

Communication Protocols in Substation Automation and SCADA

Arash Shoarinejad, System Engineer

GE Energy Network Reliability Products and Services

Canada

SCADA, protocols, automation, networking, communication

Abstract

The paper provides a brief explanation of the automation and SCADA industry along with networking schemes. Protocols as a crucial part of the system are explored in depth. In addition, commonly used protocols and standards are mentioned concisely. The newest invention of the IEC standards committee, known as IEC 61850, is also introduced. IEC 61850 and UCA have promising advantages over other protocols and will greatly change SCADA systems today. Also, a general guideline is provided for protocols, which is then used to create a comparison chart for them.

Communication Protocols in Substation Automation and SCADA

Arash Shoarinejad, System Engineer,

GE Energy Network Reliability Products and Services

Canada

SCADA, protocols, automation, networking, communication

1.0 Introduction

Electricity in today's world has become a very important source of energy. It is widely used and is vital to the social and economic life of any country. The electrical infrastructure (e.g. generation plants, transmission lines, substations, etc.) requires real-time monitoring and protection in order to be able to provide energy to all consumers. SCADA provides the means for control and supervising large electrical networks. In addition, the communication and protocol issues in SCADA are extremely important as they determine the form and speed of data in a SCADA network. In this paper, Automation and Communication Networks are briefly discussed. Later, the most frequently used protocols in today's SCADA systems from North America to Asia are introduced. It is important to note that each protocol mentioned in this paper is based upon a concept which cannot be completely explicated. This paper is intended to merely introduce each protocol and their advantages and disadvantages. IEC 61850 is also introduced as the newest and most advanced protocol.

2.0 Automation and SCADA

As industrial economies grow and become more efficient they also become more reliable on electricity as their main source of energy. Hence, a blackout in electrical system causes massive damage to social and economic aspects of a society. To prevent interruptions and to provide energy to electricity consumers reliably automation needs to take place at each stage of the electrical system: generation, transmission, and distribution. As each stage is automated, there has to be reliable, fast, and efficient communication amongst devices and the SCADA control center. Communication lines need to carry information and data between substations and control centers at different parts of the network so that monitoring and automation of the system can occur. Without adequate communication amongst devices SCADA system will render itself useless and will not be able to provide the reliability and efficiency needed in today's electricity markets.

It is also important to note that automation in electrical systems allows for the system control and operator to define specific performance and protection parameters, which will lead to consistency across the

electrical grid. For example, digital fault recording using automated networks can assist the system operators locate and correct faults in the system very quickly. An automated network will begin recording fault records (as per pre-determined standards) at all locations of the electrical system. Then, all the records will automatically be sent to the SCADA control center in an organized and in digital format for review. Automation can also assist with interlocking schemes, load shedding, transformer monitoring and diagnostics, voltage control, and many other areas of importance.

3.0 Communication Networks

A network is an interconnected system of electronic devices which share information with each other. A network provides the media in which the information is transferred from one location to another. It is also the vein or bloodline of any SCADA system, so its speed, reliability, and efficiency are absolutely crucial. There are many types of networks, but only two types apply to substation environments and power systems: Serial-

based and Ethernet-based. Ethernet-based systems in power systems are also referred to as Integrated Substation Control Systems (iSCS). There are many standards for each type of networks; however, in substation automation RS-232 (point-to-point links) and RS-485 (multi-drop links) in serial networks and IEEE 802.3 in Ethernet systems are the most common. Serial communication standards were designed in early 1960's and can provide links up to speeds of 10 Mb/s and for distances of a maximum of 1200 meters. It is noted that in computers and today's electronic devices speeds are usually limited to 115.2 Kb/s in serial links. For higher speeds Ethernet-based systems are used. Ethernet systems are much faster and provide greater capabilities than serial systems where speeds of 1 Gb/s and distances of 4 km have been achieved. There are multiple Ethernet operating systems designed over the years such as Novell Netware, OS/2 LAN manager, TCP/IP, and Banyan Vines [1].

Referring to Appendix A, part of a large typical SCADA network is shown for a 330 kV line in Italy. There are two Local Area Networks (LAN) present in this substation and each device is connected to both for redundancy

purposes. There are Intelligent Electronic Devices or IEDs (such as GE D25) connected to the protection relays (such as GE UR Series) which provide information to the SCADA center and automate tasks locally. Services such as load shedding and fault recording is accomplished at this level. Remote Terminal Unit (RTU) acts a concentrator and gateway of information to the Energy Management System (EMS) or SCADA Control Center. The LAN shown in Appendix A is also connected to a Wide Area Network (WAN) where external devices such as remote operating units can access the data present on the network. The most important observation is that a link is created amongst all devices that provides reliable highway of information and fast networking capability.

3.0 Protocols

A protocol is a set of formal rules describing how to transmit data across a network. The rules could be low-level, which define the electrical and physical standards to be observed, bit- and byte-ordering and the transmission and error detection and

correction of the bit stream. In this section the high-level protocols will be discussed which describe the data formatting, including the syntax of messages, character sets, and sequencing of messages. In short, a protocol is a predefined digital language. The following figure shows the communication in hexadecimal format between a GE D25 device and UR relays through an IEC protocol. The Bold message is D25's request for information and the Italic message shows the response of the UR relay with the data required.

```

10 49 0A 53 16 10 47 0A 51 16 10 5B 01
5C 16
68 16 16 68 28 01 09 07 02 01 02 01 02 00
02 00 02 00 02 00 02 00 02 00 02 00 CD
16
10 7A 01 7B 16
68 10 10 68 28 01 CD 81 01 01 01 01 85
25 00 00 00 00 00 00 7F 16
10 5A 01 5B 16

```

The need for a protocol is quite apparent. In any power system there are many devices from different countries and made by different manufacturers which perform different tasks in SCADA. In order to create a communication network a common 'language' or protocol is needed.

There are many committees and associations who have designed protocols for the power industry. Overall there are over 300 different protocols in today's substation environment but there are only a few that are popular and are accepted by major manufacturers.

3.1 General Properties of Protocols

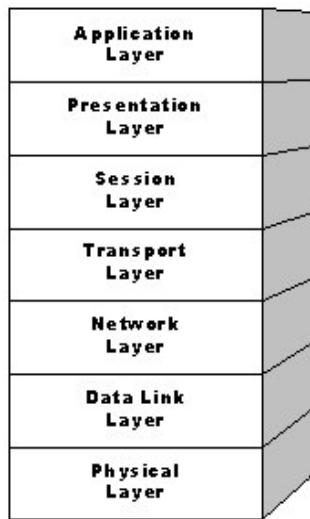
Some of the protocols used in power systems are Modbus, HR600/XA-21, DNP 3.0, IEC 60870-5-101/103/104, IEC 61850, UCA 2.0, INCOM, 8979, Cooper 2179, and Conitel. In order to differentiate between protocols and compare them some general guidelines need to be defined. The properties could be generalized as the following:

- a) *Network compatibility* – some protocols have only been defined to operate in serial networks such as Conitel. On the other hand, some protocols have been defined to work both on Ethernet and Serial systems such as DNP 3.0
- b) *Speed* – the speed at which a protocol transfers information amongst multiple

- devices is a very important measure of its performance.
- c) *Reliability* – the transfer of information has to be reliable. Some protocols may have checks in place to ensure proper communication of messages. The level of reliability is another important measure of a protocol's performance.
 - d) *Expandability* – protocols need to be able to handle small, medium, and large systems in SCADA. For example, DNP 3.0 is able to handle very large system with over 65,000 data objects, whereas, Conitel or Cooper protocols will not handle such large amounts of information well.
 - e) *Security* – in today's information age the security of information has to be ensured or else information may be hacked or hampered during its transfer through the network. The protocol's level of security and encryption of data are important issues in power systems.
 - f) *Acceptability* – a protocol needs to be accepted in the power industry and by the equipment manufacturers. Protocols that are unique to specific manufacturers and are proprietary cannot be the common 'language' in a SCADA system. When choosing a protocol one needs to determine whether all the components of the power system are able to communicate in that specific protocol or not.
 - g) *Simplicity* – It is important for a protocol to be simple so that its users can configure and maintain SCADA systems easily and without the need for special expertise. The number of features and functionalities should be limited to provide an economic solution for manufacturers and consumers.
 - h) *Consistency* – a protocol has to be controlled and standardized by one committee in the world to provide consistency.
 - i) *Functionality* – a protocol should have all the features and functions used in SCADA such as time synchronization and file transfer.
 - j) *Economics* – a protocol should be economic as its costs will determine its future in power systems.

3.2 Introduction to Protocols

All modern protocols are based upon Open System Interconnection (OSI) model. OSI is an ISO (International Organization of Standardization) standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy [4]. The following figure from [5] shows the seven OSI layers.



Refer to Appendix B for an explanation of each layer and its functions. In the following sections some of the most accepted protocols around the world have been introduced along

with a section dedicated to the introduction of IEC 61850. Appendix C contains a chart which uses the aforementioned protocol guidelines to compare them to each other.

I) Modbus Protocol

It is one of the oldest protocols in the industrial environment and was designed by Modicon for programmable logic controllers (PLC). It is easily implemented, widely accepted, and offered by most manufactures. Modbus defines an application layer messaging protocol, positioned at level 7 of the OSI model that provides "master/slave" communications between devices connected in a network [6]. It is based on a simple addressing scheme, which limits its expandability in a distributed SCADA network. In fact, the Modbus protocol is based upon a network where there is one Master Station with Multiple Slave devices. Therefore, it has great advantages in simple serial networks where there is not a lot of information being exchanged. The Master Station reads registers by their addresses one by one, which consumes a lot of bandwidth. Many

users and suppliers have modified the protocol over the years to create Modbus Plus, Modbus RTU, and Modbus TCP/IP. Unfortunately, there is not one internationally accepted committee to provide consistency across different suppliers. But overall, the protocol is the most available amongst devices [7].

II) DNP 3.0 Protocol

Distributed Network Protocol (DNP) 3.0 was developed by a division of Harris (which is now owned by GE Energy) in 1993. It is based on the OSI model and it is an open and public protocol. It is built for small to medium size systems and can handle over 65,000 addresses over one link. It is now controlled by the DNP Users Group located in North America, which provides consistency over its suppliers with certification programs. It is also widely available. DNP was designed to optimize the transmission of data acquisition information and control commands from one device to another in a substation environment [8]. The data (e.g. binary input/output, analog input/output, etc.) is transmitted in arrays or

blocks indexed from 0 to N, as a pose to some protocols such as Modbus that use single addressed registers. Therefore, DNP is very fast and efficient in communication networks both serial and Ethernet. It also allows for some advanced features such as time synchronization and configuration file transfers [9].

III) IEC 60870-5-Series Protocols

International Electrotechnical Commission (IEC) in collaboration with ISO has been very active in creating international standards for SCADA protocols. The IEC technical committee 57 (Power system control and associated communications) designed IEC 60870-5-series for telecontrol equipment and systems in 1990's [2]. It has five basic sections: IEC60870-5-1 (Transmission frame formats), IEC60870-5-2 (Link transmission procedures), IEC60870-5-3 (General Structure of application data), IEC60870-5-4 (Definition and coding of application information elements), and IEC60870-5-5 Basic application functions. Using these sections the IEC has created companion

standards 60870-5-101 (standard for basic telecontrol tasks and RTUs), 60870-5-102 (standard for the transmission of integrated totals in electric power systems), 60870-5-103 (standard for the informative interface of protection equipment), and 60870-5-104 (network access for IEC 60870-5-101 and 103 using standard transport profiles) [3]. In addition, the 104 companion is the only standard defined to work on Ethernet, whereas the rest of them operate in serial networks only. These standards are well defined and provide many forms of reporting mechanisms in SCADA. In fact, DNP 3.0 is based on an earlier version of the IEC 60870-5 so they are quite similar.

IV) IEC 61850/UCA 2.0 Protocol

Introduction

In order to promote and facilitate interoperability between computer systems supplied to the utility industry, EPRI (Electric Power Research Institute) initiated the Integrated Utility Communication (IUC) program. The UCA project began in November 1988 as the first of a series of

projects under this program. As the need for a unified standard became clear, the IEC solicited member bodies for contributions to be considered for international standardization. The lack of a consensus standard in the USA, as well as the perceived limitations of all of the existing candidate protocols, led to the formation of an utility/vendor task force sponsored by EPRI and others. This task force led the development of the Inter-Control Center Communications Protocol (ICCP). The name was later changed to Telecontrol Application Service Element 2 (TASE.2), and standardized as IEC 60870-6. TASE.2 is focused on the exchange of real-time data between EMS and SCADA databases, as well as power plant Digital Control Systems (DCS), and large-scale substation hosts such as data concentrators. TASE.2 does not (as currently defined) directly include formal field device models. The data is instead represented in the traditional form of point lists of each of the various point types, independent of the actual physical device at which the data originated. Support for time-tagged events, such as sequences-of-events (SOE), is not included in the specification, resulting in a complicated work-around when this type of information is

required. While the development of TASE.2 was in progress, aimed at inter-control center communication, EPRI was also sponsoring work on device models designed for communication with field devices. As a result, UCA has become a combination of the TASE.2 specification and the Generic Object Models For Substation and Feeder Equipment (GOMSFE) specification. IEC 61850 is in fact a more generalized form of UCA 2.0, but both share the same foundation [10]. Within the UCA framework, the definition of the data and control functions made available by the device, along with the associated algorithms and capabilities, is known as the device object model. A number of efforts were initiated to develop detailed object models of common field devices, including definitions of their associated algorithms and communications behavior visible through the communication system. An EPRI sponsored Forum provided an open and democratic process that enabled participants to create, debate, and critique the technology. The results of these efforts are contained in the Generic Object Models for Substation and Feeder Equipment (GOMSFE) document that creates a standard model or points list for transformers, circuit breakers, etc. In IEC 61850 the information exchange

methods to access the data (e.g. SOEs, historical data, control devices, and sampled value distribution) of the information models is very advanced and provide many options for the users and system operators. It also has a form in which fast peer-to-peer process data exchanges can take place (called Generic Object Oriented Substation Event or GOOSE). GOOSE is used in protection schemes very widely as it is capable of transferring substation information between protection relays in less than 1 ms. GOOSE operates in the TCP/IP network using Media Access Control (MAC) addresses and not IP addresses making it the fastest protocol in the substation environment.

The most important advantage of IEC 61850 is its use of unified system configuration language (XML based) and device online self-description. In other words, in an IEC 61850 SCADA network the idea of 'plug-and-play' becomes possible, as there is no need to configure master stations, HMI, or EMS. The protocol allows for description of data points and objects to be transferred to the master station over the network. Therefore, once all the slave devices are online, the master station can retrieve their configurations and configure itself automatically. The result is

much improved accuracy and reduced configuration and debugging time in SCADA networks. The main disadvantage of the protocol is mainly its complexity and worldwide acceptance. In fact, many of the manufacturers have not yet designed their devices to be IEC 61850 compliant. However, this protocol has the most futuristic view and can be the defining protocol of tomorrow's SCADA systems.

4.0 Conclusion

SCADA networks in any power systems are the main source of supervision and control to ensure reliable electricity supply to the consumers. Furthermore, the protocols that define the format of the digital information exchanged between SCADA control centers and its RTUs on different sections of a power grid are extremely important. The protocols determine the effectiveness of a SCADA system. Therefore, many protocols have been produced over the years to accommodate this need. IEC 61850 with its self-description and security enhancements has the most promising outlook in the protocol

future. It is a work-in-progress which should eventually dominate the electrical industry.

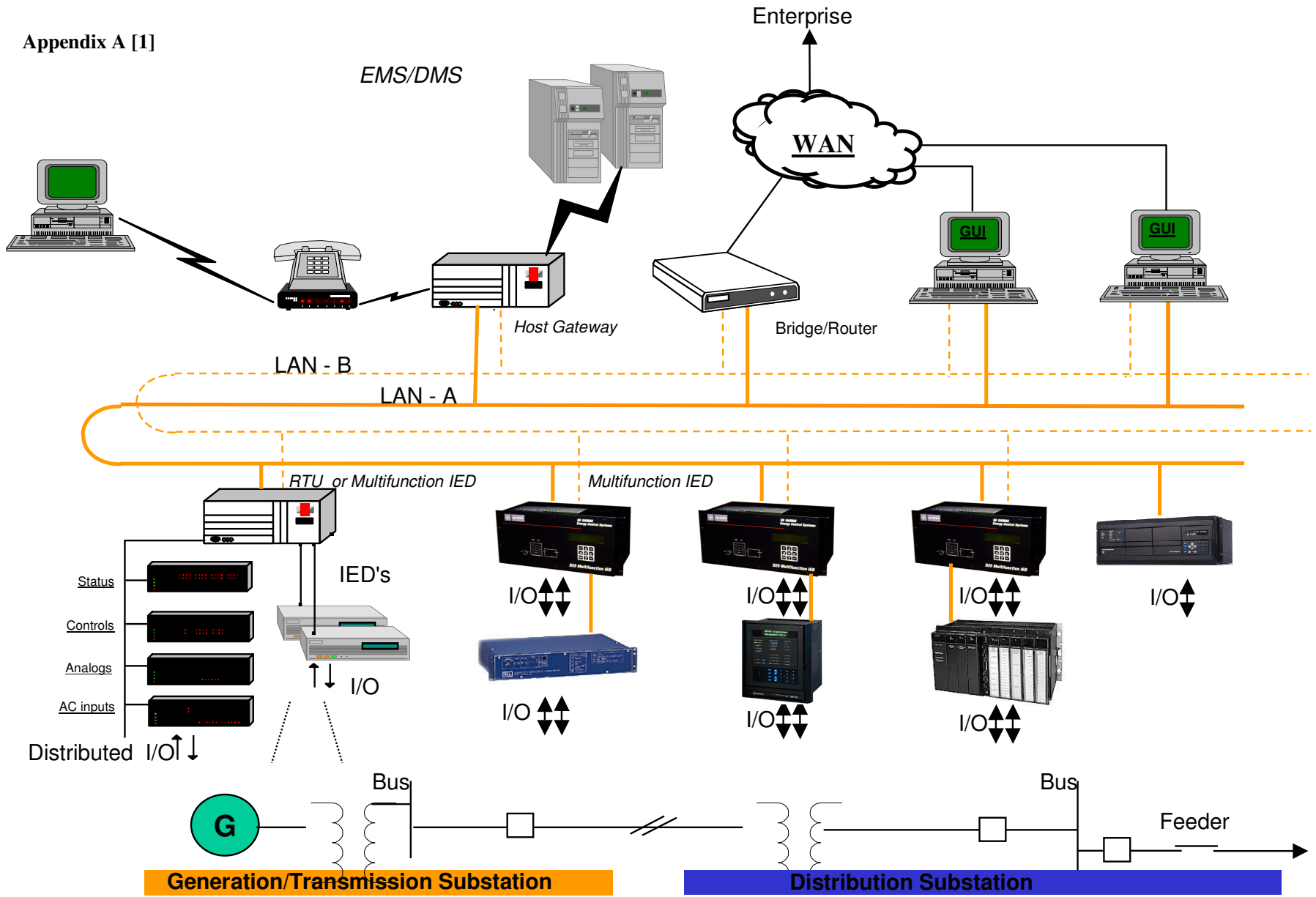
5.0 References

- [1] GE Energy Services, "Integrated Substation Control Systems and DNP 3.0 over Ethernet", Volume 4, SSD0009, 2002, pg. 12.
- [2] IEC Website, <http://www.iec.ch/>, July 2004.
- [3] GE Energy Services, "Integrated Substation Control Systems and IEC 60870-5-104", Volume 1, SSD0009A, 2002, pg. 10-60.
- [4] Computer Dictionary, <http://www.webopedia.com/TERM/O/OSI.html>, July 2004.
- [5] GE Energy Services, "Utility Communication Architecture (UCA) 2.0", Volume 1, SSD00016, 2003, pg. 9-25.
- [6] Modbus.org, "MODBUS over Serial Line Specification & Implementation guide", Volume 1, 2002, pg. 4-6.
- [7] GE Energy Services, "Modbus DPA Functional Specification", Volume 2.24, A068-0FS, 2002.
- [8] DNP Users Group, "A DNP3 Protocol Primer", June 2000, pg. 5-10.

[9] GE Energy Services, "DNP3 DPA Functional Specification", Volume 4.6, B021-0FS, 2003.

[10] GE Energy Services, "UCA & GE Energy Systems: An Introduction", Volume 1, SWM0024, Jan. 2002.

Appendix A [1]



Appendix B

- a) *Application* – is responsible for providing the window, or access, to the services provided by the communications architecture. It also provides services for task-specific functions of a protocol, such as monitoring and control of utility equipment.
- b) *Presentation* – provides for the common representation of data between end systems through the use of abstract syntaxes describing the data types and acceptable values to be transferred, and the use of transfer syntaxes.
- c) *Session* – provides services to organize and manage connections between end users such that data and control information are transferred in an organized and synchronized manner, by providing mechanisms to establish, maintain, resume and terminate session connections.
- d) *Transport* - is responsible for the end-to-end delivery of data packets between communicating session entities, using the routing services of the network layer and adding functionality for moving the data efficiently, insuring its correctness and order.
- e) *Network* – provides the routing and relaying of data between the communicating systems to dynamically determine the topology of the network, and use that knowledge to deliver the data to the proper end system.
- f) *Data Link* - is generally responsible for the error-free transmission of data between two adjacent systems by performing such functions as error checking and recovery, sequence checking, media access control, and flow control.
- g) *Physical* – provides a data path between nodes over some form of physical media. Specifies the characteristics of the media, and the nature of the signaling used.

Appendix C

All the protocols are given a score of 1 to 10 in each category. 1 is the lowest or most deficient and 10 is the highest score. The numbers are based on experiences in medium and low voltage substations and automation systems. It is noted that the numbers are not statistical values and were not measured, but they are based on the opinion of the system engineering team at GE Energy.

Protocol Name	Network Compatibility	Speed	Reliability	Expandability	Security	Acceptability	Simplicity	Consistency	Functionality	Economics
Modbus	5	2	9	2	2	9	8	4	3	9
DNP 3.0	8	9	9	6	3	7	7	9	6	8
IEC 60870-5	8	8	7	8	5	6	5	7	7	6
IEC 61850	9	6	9	9	6	2	2	N/A	9	3