 이러한 데이터를 요구할 때 데이터 타입과 범위를 지정하여 원하는 정보를 명시한다. 또한 이러한 객체들과 의미 정보를 외부 스테이션 장치 프로파일에 기술한다.

2 IEC61850의 데이터 모델링

IEC61850이 주목받고 있는 가장 큰 이유가 강력한 데이터 모델링이다. IEC61850에서는 각 기능을 하나 이상의 물리장치에 존재하는 LN(Logical Node)으로 분리한다. 이때 각 LN은 주고받은 데이터의 문법(syntax)과 의미(semantic)을 해석할 수 있어야만 서로 사용될 수 있는데, 이를 위해 응용에서는 3단계로 데이터를 모델링한다. 레벨 1 ACSI(Abstract Communication Service Interface)에서는 객체 모델로 구체화 되는 도메인 즉 SAS(Substation Automation System)의 항목을 접근하는데 사용되는 모델과 서비스로 구체화되는데, 이러한 모델과 서비스는 응용의 요구를 반영하여 적용한다. 이때 서비스는 응용의 객체 값을 읽거나 쓰는 기능뿐만 아니라 장비를 제어하는 기능도 수행한다. 레벨 2 CDC(Common Data Classes)에서는 하나 이상의 속성을 갖는 객체의 구조를 정의하는데, 이러한 속성들의 데이터 타입은 IEC 61850-7-1에 정의된다. 레벨 3 LN 클래스 및 객체 클래스에서는 CDC를 기반으로 하여, 기능 클래스와 데이터 클래스로 정의되는, 서로 호환이 가능한 객체 모델을 정의한다 [5][6][8][19].

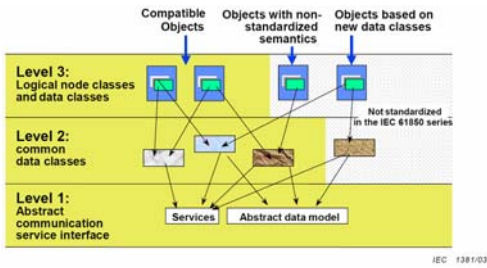


Fig. 3. IEC 61850's Data Modeling and Services
 그림 3. IEC61850의 데이터 모델링과 서비스[8][13][14]

IEC61850의 데이터 클래스는 의미 있는 정보들을 나타내며, SetDataValue로 쓰거나 GetDataValue로 읽을 수 있다. 또한 이들 데이터 클래스들을 표준화하고 있는데, [14]는 IEC [13]에 규정된 공통 템플릿(공통 데이터 클래스, CDC)을 기반으로 하여 공통 및 변전소 영역 고유의 데이터를 정의하고 있다.

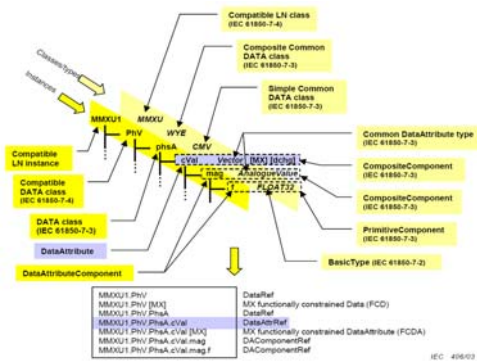


Fig. 4. Data Class Model of IEC61850
 그림 4. IEC61850의 데이터 클래스 모델[14]

3. 양 표준의 데이터 모델링 비교

DNP3.0 표준에서 객체 클래스는 일반적인 객체 타입으로 볼 수 있으며, 그 자체가 기능적인 의미가 있는 것이 아니다. 따라서 객체 클래스나 인덱스로 그 객체의 기능을 추론할 수 없다. 또한 DNP3.0의 외부 스테이션 구현 시 일반적으로 동일한 타입 즉, 동일한 객체 클래스에 속한 데이터를 배열 형식으로 저장한다. 따라서 데이터의 위치는 기능이나 데이터간 관계 등과 같은 의미적인 사항들이 고려된 것이 아니라, 구현의 편의성이나 자원(저장 공간 및 통신 대역)의 효율적인 이용에 초점이 맞추어져 있다.

이에 반해 IEC61850에서는 각 기능을 LN으로 분할하고 각 LN이 다시 객체로 분할되는 형태로 모델링함으로써 객체 클래스 자체가 의미를 가지며, 객체의 이름을 통해 그 객체의 기능을 추론할 수 있다. 특히 IEC61850은 장치에 대한 기술과 시스템 변수들을 호환성이 없는 IED 도구 사이에서 교환할 수 있도록 하는 SCL(Substation Configuration Language) [9]이 제공된다.

III. 통신 구조 비교

1. DNP3.0의 통신 기능

DNP3.0은 원래 OSI 7 계층 모델에서 3 가지 계층(물리 계층, 데이터 링크 계층 및 응용 계층)을 기반으로 하여 설계되었다. 응용 계층에서는 가장 일반적인 데이터 형태를 지원하기 위하여 객체를 기반으로 한다. 데이터 링크 계층에서는 클래스 및 객체의 변동을 폴링(polling) 하는 몇 가지 데이터 수집 방법을 제공한다. 물리 계층에서는 가장 일반적으로 사용되는 단순한 RS-232 또는 RS-485 인터페이스를 정의한다. 따라서 대역폭이 낮은 응용세어 효율적으로 동작하는데 중점을 두고 있다. 또한 확장된 RTU 기능들과 기본적인 프레임 크기(최대 16bytes)보다 더 큰 메시지(최대 255bytes)를 전송할 수 있도록 가상 트랜스포트 계층을 사용할 수 있으며, LAN 환경에서의 프로토콜 스택도 고려되어 있다[1][2]. 다음 그림은 DNS 시리얼과 DNP LAN의 프로토콜 스택을 보여주고 있는데, 원래 DNP 시리얼로 표준이 개발되고 나중에 DNP LAN이 개발된 관계로, TCP 또는 UDP 계층 위에 DNP 데이터 링크 계층이 있으며, 에러 제어 기능이 중복될 수 있는 문제점이 있다.

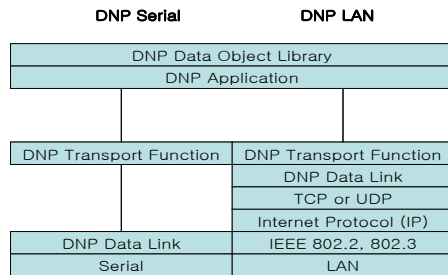


Fig. 5. Protocol Stack of DNP 3.0
 그림 5. DNP 3.0 프로토콜 스택[2]

DNP3.0의 응용 계층 메시지 교환은 2가지가 제공되는데, (1) 마스터에서 요청을 하고, 이에 대한 응답

을 외부 스테이션에서 보내는 방식과, (2) 외부 스테이션에서 감지된 변화를 스스로 보내는 방식이 있다.

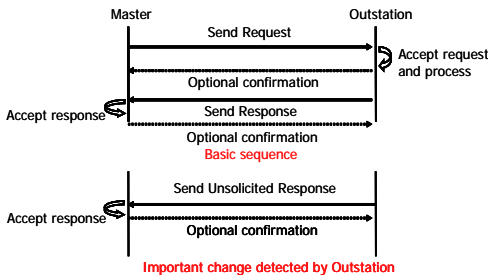


Fig. 6. Exchange of Application Messages in DNP 3.0
그림 6. DNP 3.0 응용 계층 메시지 교환[1]

다음 표는 DNP 3.0 응용 계층 SDU의 FC 코드를 보여준다.

Table 1. FC codes of DNP's ASDU
표 1. DNP의 ASDU FC 코드[1]

코드	Master	Slave
0x00	Confirm	Confirm
0x01	Read	Response
0x02	Write	Unsolicited Response
0x03	Select	
0x04	Operate	
0x05	Direct Operate	
0x06	Direct Op. No Ack	
0x07	Immediate Freeze	
0x08	Immediate Freeze No Ack	
0x09	Freeze and Clear	
0x0A	Freeze and Clear No Ack	
0x0B	Freeze with Time	
0x0C	Freeze with Time No Ack	
0x0D	Cold Restart	
0x0E	Warm Restart	
0x0F	Init Data to Default	
0x10	Initialize Application	
0x11	Start Application	
0x12	Stop Application	
0x13	Save Configuration	
0x14	Enable Unsolicited Messages	
0x15	Disable Unsolicited Messages	
0x16	Assign Class	
0x17	Delay Measurement	
0x18	Record Current Time	

2. IEC61850의 통신 기능

IEC61850의 통신 기능과 관련된 특징은 응용과 통신의 분리이다. 응용은 ACSI에 적합하게 통신을 하는데, 이를 위해서는 응용 계층 프로토콜에 알맞게 변환이 가능해야 하고, 통신 프로파일에 정상적으로 받

여되어야 한다. ACSI는 SCSM(Specific Communication Service Mapping)으로 매핑된다[4].

통신에서 이용하는 메시지 타입들을 다음 표 1과 같은데 특히 각 메시지 타입마다 엄격한 시간 제한이 설정되어 있다.

Table 1. Message Types and Time Constraint
표 1. 메시지 타입 및 시간 제한[15]

타입	설명	시간제한
Type 1	Fast message	100ms~20ms 이하
Type 1A	Trip	10ms~3ms 이하
Type 2	Medium speed message	100ms 이하
Type 3	Low speed message	500ms 이하
Type 4	Raw data message	10ms~3ms 이하
Type 5	File transfer functions	제한 없음
Type 6	Time synchronisation message	1ms~0.1μs 이하

다음 그림은 각 메시지들을 전송하기 위한 프로토콜 스택을 보여준다. 각 메시지 타입이 갖는 엄격한 시간 제한을 만족시키기 위해, 타입 1과 4의 경우 중간 통신계층을 거치지 않고 바로 이더넷(Ethertype)으로 매핑됨을 확인할 수 있다.

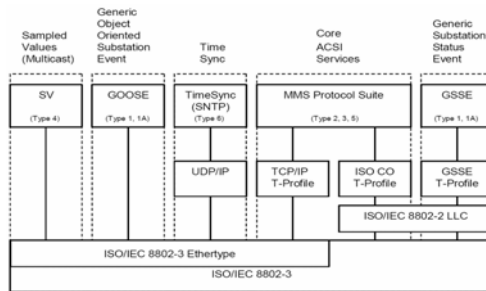


Fig. 7. SCSM of the IEC61850
그림 7. IEC61850의 SCSM 매핑[15]

다음 표는 IEC61850의 클라이언트-서버 모델과 통신 프로파일을 보여준다.

Table 2. Service requiring client/server communication profile

표 2. IEC61850의 서비스와 통신 프로파일 관계 [15]

IEC61850-7-2 모델	IEC61850-7-2 서비스
Server	GetSeverDirectory
Association	Associate, Abort, Release
Logical Device	GetLogicalDeviceDirectory
Logical Node	GetLogicaNodeDirectory, GetAllDataValues
Data	GetDataValues, SetDataValues, GetDataDirectory, GetDataDefinition
Data Set	GetDataSetValues, SetDataSetValues, CreateDataSet, DeleteDataSet, GetDataSetDirectory
Substitution	GetDataValues, SetDataValues
Setting Group Control Block	SelectActiveSG, SelectEditSG, SetSGValues, ConfirmEditSGValues, GetSGValues, GetSGCBValues
Report Control Block	Report, GetBRCBValues, SetBRCBValues, GetURCBValues, SetURCBValues
LOG Control Block	GetLCBValues, SetLCBValues, GetLogStatusValues, QueryLogByTime, QueryLogAfter
GOOSE	GetGoCBValues, SetGoCBValues
GSSE	GetGsBValues, SetGsCBValues
Control	Select, SelectWithValues, Cancel, Operate, CommanfTermination, TimeActivatedOperate
File Transfer	GetFile, SetFile, DeleteFile, GetFileAttributeValue

3. 양 표준의 통신 기능 비교

DNP3.0에 비해 IEC61850 표준이 보다 다양한 메시지 타입과 프로토콜 스택을 제공하고 있으며, 보다 엄격한 시간 제한을 두고 있다. DNP 3.0의 요청-응답 형태의 메시지 교환과 스테이션에서 스스로 보고하는 메시지는 IEC61850의 타입 3 메시지로 매핑될 수 있다. IEC61850에서 제공하는 SV(Sampled Values) 방식이나 GOOSE(Generic Object Oriented Substation Event) 방식에 대응하는 DNP3.0의 통신 기능은 존재하지 않는다.

IV. 게이트웨이 기능 설계

IEC61850-8-1에서는 클라이언트-서버 통신에서 필요한 서비스와 프로파일간 관계를 제시하고 있다. DNP3.0 게이트웨이는 이들을 다시 DNP3.0 서비스로 변환할 필요가 있는데, 그것은 다음 표와 같다. 표에 명시되지 않은 IEC61850 서비스들은 DNP 3.0 서비스로 변환이 불가능한 것들이다. 예를 들면, 여러 객체를 하나의 집합으로 설정하여 값을 가져오거나 변경하도록 하는 DataSet 관련 서비스와 그룹 설정 제어에 관련된 서비스들, 로그 관련 서비스, GOOSE와 GSSE(Generic Substation Status Event) 관련 서비스들은 DNP3.0 서비스로 변환할 수 없다.

Table 3. DNP3.0- Services mapping to IEC61850

표 3. IEC61850과 DNP 3.0 서비스 변환

IEC61850 모델	IEC61850 서비스	DNP3.0 서비스
Data	GetDataValues	Read
	SetDataValues	Write
Substitution	GetDataValues	Read
	SetDataValues	Write
Report Control Block	Report	Unsolicted response
	GetBRCBValues	Read
	SetBRCBValues	Enable/(disabled) Unsolicted Messages
	GetURCBValues	Read
Control	SetURCBValues	Enable/(disabled) Unsolicted Messages
	Select	Select
	SelectWithValue	Select
	Operate	(Direct) Operate

이러한 서비스 변환이 결정된 다음 처리되어야 하는 것이 IEC61850의 객체와 DNP3.0의 객체(인덱스) 간 변환이다. IEC61850의 객체는 구현과 독립적으로, 객체 이름 자체에서 기능을 추론할 수 있지만, DNP3.0에서는 이것이 불가능하며, 따라서 IEC61850의 객체에 대응하는 DNP3.0 객체의 인덱스를 저장하는 표를 생성하여야 한다. 각 장비마다 이러한 표는 따로 생성되어야 하며, 이를 자동으로 생성하는 도구의 개발도 고려할 수 있다.

IEC61850의 클라이언트-서버 모델 서비스들 중 위의 표에 나타난 서비스들은 다음 그림8과 같은 절차로 처리될 수 있다.

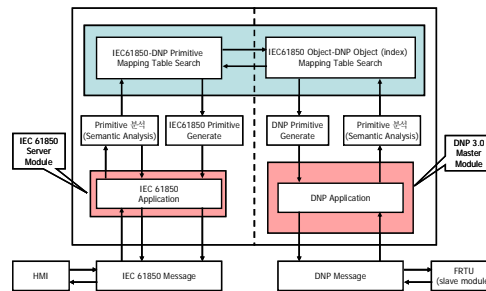


Fig. 8. IEC61850-DNP3.0 mapping procedure

그림 8. IEC61850-DNP3.0 변환 과정

여기서 서비스 변환이 가능한 것들은 변환 과정을 거쳐 RTU에게 서비스를 요청하고 그 결과를 응답으로 돌려준다. 이에 반해 서비스 변환이 불가능한 것들은 IEC61850 서버 역할의 동작으로 오류 메시지를

생성하거나 다른 처리를 할 수 있다.

DNP3.0에서는 슬레이브에서 스스로 사건을 보고하는 Unsolicited 메시지가 존재하는데, 그것들은 IEC 61850의 Report 서비스로 변환시켜 처리할 수 있다. 이런 사건보고 처리 과정은 다음 그림9와 같다.

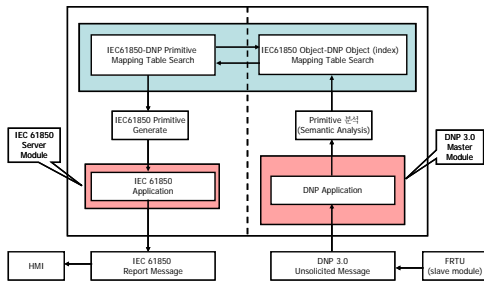


Fig. 9. DNP3.0 Unsolicited message mapping procedure
그림 9. DNP3.0 Unsolicited 메시지 변환 과정

V. 결론

전력 SCADA 시스템용 표준 중 대표적인 프로토콜들인 DNP3.0과 IEC61850은 각각의 장단점을 가지고 있으므로 상당기간 공존할 것으로 예상된다. 따라서 이들 표준을 적용한 기기들간 통신이 요구될 수 있는데, 본 논문은 이들 기기간 통신을 가능하게 하는 게이트웨이 기능을 제안하였다.

DNP3.0-IEC61850 게이트웨이 기능은 크게 둘로 나누어지는데, 하나는 객체간 변환이고, 다른 하나는 통신 프리미티브 변환이다. DNP3.0 객체는 객체 번호와 인덱스로 묘사되고, IEC61850 객체는 이름으로 묘사되므로, 이들을 변환시켜주는 기능이 필요하며, 두 표준의 통신 프리미티브들이 다르므로, 각각을 분석하여 변환 가능한 프리미티브들만을 표로 따로 정리하였다.

현재 본 논문에서 제안한 기능을 확인할 수 있는 게이트웨이 프로토타입을 구현 중이며, 구현된 결과를 현재 운용 중인 SCADA 시스템과 연계하여 실효성을 검증하는 작업을 진행할 예정이다.

참고문헌

[1] DNP User Group, "Distributed Network Protocol DNP 3.0 BASIC 4 DOCUMENT SET"

[2] DNP User Group, "DNP3 Protocol Primer"
 [3] www.dnp.org
 [4] IEC 61850-1, Communication networks and systems in substations - Part 1: Introduction and overview
 [5] IEC 61850-2, Communication networks and systems in substations - Part 2: Glossary
 [6] IEC 61850-3, Communication networks and systems in substations - Part 3: General requirements
 [7] IEC 61850-4, Communication networks and systems in substations - Part 4: System and project management
 [8] IEC 61850-5, Communication networks and systems in substations - Part 5: Communication requirements for functions and device models
 [9] IEC 61850-6, Communication networks and systems in substations - Part 6: Configuration description language for communication in electrical substations related to IEDs
 [10] IEC 61850-7-1, Communication networks and systems in substations - Part 7-1: Basic communication structure for substation and feeder equipment - Principles and models
 [11] IEC 61850-7-2, Communication networks and systems in substations - Part 7-2: Basic communication structure for substation and feeder equipment - Abstract communication service interface (ACSI)
 [13] IEC 61850-7-3, Communication networks and systems in substations - Part 7-3: Basic communication structure for substation and feeder equipment - Common data classes
 [14] IEC 61850-7-4, Communication networks and systems in substations - Part 7-4: Basic communication structure for substation and feeder equipment - Compatible logical node classes and data classes
 [15] IEC 61850-8-1, Communication networks and systems in substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) over ISO 8802-3
 [16] IEC 61850-9-1, Communication networks and systems in substations - Part 9-1: Specific Communication Service Mapping (SCSM) - Sampled values over serial unidirectional multidrop point to point link
 [17] IEC 61850-9-2:2002, Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC

8802-3 3

- [18] IEC 61850-10, Communication networks and systems in substations - Part 10: Conformance testing
- [19] Ralph Mackiewicz, "IEC61850 & ICCP-TASE.2 Technical Overview", SISCO
- [20] "Increases in Substation Related Automation and Integration Program Spending Reported by World's Major Electric Power Utilities", Substation Automation News March 2006

저 자 소 개

송 병 권 (정회원)

1995년 3월~현재 : 서경대학교
 정보통신공학과 교수
 <주관심분야>
 망관리시스템, SCADA 시스템,
 인터넷주소자원

김 건 용 (정회원)

1990년 : 고려대학교
 전자전산공학과 졸업 (공학사)
 1994년 : 고려대학교 대학원
 전자공학과 (공학석사)
 1998년 : 고려대학교 대학원
 전자공학과 (공학박사)
 1999년 9월~현재 :
 목포해양대학교 해양전자통신공학부 부교수
 <주관심분야>
 망관리시스템, SCADA 시스템, 인터넷주소자원