# Automating Electric Substations Using IEC 61850

**Peter J. Hawrylak , Jeyasingam Nivethan and Mauricio Papa**

**Abstract** The Smart Grid will enhance the generation, distribution, transmission, and use of electricity by incorporating elements that will greatly help improve energy efficiency. In addition to traditional components, it will also incorporate small-scale generators, such as home wind turbines and solar panels, into the larger grid. In order to enable energy efficiency as well as other features, two-way communication between utilities and customers (users) will be required. This communication will most likely travel in large part over public networks. The Smart Grid, through the addition of bi-directional communication links throughout the infrastructure, will enable utilities to enhance their service, monitoring, and maintenance activities. Electric power substations will play a major role in the Smart Grid. IEC 61850 is a family of standards that defines network protocols, and data and device naming conventions for electric substation automation. IEC 61850 provides utilities with the ability to better monitor operation and even remotely control the substation when necessary. Part of the utility-substation communication link will be facilitated by public networks (e.g. the Internet). This chapter provides an overview of the IEC 61850 standards and discusses recent experiences with IEC 61850. Challenges facing IEC 61850 deployments, namely security, are presented. Potential solution paths to these challenges are provided.

**Keywords** IEC 61850 · Smart grid · Security · Automation · Ethernet

P. J. Hawrylak (✉)
Department of Electrical Engineering, University of Tulsa, Tulsa, OK, USA
e-mail: peter-hawrylak@utulsa.edu

J. Nivethan · M. Papa
Tandy School of Computer Science, University of Tulsa, Tulsa, OK, USA

V. Pappu et al. (eds.), *Optimization and Security Challenges in Smart Power Grids*,
Energy Systems, DOI: 10.1007/978-3-642-38134-8_6,

# 1 Introduction

Modern electric distribution and transmission systems are complex and must respond to varying customer consumption patterns. The purpose of the transmission system is to transfer the electricity generated at the power plants to the customer (end user). Substations are positioned between the power plant and the customer to help distribute electric energy. The power plant-to-substation link is typically constructed using very high voltage lines in order to minimize the current flowing through the lines, thus, reducing power loss due to the resistance of the lines. Customers require low-voltage power, on the order of 120 VAC at 60 Hz in the United States, and the substation provides the conversion from high-voltage to low-voltage that are more suitable for final distribution to customers. In larger distribution networks there may be a series of substations, each stepping the high-voltage output of the power plant to a lower voltage for transmission to the next substation. Ultimately, a substation provides electricity to a group of customers.

Substations are often located in remote, rural, or difficult to access locations because electricity must be provided to each customer at the location where it is needed. Therefore, the cost of sending an engineer or technician to a substation can be significant and utilities would like to reduce the number of times an engineer or technician must visit a substation. In addition, this service model prevents utilities from making real-time changes to the operation of the substation. Inability to make real-time operational adjustments prevents the substation, and by extension, the electric grid from instantly responding to changes in electric demand. Real-time control and updates of device operating settings to optimize electricity delivery and use are two of the major benefits of the next-generation electric grid, termed the *Smart Grid*.

Previously electricity was provided to the electric grid only by power plants operated by electric utilities and flowed in one direction: power plant to end-user. Communications throughout the grid, for the most part, were also unidirectional in nature. With the advent of small-scale generation, such as solar panels and small wind turbines, end-users can generate their own electricity. The Smart Grid will enable end-users to sell excess energy back to the utility. This requires an electric grid and control system that supports a bidirectional flow of electricity between utility and end-user. To determine how to handle this bidirectional flow of electricity, the Smart Grid must be informed when users will push electricity onto the grid and this requires bidirectional communication between the utility and the end-users. The Smart Grid will utilize bidirectional communication links between end-user and utility to manage and control the flow of electricity. Many different types of communication technologies will be used to construct the communication infrastructure of the Smart Grid. An overview of the communication technologies that could be used in the Smart Grid is provided in Wang et al. (2011). Substations will play a key role in the Smart Grid by adjusting the amount of electric power they provide in response to current demands and the amount of customer generation (e.g. excess power from solar panels) provided to the grid. These types of functional requirements will in turn require the substation and substation equipment to be interconnected to coordinate action for normal substation operation, receiving updates from the utility, and receiving information from end-users.

Substations in the Smart Grid will employ local area networks (LANs) to connect internal devices together to reduce construction and management costs. The Smart Grid offers utilities an increased level of control and remote operation of substations. The shift from direct point-to-point connections to a LAN environment requires reevaluation of the operating and security guidelines and best practices. Remotely controlling substations requires enhanced safety systems that can take over control during faults or unknown conditions to maintain safe operation of the substation and maintain the Smart Grid (Myrda and Donahoe 2007).

The Smart Grid will consist of a number of different network technologies and devices. Interoperability is a key requirement for the Smart Grid. Interoperability can be provided by standardizing how data is presented and communicated. Efforts in this area are underway within the IEEE, US National Institute of Standards and Technology, and the International Electrotechnical Commission (IEC). An overview of the various standards being developed within these groups is provided in Wang et al. (2011).

The IEC 61850 family of standards provides guidelines to implement communication within the substation and between the electric utility and substation. Thus, the IEC 61850 standards enable the automation of substation control from a central location. This automation provides the ability for the electric utility to respond to changing conditions in real-time and achieve one of the primary requirements for the Smart Grid. However, this automation or remote control introduces a number of issues that must be addressed in order to provide a safe and reliable Smart Grid. This chapter explores these issues. First, an overview of the IEC 61850 family of standards is presented, followed by a discussion on how substations can be automated using the IEC 61850. Next, the challenges in achieving and maintaining the remote control substation are discussed and potential solution paths to address these challenges are presented. The chapter concludes with a presentation of the necessary future work and research directions in this area.

## 2 Brief Overview of IEC 61850 Standards

The IEC 61850 standard is divided into ten parts with some parts having multiple sub-parts. A number of other technical reports are included with these parts. These technical reports provide additional information about the application of IEC 61850 and some include descriptions of IEC 61850 use-cases or potential implementations. Brief summaries of the technical reports follow the overview of the standards.

IEC 61850-1 provides an introduction and overview to the IEC 61850 family of standards. The introduction covers basic information about protection, control, and monitoring needs for electric; it is not a comprehensive overview of electric protection, control, and monitoring. The goal of this part is to introduce the fundamentals of IEC 61850 and provide illustrative diagrams and figures.

IEC 61850-2 contains the glossary of terms used in IEC 61850. This document houses these definitions for the entire family of standards and is updated as needed when other parts are updated or modified.

IEC 61850-3 contains the basic operating requirements for the IEC 61850 network. These include quality, security, environmental conditions requirements, and voltage requirements for the communication network.

IEC 61850-4 describes the system and project management aspects of IEC 61850. This includes quality assurance, beginning with the design stage, and engineering requirements. This part provides management guidelines for the entire life cycle of the system from design through decommissioning.

IEC 61850-5 explains and identifies the communication requirements of the all known tasks (functions) performed in the substation automation system (SAS). This part covers the lower level of the communication stack and is intended to be flexible to accommodate a range of devices and expandable to adapt to new networking technologies. Descriptions of the logical node concept and performance requirements for the network are also provided.

IEC 61850-6 describes the substation configuration language (SCL) that is used to initialize and describe devices within the substation. The SCL is used to describe the communications between devices, and the relationship between devices and functions performed by the substation.

IEC 61850-7-1 explains the basic communication architecture among the devices. It provides the communication modeling methods, modeling concepts, communication principles and the information models discussed in IEC 61850-7-x documents. Communication modeling methods, modeling concepts, communication principles and the information models used in the remaining subparts of IEC 61850-7 are described. Data formatting information is provided to enable interoperability between devices.

IEC 61850-7-2 describes and explains the abstract communication service interface (ACSI) that is used for the substation commination in the IEC 61850 model. ACSI is defined to be protocol agnostic and provides the basis to build the IEC 61850 protocol. This abstract interface provides services for (1) communication between the client and a remote device; (2) the transmission of messages using the publisher/subscriber method; and (3) the transmission of sampled values using the publisher/subscriber method. In the publisher/subscriber method, the each device monitors the network for messages to which it subscribes (that are of interest). Each message contains publisher and identification information so that the subscribers can identify those messages as being of interest.

IEC 61850-7-3 specifies common data classes and common attribute types for substation applications. The data classes and common attributes are used to define communication between applications.

IEC 61850-7-4 defines naming conventions for logical nodes and data structures used in the IEC 61850 model. The standardized naming convention is central to providing interoperability between devices and enabling information sharing.

Several standards and technical reports (denoted by a TR in the IEC standard name) have been published or are under development (IEC 61850-7-x10 and IEC

61850-7-x20) to provide extensions of the IEC 61850 naming and data format conventions to applications outside of the substation. Extensions to distributed energy resources (IEC 61850-7-420) and hydroelectric facilities (IEC 61850-7-410 and IEC/TR 61850-7-510) have been published.

IEC 61850-8-1 defines and explains a method for mapping the ACSI messages to Manufacturing Message Specification (MMS) messages in order to transfer non-time critical data through local area networks, and a method for mapping ACSI to Ethernet in order to transfer time critical data through local area networks.

IEC 61850-9-1 has been withdrawn and was replaced by IEC 61850-9-2. IEC 61850-9-2 defines and explains the specific communication service mapping (SCSM) of sample values to Ethernet. This standard describes how to take the ACSI model defined in IEC 61850-7-2 and convert those data items for transmission over Ethernet.

IEC 61850-10 defines the conformance requirements for IEC 61850 installations. This standard defines the tests and pass/fail conditions for determining conformance to IEC 61850.

Technical reports having the numbers IEC/TR 61850-90-x describe how to use IEC 61850 and provide additional information about implementation. Two technical reports have been published, IEC/TR 61850-90-1 covering communications between substations, and IEC/TR 61850-90-5 covering how to transmit synchrophaser data using the IEEE C37.118 standard.

## 3 Substation Automation with IEC 61850

The IEC 61850 series of standards defines how data is represented, the network protocols for transmitting the data, and the network requirements for substation automation. The benefit of IEC 61850 is that it helps replace the dedicated connections to each device with a single Ethernet connection. This provides significant savings in cable cost and more sophisticated functionality provided by more advanced devices capable of interacting with any other device in the substation.

The communication infrastructure utilized by the current power grid is composed of dedicated point-to-point connections between a local controller and the device. Networks based on this type of topology do not scale well and are limited to small geographic areas (Wang et al. 2011). An IEC 61850 based Smart Grid will use a different topology that is similar to what is often seen in current LAN designs and deployments, most likely based on Ethernet. In fact, current versions of IEC 61850 use Ethernet (Ozansoy et al. 2009) as the network infrastructure although the protocols defined by IEC 61850 could be transported using a number of other network infrastructures. Such a network can be connected into the same network that is used for providing Internet connections to business and private homes.

IEC 61850 defines the network protocol for intelligent electronic devices (IEDs). IEC 61850 focuses on Layers 5 (session), 6 (presentation), and 7 (application) of the OSI (Open Systems Interconnection) model (Forouzan 2003). One of the goals of IEC 61850 is to provide a mechanism to describe data and control commands independently from the underlying network (Mackiewicz 2011). To accomplish this, IEC 61850 defines the data format for the messages and the data labels in each message. Each message is constructed at the higher levels in the IEC 61850 format and is then translated and encapsulated by the network infrastructure into the appropriate format for transmission. Upon reception, the message is again translated by the network infrastructure and the receiver processes the resulting data according to the IEC 61850 standard. This allows the IEC 61850 protocol to be used with a number of network technologies (e.g. Ethernet, WiFi, or ZigBee). Being network agnostic is important because it enables the IEC 61850 protocol to continue to be used as network technologies advance.

The Smart Grid also requires devices to communicate with devices from other vendors and this requires interoperability, which is a major goal of IEC 61850. The issue of interoperability is addressed by defining the structure and ordering of data items in messages and how these data are presented in those messages (Mackiewicz 2011; Xiong et al. 2008). The goal is to achieve plug-and-play capability (similar to the capability provided by USB for PCs) for IEDs to provide the interoperability necessary for the Smart Grid (Hossenlopp 2007). In the Smart Grid, the equivalent of the driver for the hardware device that plugs into the USB port is the IEC 61850 definition of the data items and how those data items are presented. Standardizing the data and their presentation also reduces the amount of work required to connect IEDs to the Smart Grid network because each device uses the same standardized communication protocol and data definitions (Mackiewicz 2011).

The base component of an IEC 61850 network is the physical device, e.g. a smart relay. The physical device has a defined location and purpose and is given a network address (Mackiewicz 2011). A physical device may perform a single function or multiple functions, e.g. measuring current, status monitoring, or controlling a circuit. Each function that a physical device performs is considered a logical device (Mackiewicz 2011), and is similar to the concept of a port in computer networking. Hence, a single physical device may contain multiple logical devices: one for each function. In turn, each logical device is composed of multiple logical nodes, which are groups of data items and procedures provided by the logical device (Mackiewicz 2011). The data items can be measurements or set-point values, while the procedures perform the actions required to maintain the power grid. The format and presentation of these data items is provided in IEC 61850-7 (Mackiewicz 2011). The architecture of IEC 61850 lends itself well to being implemented in Object-Orientated code. In Ozansoy et al. (2009), the authors describe an Object-Oriented framework that can be used to implement IEC 61850 IEDs and the communication exchanges between those IEDs. In Mercurio et al. (2009), the authors present an implementation in simulation of a substation communication and control network based on the IEC 61850 and IEC 61970 standards using the Object-Oriented program design philosophy. They define a framework for building software objects to represent the components of a substation network and investigated the use of the common object request broker architecture (CORBA) to send messages (Mercurio et al. 2009). The use of CORBA does not allow this implementation to be used in real-time monitoring or control systems that have hard deadlines (Mercurio et al. 2009). Although use of CORBA has declined significantly over the last few years, integration efforts within the CORBA framework can be easily ported to other frameworks.

### *3.1 IEC 61850 Network Architecture*

IEC 61850 defines two different buses or local networks: the station bus and the process bus (Mackiewicz 2011). The process bus connects the relays and primary equipment to the IEDs in the substation (Mackiewicz 2011). The process bus is typically deployed at the bay level and may cover a single bay or span multiple bays. Data aggregators termed merging units combine information from multiple IEDs into a single message and then pass this on to the process bus (Mackiewicz 2011). This helps reduce traffic on the process bus and reduces the number of network connections the process bus must support. The IEDs act as the bridge between the process bus and the station bus. The station bus connects all of the process buses together and provides the connection to the utility control center (outside world) and other substation management functions (e.g. substation historian) (Mackiewicz 2011). Figure 1 illustrates the process and station buses in relation to substation management and primary equipment.

An alternative approach to having both a station and process bus is to implement only a station bus. In this case, hardwired direct connections are still present between the IEDs and the relays and primary equipment. The former option (station and

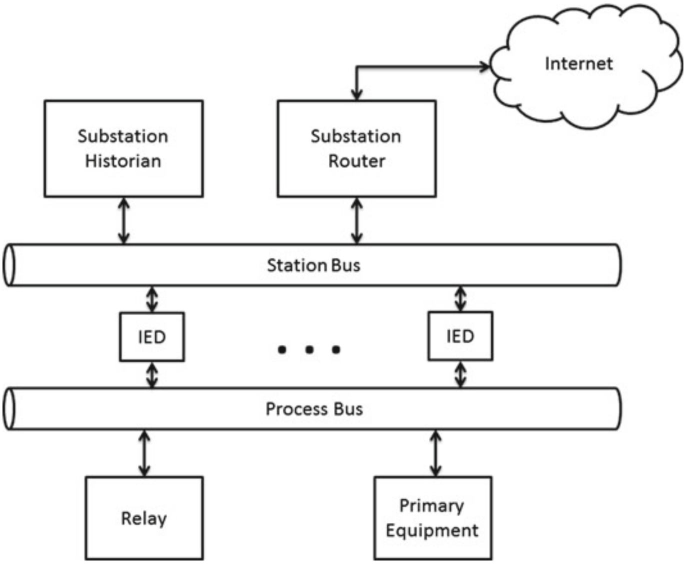

**Fig. 1** Typical IEC 61850 network architecture with process and station buses

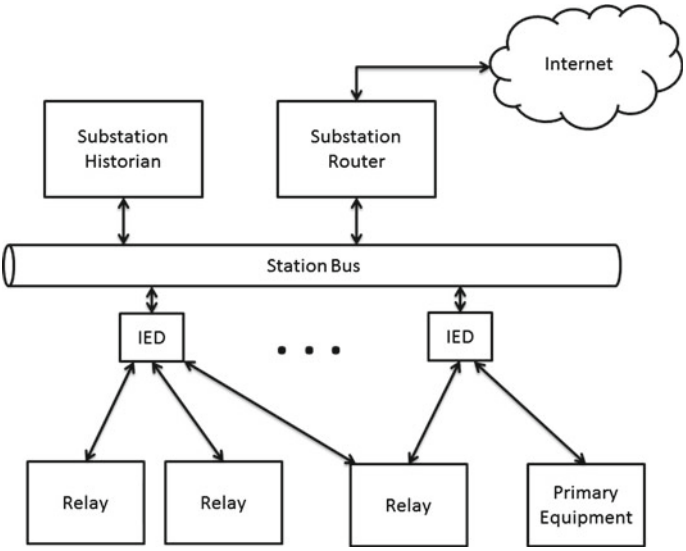

**Fig. 2** Typical IEC 61850 network architecture with only a station bus

process bus) is often employed for new substations and this option (station bus only) is useful for a retrofit of an existing substation to upgrade it to use IEC 61850. This option minimizes the impact on the internals of each bay because only the connection between the station bus and bay equipment must be updated. Figure 2 illustrates the basic network architecture for the station bus only option.

IEC 61850 defines two communication functions to provide an interface between an IEC 61850 IED and a supervisory control and data acquisition (SCADA) system (Higgins et al. 2011). Both functions deal with the IED reporting changes or alerts in signals that the IED is monitoring to the SCADA controller. Alerts can be generated when a signal is detected outside of a predefined range (e.g. exceeds a threshold value) or when a signal changes too quickly (Higgins et al. 2011).

Two types of connection strategies are possible: data gathering only, or data gathering and control. Initial implementations were data gathering only and are not required to meet the timing requirements of control systems. In these systems, the data gathering connections are simplified into a single Ethernet connection that links the device back to the central control center.

Control applications require time critical operation. Typically, faults must be identified, processed, and corrected within two cycles. IEC 61850 specifies that time-critical messages must be delivered within 4ms from the time they are sent. The 4ms requirement in less than the two-cycle time but it is important that the message arrives in time for the protection device to process, respond and take action. Thus, the IEC 61850 network must provide the communication bandwidth and transit time to meet this requirement.

Support vector machines (SVMs) (Cortes and Vapnik 1995) are used in pattern matching applications and are one technique to monitor power systems for stability. SVMs can also be used to help secure power systems by identifying abnormal behavior patterns, and can be integrated into an intrusion detection system (IDS) for the power sector. SVMs must be trained with known input sets representing normal and abnormal behavior or conditions. Once trained, SVMs can be used to identify suspicious behavior in the Smart Grid. SVMs have been used to forecast electricity demand based on data from Smart Meters (Men and Liu 2011).

IEC 61850 provides support to transmit sampled value data, which are data taken from sensors. Merging units can be employed to collect and aggregate sample value points together to send in one large packet verses several smaller packets, reducing network load in terms of the number of messages. Thus, the IEC 61850 sampled value message type can be used as input to SVMs. The critical concern is for the network and system to be capable of providing data input at the required rate.

## *3.2 IEC 61850 Deployments and Pilot Projects*

The Tennessee Valley Authority (TVA) designed their Bradley Substation to use IEC 61850 (Ingram and Ehlers 2007). IEC 61850 provides a substation configuration language that can be used to encode the equipment description for an IEC 61850 network. Naming conventions for the SCL description are defined in IEC 61850 to simplify identification of information to other IEDs and devices (Ozansoy et al. 2009). In this manner, the SCL provides part of the driver for the plug-and-play capabilities of the IED. The SCL also provides the ability to describe the connections between devices in the substation (Higgins et al. 2011). Thus, the SCL maintains the network topology for the substation. This enables the user to obtain a snapshot of the network topology at any time. Using the SCL provides automated book-keeping for new devices or those that are replaced: changes in the SCL can be easily documented by periodically requesting the SCL information from the IEC 61850 network. This is very important for auditing and scheduling of routine maintenance of equipment. Further, each piece of equipment can be tracked even if it is moved around in the substation or to a different substation. Such tracking is important because it allows detailed maintenance and service logs to be kept for each device. TVA cited the SCL as one of the major benefits of IEC 61850 because of the labor savings in IED setup and installation, and in the simplification of device management in the future (Ingram and Ehlers 2007; Rietmann and Reinhardt 2006).

TVA will realize a significant savings due to automation because routine inspections of the substation can be limited. This automation requires that TVA be able to remotely query IEDs to see not only their published readings but also internal settings and measurements to enable TVA to remotely diagnose problems (Ingram and Ehlers 2007). Remotely diagnosing problems will ensure that the technician sent to repair the substation has the proper training and equipment (Ingram and Ehlers

2007). This will reduce operating expenses, as technicians know exactly what the problem is and already have a plan to address it before arriving at the substation.

The Comisión Federal de Electricidad (CFE) upgraded some of their substations to an IEC 61850 based network beginning in 2005 (Moreno et al. 2012). They cite interoperability, interchangeability—the ability to swap devices with ones from different manufacturers, use of an open and royalty free protocol, vendor independence—not being restricted to a single vendor's vertical solution, and a LAN network to link components together in a cost-efficient and safe manner as the primary goals/benefits of moving to IEC 61850 (Moreno et al. 2012). They found that documentation of the network configuration, especially, maintaining a current list of the IP address assigned to each IED was critical (Moreno et al. 2012). Interchangeability was possible with only one manufacturer's IED and that IED stored the SCL internally (Moreno et al. 2012). Hence, for interchangeability, it is recommended that IEDs store the SCL internally.

It is important to note that CFE found that IEC 61850 did not provide all of the alarm and data types they required, but they were able to extend the IEC 61850 data types to accommodate their new requirements (Moreno et al. 2012).

## 4 Challenges for Substation Automation

There are a number of challenges to using IEC 61850 for substation automation. Moving to a LAN structure introduces many variables in the communication infrastructure that must be taken into account. Maintaining accurate date and time settings and maintaining quality of service under variable traffic loads are two examples. The non-deterministic nature of an Ethernet network complicates these requirements and introduces other issues. In particular, the non-deterministic nature of Ethernet may produce scenarios where packets containing measurements arrive out of order. This is due to network relay devices (e.g. switches and hubs) that must retransmit packets as they move between networks. Large packets may be broken up into smaller packets based on network infrastructure or current traffic loads. The IEC 61850 network must ensure that all parts of the message reach the destination and are reassembled within the 4ms time window. Using commercial networks to link the substation to the utility as opposed to dedicated private connections, requires strong security on both the IEC 61850 network and the physical devices themselves. These challenges are described in this section and potential solutions to each challenge are described.

### *4.1 Timing Synchronization*

In a distributed control system, it is important that the IEDs are synchronized with each other. This enables accurate timestamps to be applied to data readings that are used by data aggregators to make control decisions. This is especially important with Ethernet because messages may arrive out of order: readings at time $t$+30 may arrive before readings from time $t$. There are many methods of clock synchronization available and one is the network time protocol (NTP) that is standard on most Ethernet TPC/IP based networks. The IEC 60870 family of protocol defines the communication between the substation and control center (Sanchez et al. 2010). In Sanchez et al. (2010), the authors present an implementation and simulation of an IEC 60870-5-104 protocol using standard Internet protocols, SNMPv3 (simple network management protocol ver. 3), SSH (Secure SHell), and network time protocol (NTP), instead of the IEC 60870-5-104 stack. They use a database table system, called management information base (MIB) (Stallings 2000), to provide read and write access to the intelligent electronic devices (IEDs) (Sanchez et al. 2010). The MIB concept is widely used in networks to manage the devices connected to the network (Stallings 2000). They compare their implementation to an implementation using the IEC 60870-5-104 stack in terms of number of bits transmitted and percentage of communication that is related to electric power data and control. The method proposed by Sanchez, et al., yields better performance than the IEC 60870-5-104 stack: fewer bits transmitted and a higher percentage of messages containing useable information verse book-keeping information (Sanchez et al. 2010). However, using NTP they are only able to obtain a synchronization within 10 ms (Sanchez et al. 2010). Hence, their proposed system is not suitable for control and monitoring applications requiring hard real-time deadlines of under 10ms and is not suitable for IEC 61850. Other synchronization methods, such as IEEE 1588 (IEEE 2008) and GPS (global positioning system) timing information, may yield better results. Variable network traffic must be taken into account and proposed solutions to the synchronization and other problems must be analyzed to determine their impact on the overall network load and message transit times.

Clock synchronization is important and this synchronization will require additional traffic on the network. Other maintenance tasks will add to this overhead. One option is to use a separate (redundant) network to provide synchronization and other maintenance tasks, leaving the primary network to carry just monitoring data and control information. This has the added advantage of providing another redundant connection that could be used for other forms of data transfer during an emergency.

## *4.2 Network Traffic Load*

The amount of messages present on the network is directly related to the level of congestion on the network. Gao, et al., investigate the congestion of a network based on the amount of bandwidth that is utilized on the network (Gao et al. 2008). They found that under normal conditions that messages could be delivered within the 4 ms limit, but that a slight increase in utilization caused message delays to exceed the 4 ms limit (Gao et al. 2008). Periodic status reports and heartbeat signals from physical devices can be scheduled to avoid such congestion. However, during a fault or emergency condition the network utilization will increase substantially leading to increased congestion and delay. One alternative is to provide multiple network links to each device, with each link serving a different type of message class. For example, one link could be dedicated to periodic status and heartbeat signals, while a second could be dedicated for control and emergency messages. Unfortunately, the use of multiple links is contrary to the goal of IEC 61850 to reduce the number of communication links in a substation. Another solution is to increase the bandwidth of the network infrastructure (Gao et al. 2008). Increasing the bandwidth solves the present problem, but most likely only for a short time because the extra bandwidth will be used up to provide new features or improved control.

The architecture of the Ethernet network is important to its performance. The network must be designed to minimize packet delay in order to meet the 4ms timing requirement specified by IEC 61850. In their initial deployment, CFE used two ring topologies connected at a few places for their substation network (Moreno et al. 2012). This architecture did not perform well and resulted in significant delays during fault conditions (Moreno et al. 2012). A single ring topology provided better performance when clearing a fault (Moreno et al. 2012). As a result, CFE's recommended network topology is a single ring with one Ethernet switch per panel (Moreno et al. 2012). Using one Ethernet switch per panel will dramatically reduce the number of connections to the backbone substation network and allow intra-panel messages to be delivered without having to travel over the backbone substation network. This provides significant reduction in network traffic, thus, improving performance on the process bus.

## *4.3 Communication Protocol with Non-Deterministic Timing*

The Ethernet protocol does not provide deterministic transit times for messages from sender to receiver. First, Ethernet defines a non-deterministic exponential back-off time when a collision or consecutive collisions are detected. While this method works well to address collisions, it yields a protocol where the delay in transmitting a message from the sender to the physical network varies with current network traffic. Second, Ethernet networks are multiple hop networks with intermediate devices, e.g. hubs, switches, and routers, routing messages to their proper destination. As these intermediate devices receive input from multiple senders, incoming messages are placed in a queue and are processed sequentially. When sending the message the first issue is again present. This issue is also dependent on network traffic, but also on network topology. Network topology is important because it defines choke-points, e.g. a central switch, in the system that receive an increased amount of traffic. Network topologies for IEC 61850 substations must take this into account and not route too much traffic through a single choke-point (e.g. switch).

Evaluations (Kanabar and Sidhu 2011) have shown that IEC 61850 can provide the needed latency for data reporting, but not for control. Control requires at least two messages to be sent. The first message is from the device to the central controller reporting a fault or abnormal data. The central controller then responds with a message indicating what action to be taken to clear the fault. Possible solutions to the latency problem are described below.

High-end Ethernet switches have Quality of Service (QoS) capabilities that allows system designers and system administrators to attach a priority to a message or communication channel. Higher priority messages are given preference over lower priority messages and are relayed first. Sidhu and Yin investigate the performance improvement of QoS using a network simulation of a sample IEC 61850 enabled substation (Sidhu and Yin 2007). Their results indicate that using QoS improves performance (lower transit time) for an Ethernet network based on 10Mb/s equipment, but that no improvement was observed for an Ethernet network based on 100 Mb/s equipment (Sidhu and Yin 2007). Thus, the QoS feature may not provide the needed savings to meet the timing requirements of substation for higher speed networks.

As the number of devices connected to the network increases so will the transit time of messages due to increased contention and traffic being routed though choke points. Scalability was also found to be an issue as a 3.14X increase in transit time was observed when the number of Ethernet switches in the example substation was increased to 14 from 9 (Sidhu and Yin 2007). Detailed network simulations must be conducted to verify that the proposed network topology for a substation can provide the required speed. Choke-points must be identified and the topology changed as needed to provide the required QoS.

The bandwidth of the network is an important consideration and must be sufficient to handle the network traffic while ensuring delivery of messages within the required time. Messages in the substation will have different priorities based on type and current operating conditions. Message priority can change as the current operating conditions change making it difficult to meet the timing requirements using the QoS features of Ethernet (Deshpande et al. 2011). Deshpande et al. (2011) propose a strict priority queue (SPQ) and provide a priority ordering of Smart Grid message types for the Differentiated Service Code Point (DSCP) feature in the IP header. The SPQ feature provides a means to enable high priority messages to meet their delivery time requirement by preempting lower priority messages that have larger maximum allowable delays (Deshpande et al. 2011). They simulate a small substation network to determine the bandwidth required to meet the message delivery time requirements. In their simulation the maximum allowed time for a message to be delivered is 8 ms, which is twice that allowed by IEC 61850 (Deshpande et al. 2011). Their results show that a network bandwidth of 3.072 Mb/s is required to meet the 8 ms delivery requirement (Deshpande et al. 2011). This translates into a bandwidth requirement of 7.144 Mb/s for an IEC 61850 network. This bandwidth is easily achieved using a standard 10 Mb/s network. Most Ethernet installations today offer a bandwidth of 100 Mb/s so this should easily meet the message delivery requirements. However, differences in the traffic on the network and network architecture from the simulated network will alter the results. Thus, a higher or lower bandwidth may be required for an arbitrary network.

The use of multiple links in a substation can be used to reduce message transit time. One method of reducing the transit time is to use these multiple links in the same manner as a parallel I/O port. Large messages can be broken into smaller parts and transmitted over several links in parallel (Deshpande et al. 2011). The Multilink Point-to-Point Protocol (MLPPP), defined by IETF (Internet Engineering Task Force) RFC (request for comments) 1990, can be used to provide this functionality (Deshpande et al. 2011). The use of MLPPP may result in a lower bandwidth requirement (Deshpande et al. 2011). The redundant links in the substation could be used to provide the parallel connections. However, this use of the backup (redundant) network links must be weighed against the need to have backup network links in the event that some of the primary links fail. Network bandwidth should not be designed using MLPPP as some of the parallel links are provided by the backup network in the substation. The required bandwidth must be computed based only on the non-backup links and enough redundant links must be installed to provide the MLPPP service.

## *4.4 Order of Packet Reception*

The Ethernet protocol does not guarantee that the receiver will receive the packets in the same order as the transmitter sent them. Higher level protocols, such as TCP guarantee in-order delivery by default and IP provides means to establish packet order at the receiver. This can be problematic for data monitoring applications that are performing calculations to monitor the stability of a power line in real-time. IEC 61850 uses a mix of protocols (e.g. Ethernet, IP, and TCP) transmitted over an Ethernet medium. The GOOSE (Generic Object Orientated Substation Event) IEC 61850 message is transmitted at the Ethernet level and the Ethernet header does not contain any information about ordering. Hence, the packet must include a field to denote the order or a timestamp having the required precision associated with each reading. This is necessary to allow the receiver to reconstruct the ordering of packets and to process the data in the appropriate order. This added field increases the time required for communicating the message (more bits to send and receive) and the processing time on each end (receiver must reorder packets). This field may be in the header for the protocol (e.g. fragmentation information in the IP header), associated with an acknowledgement and transmission scheme inherent to the protocol (e.g. acknowledge/retransmit scheme for transmission of data segments using TCP), or as part of the data itself.

The data analysis algorithms used in substations automated using IEC 61850 must support reception of packets in a different order than they were sent by the transmitter. Reordering of messages at the receiver is not always feasible, for example, in monitoring applications where data must be processed to derive current values. In extreme cases, earlier packets may be significantly delayed and arrive at the receiver too late to be of any value or the packet may be dropped (never arrives). Hence, the monitoring algorithms must be designed to account for missing or late data due to the non-deterministic nature of the Ethernet communication medium. Kanabar and Sidhu (2011) present an algorithm to estimate missing data values in their monitoring functions. Based on their results, monitoring systems with higher sampling rates were more resistant to consecutive missing samples.

Estimation of missing data also affects the response time of an IED. Kanabar et al. (2011) investigate the response time of IEDs for monitoring and controlling phase delay in the electric grid. The IEDs they used in their experiments assumed a value of 0 for missing phase measurements (Kanabar et al. 2011). They propose an algorithm to estimate the missing values and their results indicate that the response time of the IED is reduced to 23–25 ms from 23–41 ms without the estimation (Kanabar et al. 2011). IEDs must support robust estimation algorithms to estimate the value of missing data items. These algorithms must provide high quality estimates while also being able to detect fault and abnormal conditions to which the IED must respond. Designers must thoroughly understand how the IED handles missing data values and design the control algorithm and system to handle these events safely.

## 4.5 Fragmentation of Large Packets

The TCP/IP protocol supports *fragmentation* or the breaking up of large packets into smaller packets (Forouzan 2003). The maximum size of a packet is defined by a number of factors including network capabilities and network traffic. In an IEC 61850 Ethernet based substation, the network is defined to meet a specified criteria and should be uniform across the substation. Hence, network capabilities should not have much impact on variations in maximum packet size. However, in substations that utilize multiple types of physical networks, e.g. Ethernet, WiFi, and ZigBee, the network capabilities may influence the maximum packet size. This is especially true at the interfaces between networks. The current amount of traffic on a network is the major factor in determining the maximum packet length. Longer packets take up space on the medium and other messages may not arrive in time. Smaller packet sizes may be used to send parts of multiple messages in the same time. Here, fragmentation enforces fairness on the communication medium and prevents any one device from being starved out of communication. Message size is an important factor in the time required for a message to be received. One simulation, showed that message sizes of 2 kB were able to be transmitted within the 4ms limit but those of 4 kB were not (Gao et al. 2008). Fragmentation can reduce the delay in transit across the network, but the key metric is not the delay of each fragment (part of the message), but the reception of the entire message (Gao et al. 2008).

One solution is to keep the size of each message small enough to fit into the smallest packet size supported by a physical layer. This will reduce the delay significantly and can allow the entire message to be received within the 4 ms required by IEC 61850. However, sending multiple small messages will increase congestion on the network, introducing additional delay. Thus, the optimal size of the message to reduce transit delay is dependent on the network protocol and the network architecture. The optimal values for message size can be investigated using standard discrete event simulation models of Ethernet. Such simulations should be conducted for each variation of network architecture early in the project.

## *4.6 Security Implications of Wireless for IEC 61850 Networks*

Wireless networks offer many benefits over wired networks. First, the need for cabling between nodes is eliminated. Second, nodes can be located in locations that are difficult to access with a wired connection. For example, a wireless node located on a piece of moving equipment can be placed without the need to provide a connection to it through stationary parts of the equipment. Another example is to place a node in a hazardous environment and communicate using wireless means. Third, wireless networks are more easily upgraded. Additional hardware is not required to add more connections. Although access time will increase as more connections are made, there is no problem of running out of ports as on an Ethernet switch. Finally, a wireless network provides easy access for the technician: through a cellular link or by driving by the substation and connecting with a traditional wireless, e.g. WiFi, link.

Wireless networks are visible to anyone within range with the appropriate receiver. This availability reduces the effectiveness of physical security solutions in protecting the substation. Because an economical infrastructure is one of the goals of the Smart Grid, these networks will be commercially available technologies, e.g. WiFi or ZigBee. While security can be activated on wireless networks this comes at the price of added overhead and slower communication speeds. Further, as computing technology advances, these security measures will become outdated and are subject to being hacked.

Wireless communication can also be affected by electro-magnetic interference (EMI) generated from other wireless equipment or from electric equipment in the substation (Yu and Johnson 2011). EMI can cause messages to be corrupted resulting in a retransmission or not being received at all. Intentional EMI generated from an attacker using a jamming device could be used to disable parts of the IEC 61850 network. Physical security should address the jamming attack by keeping the attacker out of range of the substation. Verification and testing of wireless equipment for the substation for EMI immunity must be conducted and the design engineer must be aware of other devices that will also use the wireless spectrum (Yu and Johnson 2011). Transmission algorithms must be developed to coordinate transmissions among multiple wireless devices. Definition and use of accepted testing standards and best practices will address the EMI immunity concerns (Yu and Johnson 2011).

## *4.7 Integration of Control and Protection Functions into a Single Device*

Older substations have little or no integration of functions for control and protection, typically employing a one function per device model. The logical node feature of IEC 61850 provides the ability to integrate several functions into a single IED. Integration reduces the number of point-to-point connections and the amount of cabling, but increases the impact of a device failure. The IEC 61850 protocol allows the integrated node to collect and package input from multiple sensors or distribute commands to multiple actuators. Hence, the integrated node can be visualized as a collection of sensors and actuators that communicate with the outside world through a centralized router block.

From a security standpoint, a system composed of a number of individual nodes may be more secure than one with a few nodes, each containing several functions. In the event that a node is compromised in the one function per node case, the attacker can control or affect only one function. However, in the integrated case, the attacker can control or affect multiple functions. If the attacker is able to compromise or disable the centralized router or switch they can block all communication with the IED resulting in the loss of information and capability provided by that IED.

Normal failure of IEDs is another event that must be guarded against. Simple, but robust solutions employ redundant sets of IEDs throughout the substation. With the merging of functionality of several non-IEC 61850 IEDs into one IEC 61850 IED, this becomes a larger concern because the failure of one IEC 61850 IED disables several functions. One method proposed in Xiong et al. (2008) is a generic control IED that sits in the background and only becomes active when there is a fault that disables an IED. This backup IED then provides the analysis and reporting features, filling in for the disabled IED (Xiong et al. 2008). If the disabled IED is in direct control of electric machinery, the spare IED can only provide analysis and reporting information to the central controller. However, if the IEDs directly controlling the machinery are intact the spare IED can establish communication with these IEDs and provide control and well as monitoring functions.

Integration of control and protection functions into a single IED requires a reevaluation of the accepted best practices for providing adequate backup and redundancy for substations. Security is also an issue and best practices need to be developed for security IEDs integrating multiple functions.

## *4.8 Potential Attack Vectors to the IEC 61850 Network*

The IEC 61850 network architecture is susceptible to the same attack vectors that a traditional data network is. The US National Institute of Standards and Technology (NIST) has published a report, NIST Special Publication 800-82 (Stouffer et al. 2011), covering security issues in SCADA and control systems for the critical infrastructure. This report provides an overview of the entry points for threats and attacks into these systems. Recommendations are provided to address and guard these entry points.

The substation network can be divided into two areas or sub-networks. The first sub-network is a local area network (LAN) entirely within the substation and connects the protection devices and monitoring systems together. This network is based on IEC 61850 and is typically contained entirely within the substation perimeter. The substation perimeter provides protection to the substation and IEC 61850 network from physical attacks. The second sub-network is the connection between the substation and the utility. It is more economical to have the substation tie into a large commercially available network to link back to the utility than for the utility to construct a private dedicated network connection (Dondossola et al. 2009). The commercial network provides the attacker with a potential entry point into both the substation and utility. Often multiple independent connections between the substation and utility exist to address the redundancy requirements of the electrical grid (Dondossola et al. 2009). Each of these links is a target for an attacker and must be secured and monitored. Within the Smart Grid data integrity and device availability are the two key requirements (Giani et al. 2008). Integrity includes verifying that the sender is a legitimate part of the network and not a rouge device (Giani et al. 2008). Availability is critical because the IEDs must respond to faults and changing conditions within a hard-real-time deadline. Potential attack vectors are described in the following sub-sections.

### 4.8.1 Eavesdropping on Network Traffic

The attacker must acquire knowledge of the system they are planning to attack to identify vulnerabilities. The network architecture is a valuable piece of information that the attacker can use in their attack. Based on this information they can identify the structure of the network, including central Ethernet switches, and can discover the type of devices on the network. Using this information the attacker can select targets on the network that they can exploit.

This information can be obtained through eavesdropping on the messages carried by the network. There are several tools available for sniffing network traffic or the attacker can compromise a device on the network and use that device to eavesdrop. Encryption is one method to counter eavesdropping because the attacker is not able to decrypt the messages. Jung et al. (2008) propose deploying a security device between each device (e.g. a RTU) and the centralized SCADA network to counter the eavesdropping attack. While encryption will counter eavesdropping it will not counter a replay attack were an attacker sends a previously recorded message, e.g. a trip command, at a later time. A replay attack compromises data integrity by reusing a previous message or command to affect some change to the system. It is important to ensure that any solutions used by IEC 61850 include protection against replay attacks.

### 4.8.2 Countermeasures to the Replay Attack to Ensure Data Integrity

The use of a timestamp in each message or a challenge-response protocol will counter the replay attack. Any encryption or challenge-response based security measure must be implemented to meet the timing requirements of the system (4 ms in IEC 61850). Challenge-response based approaches while powerful from a data security standpoint require multiple messages to be exchanged and this may be problematic from a timing standpoint. An implementation of the encryption/decryption in hardware, such as an FPGA (field programmable gate array), will most likely be necessary to meet the timing requirements while maintaining the required network throughput. The FPGA has the advantage that it can be reprogrammed in the field, simplifying the update and patching process.

### 4.8.3 Denial of Service Attacks

Denial of service (DOS) attacks are used to prevent users from accessing network resources. A DOS attack is relatively simple to carry out and requires significant resources to counter and recover from such an attack. In a DOS attack, the attacker sends a large number of messages to the machine under attack. Often the attacker uses a large group of machines that they have compromised to conduct the attack and increase the difficulty in stopping the attack. In the case of the substation, the goal of a DOS attack most likely would be to slow the delivery of critical messages between the substation and utility enough to disable the remote control and monitoring capabilities the utility has over the substation.

High-profile websites employ large numbers of web servers to handle their normal load and can switch loads between servers to counter a DOS attack. In this case, those servers under attack will not be used and traffic will be redirected to other servers. Firewalls can be used to ignore messages from the attacking machines but with a large number of machines, the firewall must identify which are involved in the DOS attack. These countermeasures require significant investment and network monitoring. This investment negates some of the benefits of using a commercial network to link the substation to the utility.

One solution to the DOS threat is to use a firewall with strong rules and dedicated IP addresses for the substation and utility. The dedicated IP addresses allow firewall rules to be developed to only accept traffic from a specific set of IP addresses. This will help prevent DOS attacks from getting inside the substation or utility, but will still cause problems at the firewalls where the substation and utility connect to the commercial network. Another solution is a dedicated phone line, cellular link, or satellite link that supports high-speed data transfer, e.g. DSL. This link could be used in emergency situations to provide basic monitoring and control functionality from the utility. The wireless long-range links provide the benefit of being able to function in the event of a disruption of the communication infrastructure. This is especially true for the satellite link. The redundant communication links also provide some protection because an attacker must identify all the links to completely block communication.

### 4.8.4 Insertion of Malicious IEDs

Substation networks assume that all participants on the network are legitimate IEDs. The presence of a malicious or fake node or a legitimate node that has been compromised provides the attacker with a significant abilities. Through the malicious node, the attacker can inject false information into the substation (Stouffer et al. 2011).

This false information can cause the substation to react to a false set of conditions and provide non-optimal output and in extreme cases even cause a blackout (Dondossola et al. 2009; Stouffer et al. 2011). In the blackout scenario the false information makes the substation believe that a substantial fault is present causing the substation to isolate a sector to protect the rest of the grid. Alternatively, the malicious device can be used to alter the operating condition of the substation to physically damage equipment (Stouffer et al. 2011). This is more problematic because the damaged equipment must be repaired or replaced. The resulting service interruption will take longer and be more costly to correct. Strong authentication methods, such as challenge-response, that meet the timing requirements are needed.

### 4.8.5 Alteration of Operating Parameters

The operating parameters of the IEDs can be configured remotely using IEC 61850. Of particular interest are parameters relating to the control or operation of the IED, such as set points or an operating mode setting (e.g. normal or test mode flag). Often set points are updated regularly by the control system as it responds to the current electric demand and conditions. Operating mode parameters can be used to set the IED into a diagnostic or test mode during a routine inspection, outage, or during maintenance. If an attacker can access and change these parameters, they can cause blackouts and/or significant damage to equipment (Stouffer et al. 2011). Strong authentication is required for accessing the operating parameters. Some settings such as switching the IED to diagnostic mode could be restricted to manual operation, e.g. a switch, at the substation. Typically, personnel will be present at the substation during maintenance and routine outages to conduct the testing. Hence, the physical security employed at the substation will deter this type of attack. Multiple levels of access requiring additional passwords can help address this threat (Anderson and Leischner 2007).

## *4.9 Testbeds*

Testbeds are important in the evaluation of systems under controlled conditions and without the risk of causing harm to physical equipment. A number of testbeds exist for Smart Grid related applications. These testbeds fall into three categories: real-world testbeds, hardware-in-the-loop testbeds, and simulation testbeds. Real-world testbeds are built using actual components and equipment that are isolated from the larger system. In addition, a testbed environment allows new technologies and security measures to be tested for backward compatibility with legacy devices. Because it is not feasible to upgrade the entire power grid in one iteration, new technologies and security measures must not negatively affect existing devices present in the system. Real-world testbeds provide the best accuracy because real devices are used, but are costly to build and do not easily support investigation of scenario variations. Simulation testbeds are contained entirely in software and use mathematical or discrete event models to model physical and digital processes. Hardware-in-the-loop testbeds are a hybrid of real-world and simulation testbeds, incorporating equipment into a software simulation. Hardware-in-the-loop testbeds simplify evaluations of systems as they scale up in size. The hardware components provide the physical response to the current state of the system and this response is fed into the simulation. The system is scaled up by replicating this behavior within the simulation in software. This type of testbed is useful in analyzing the behavior of a small group of devices or small piece of the larger system.

A simulation testbed for the distribution network for the power grid has been developed by University of Chicago to study the effect of DOS attacks against the Smart Grid communication network on electricity distribution (Davis et al. 2006). This testbed enabled the simulation of a large network where the attacker used the DOS attack to prevent the utility from receiving updated load information showing an increase in load resulting in a blackout (Davis et al. 2006). A defense against the DOS attack based on filtering or blocking the attacking computers was developed and tested yielding promising results allowing the updated load information to reach the operator in time (Davis et al. 2006).

Connecting multiple testbeds together improves the quality and capability of the test by leveraging each testbed's strengths. The Virtual Power System Testbed (VPST) is a hardware-in-the-loop testbed that supports an interface to connect to other testbeds (Bergman et al. 2009).

Another hardware-in-the-loop testbed incorporates an IEC 61850 overcurrent relay with a simulated network and computer workstations (Hahn et al. 2010). This testbed was developed to evaluate a method to search a substation network for NERC CIP (North American Electricity Reliability Council 2009) violations and the proposed method was successful in finding NERC CIP violations (Hahn et al. 2010). NERC CIP is a set of standards providing regulations, best practices, and guidance for security the power grid.

## 5 Future Work

The use of IEC 61850 to automate and provide remote control to substations requires careful review and reevaluation of operational challenges as well as compliance with existing regulations. Networks must be evaluated to quantify the effect variables such as traffic load, topology, and security requirements have on quality of service and design requirements. This evaluation could be conducted using discrete event simulations and testbeds to verify simulation results. Algorithms for handling missing data items and data received out of order must be researched and developed.

Revision of the regulations and best practices for providing redundant devices will be required as control and protection functions are combined into a single IEC 61850 device. The security implications of this combination must also be researched and the findings reflected in the revised regulations and updated best practices.

Security for the Smart Grid is a critical area of research. Solutions to protect availability of devices, integrity of data, and confidentiality of the data meeting the requirements of the Smart Grid must be researched. Traditional information technology (IT) solutions will not meet the timing requirements of the Smart Grid. Furthermore, solutions with availability of devices as the first priority must be established. This differs from the typical IT case where confidentiality, e.g. for financial transactions, is typically the primary concern. Best practices must be developed to address the security needs while meeting the operational requirements of the Smart Grid.

Standards and best practices for reliability and certification of wireless Smart Grid equipment must be evaluated and revised (Yu and Johnson 2011). Standards from many fields must be analyzed (e.g. electrical protection, EMI, shock, temperature, and humidity) and requirements harmonized for operation of wireless devices in the Smart Grid. These testing and reliability standards must also be converted for use with non-wireless digital systems that will be found within the Smart Grid.

## 6 Conclusions

The Smart Grid promises to improve electricity delivery, reduce cost, and conserve resources. However, there are many challenges that must be addressed. This chapter has presented the challenges regarding substation automation using the IEC 61850 family of standards. Implementation and deployment of IEC 61850 will require revisions to existing best practices and new best practice guidelines to be developed. These revisions will include topics from the fields of electrical engineering—power engineering and power system protection, and computer science—network architecture and security. A joint effort will be required to address the challenges associated with moving to IEC 61850 and meeting the requirements to provide safe and reliable electricity.

## References

Anderson D, Leischner G (2007) Cybersecurity as part of modern substations. Schweitzer Engineering Laboratories, Inc. http://www.selinc.com/WorkArea/DownloadAsset.aspx?id=3530. Accessed 21 Jan 2011

Bergman DC, Jin D, Nicol DM, Yardley T (2009) The virtual power system testbed and inter-testbed integration. In: Proceedings of the 2nd conference on cyber security experimentation and test, USENIX Assoc., Berkeley, CA, USA, 2009

Cortes C, Vapnik K (1995) Support-vector networks. Mach Learn 20(3):273–297

Davis CM, Tate JE, Okhravi H, Grier C, Overbye TJ, Nicol D (2006) SCADA Cyber security testbed development. In: 38th North American Power Symposium, pp 483–488, Carbondale, IL, 17–19 Sept 2006

Deshpande JG, Kim E, Thottan M (2011) Differentiated services QoS in smart grid communication networks. Bell Labs Tech J 16(3):61–81

Dondossola G, Deconinck G, Garrone F, Beitollahi H (2009) Testbeds for assessing critical scenarios in power control systems. In: Setola R, Geretshuber S (eds) Critical information infrastructure security. Lecture Notes in Computer Science, vol 5508. Springer, Heidelberg, pp 223–234

Forouzan BA (2003) TCP/IP Protocol suite, 2nd edn. McGraw-Hill, New York, NY

Gao H, Jin W, Liu G (2008) Simulation study on delay of end-to-end data communication for protective relaying in substations. Front. Electr. Electron. Eng. China 3(2):246–250

Giani A, Karsai G, Roosta T, Shah A, Sinopoli B, Wiley J (2008) A testbed for secure and robust SCADA systems. SIGBED. doi:10(1145/1399583):1399587

Hahn A, Kregel B, Govindarasu M, Fitzpatrick J, Adnan R, Sridhar S, Higdon M (2010) Development of the PowerCyber SCADA security testbed. In: Sheldon FT, Prowell SJ, Abercrombie RK, Krings A (eds) Proceedings of the sixth annual workshop on cyber security and information intelligence research. ACM, New York, NY, USA

Higgins N, Vyatkin V, Nair N-KC, Schwarz K (2011) Distributed power system automation with IEC 61850, IEC 61499, and intelligent control. IEEE Trans Syst Man Cybern Part C Appl Rev 41(1):81–92

Hossenlopp L (2007) Engineering perspectives on IEC 61850. IEEE Power Energ Mag 5(3):45–50

IEEE (2008) IEEE 1588–2008—IEEE standard for a precision clock synchronization protocol for networked measurement and control systems, IEEE.

Ingram M, Ehlers R (2007) Toward effective substation automation. IEEE Power Energ Mag 5(3):67–73

Jung S, Song J, Kim S (2008) Design on SCADA test-bed and security device. Int J Multimedia Ubiquitous Eng 3(4):75–86

Kanabar MG, Sidhu TS (2011) Performance of IEC 61850–9-2 process bus and corrective measure for digital relaying. IEEE Trans Power Delivery 26(2):725–735

Kanabar MG, Sidhu TS, Zadeh MRD (2011) Laboratory investigation of IEC 61850–9-2-based Busbar and distance relaying with corrective measure for sampled value loss/delay. IEEE Trans Power Delivery 26(4):2587–2595

Mackiewicz R (2011) Technical overview and benefits of the IEC 61850 standard for substation automation. http://www.sisconet.com/downloads/IEC61850_Overview_and_Benefits_Paper_General.pdf. Accessed 5 Nov 2011

Men D-Y, Liu W-Y (2011) Application of least squares support vector machine(LS-SVM) based on time series in power system monthly load forecasting. In: 2011 Asia-pacific power and energy engineering conference, Wuhan, China, 25–28 March 2011

Mercurio A, Di Giorgio A, Cioci P (2009) Open-source implementation of monitoring and controlling services for EMS/SCADA systems by means of web services—IEC 61850 and IEC 61970 standards. IEEE Trans Power Delivery 24(3):1148–1153

Moreno N, Flores M, Torres L, Juárez J, González D (2010) Case study: IEC 61850 as automation standard for new substations at CFE, practical experiences. Schweitzer Engineering Laboratories, Inc. http://www.selinc.com/WorkArea/DownloadAsset.aspx?id=7405 Accessed 23 Jan 2012

Myrda P, Donahoe K (2007) The true vision of automation. IEEE Power Energ Mag 5(3):32–44

North American Electricity Reliability Council (2009) NERC Critical infrastructure protection (CIP) Reliability standards, North American Electricity Reliability Council

Ozansoy CR, Zayegh A, Kalam A (2009) The application-view model of the international standard IEC 61850. IEEE Trans Power Delivery 24(3):1132–1139

Rietmann P, Reinhardt P (2006) Applying IEC 61850 to substation automation systems. Paper presented at the PSP, (2006) Power System Protection Conference, Bled. Slovenia. 6–8 Sept 2006

Sanchez G, Gomez I, Luque J, Benjumea J, Rivera O (2010) Using internet protocols to implement IEC 60870–5 telecontrol functions. IEEE Trans Power Delivery 25(1):407–416

Sidhu TS, Yin Y (2007) Modelling and simulation for performance evaluation of IEC61850-based substation communication systems. IEEE Trans Power Delivery 22(3):1482–1489

Stallings W (2000) Data and computer communications, 6th edn. Prentice Hall, Upper Saddle River, NJ

Stouffer K, Falco J, Scarfone K (2011) Guide to industrial control systems (ICS) security. NIST Special Publication 800–82, Gaithersburg, MD

Wang W, Xu Y, Khanna M (2011) A survey on the communication architectures in smart grid. Comput Netw 55:3604–3629

Xiong X, Yu J, Liu X, Shen Z (2008) Reliability of substation protection system based on IEC61850. Trans Tianjin University 14(2):118–122

Yu Q, Johnson RJ (2011) Smart grid communications equipment: EMI, safety, and environmental compliance testing considerations. Bell Labs Tech J 16(3):109–131