IEC 61850: WHAT YOU NEED TO KNOW ABOUT FUNCTIONALITY AND PRACTICAL IMPLEMENTATION

Dave Dolezilek
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

ABSTRACT

Today, all utility users and manufacturers recognize the desire and the need to merge the communications capabilities of all IEDs in a substation, or even across the entire power network. This wide-area interconnection can provide not only data gathering and setting capability, but also remote control. Furthermore, multiple IEDs can share data or control commands at high speed to perform new distributed protection, control, and automation functions. This sort of cooperative control operation has the potential to supersede and eliminate much of the dedicated control wiring in a substation, as well as costly special-purpose communications channels between the stations and around the power network.

Many utilities have already installed systems of interconnected IEDs, which provide some degree of centralized substation and system monitoring and control. In practice, the majority of information available in installed IEDs is abandoned and left uncollected because traditional integration techniques were designed to exclusively support SCADA. Rather than being conceived as another protocol, IEC 61850 was created to be an internationally standardized method of communications and integration with goals of supporting systems built from multi-vendor IEDs networked together to perform protection, monitoring, automation, metering, and control. This paper is the second in a series documenting the evolution of the IEC 61850 standard. The first paper, titled “Significant Substation Communication Standardization Developments,” was written in early 2000. It provides a complete introduction to IEC 61850, discusses the harmonization with UCA, provides terms and definitions, and remains a useful resource.

Using the knowledge gained from numerous network designs, this paper focuses on the realities of actual implementation. Parts one through seven of the IEC 61850 standard deal with the abstract concepts of data groupings and naming conventions so that information is associated and described in the same fashion regardless of the vendor. When putting the abstract concepts of the standard on a physical network, as described in parts eight and nine, details emerge that need to be addressed. This paper identifies contemporary observations, documents several implementation lessons learned, and provides recommendations.

INTRODUCTION

The International Electrotechnical Committee (IEC) Technical Committee (TC) 57 was established in 1964 because of an urgent need to produce international standards in the field of communications between the equipment and systems for the electric power process, including telecontrol, teleprotection, and all other telecommunications that control the electric power system.

Having to take into consideration not only equipment aspects, but more and more system parameters, the scope was modified to prepare standards for power system control equipment and systems, including supervisory control and data acquisition (SCADA), energy management systems (EMS), distribution management systems (DMS), distribution automation (DA), teleprotection, and associated communications.

The technical experts of 22 participating countries have recognized that the increasing competition among electric utilities caused by the deregulation of energy markets requires more productivity and efficiency from electric power systems. The integration of equipment and systems for controlling the electric power process into complete system solutions is needed to support the utilities' core processes. Equipment and systems have to be interoperable. Interfaces, protocols, and data models must be compatible to reach this goal.

Since the publication of the first paper, it has become obvious that this standard also needs to support substation automation (SA), asset management, equipment monitoring, wide-area monitoring and control, reliability-centered maintenance (RCM) as well as the associated data-access security. It is also likely that this standard will be one of the vehicles to support reliability management and reporting in the wake of recent blackouts. Data to support these applications are often referred to by others as "non-operational data" because they are not used for commanded control operation today. This term may be familiar, but is inaccurate because many of these data will be used in the future to operate the power system in innovative ways.

Communications traffic on actual substation Ethernet LANs will not be limited to the handful of protocols within the IEC 61850 standard. Substation Ethernet LANs will also support traffic for web server applications in IEDs and HMIs; nonstandard IED protocols such as vendor specific, Modbus IP, and DNP IP, email; legacy SCADA protocols such as IEC 60870; vendor-specific IED configuration and diagnostic applications; network analyzer configuration and diagnostic applications; telephone and camera applications, etc.

Choice of Ethernet LAN

When communications connections are made between integrated IEDs, a trusted, physically distinct local area network (LAN) is created. LANs are created from copper, fiber, and/or wireless media connected in a star or multidrop fashion. LANs are created from EIA-232, EIA-485, Ethernet, and/or various other connections supporting one or many protocols. Hybrid LANs are made from collections of all of these components such that the IEDs interact with one another as if they were all directly connected locally to one another. One or two integrated devices on a pole top comprise a small LAN. Large LANs are created by directly connecting, or bridging, one or more physically separate LANs together using trusted connections.

The design choice within IEC 61850 to use Ethernet was made to leverage the emerging Ethernet technologies being developed for multiple industries. In addition, it makes use of common and familiar visibility tools (such as browsers) and devices that already exist within utility business networks (such as switches, routers, and Ethernet cable). However, the common misunderstanding of direct Ethernet connections between client and IED has also migrated to our market from other industries. Modern Ethernet LANs are most often implemented as star topology, even though they are often logically represented as direct connections. This difference is important to understand during design so that reliability, performance, data latency, and cost of the Ethernet devices are considered. Figure 1 illustrates the difference between logical and actual representations of Ethernet LANs.

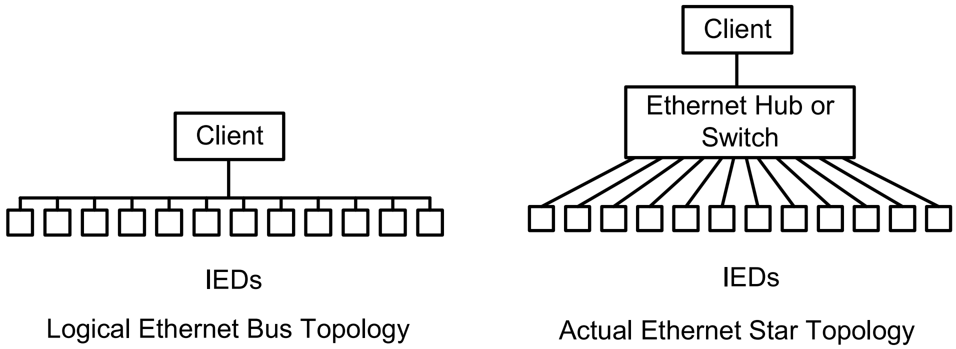

Figure 1 Logical Versus Actual LAN

Briefly, other issues that need to be addressed when designing a network that uses Ethernet include:

- Reaction of networked automation and protection during Ethernet failure
- Communication and IED performance during data storm, hacking, and denial of service attack
- Accidental network overload caused by outside connection or newly connected IED, technician laptop, or test device
- Functionality of IED if the same CPU is performing protection and network communications
  - It is possible for single CPU designs to suspend protection while servicing network communication requests

Station and Process LAN

Within the standardization work, two separate substation LANs are being considered: the station LAN and the process LAN or bus. The station LAN connects all of the IEDs to one another and to a router or other device for communicating outside the substation onto a wide area network (WAN). The process LAN conveys unprocessed power system information (voltage and current samples and apparatus status) from switchyard source devices to the relays or IEDs that process the data into measurements and decisions. For the process LAN, future developments may include microprocessor-based data acquisition units (DAUs), which will act as Current Transformers (CTs), Potential Transformers (PTs), and status indicators. These forward data via a communications connection to the IED rather than the traditional hard wired method. When these data are communicated over fiber connections, isolation is provided between the DAU and the IED. Each individual DAU, such as a CT, is capable of providing data to several IEDs, such as protective relays. DAUs also include intelligent processors imbedded directly in the switch or circuit breaker and merging units (MUs) that merge data from several devices such as CTs or PTs and communicate the values on the process LAN. It is also possible to merge the station and process LANs into one physical communications network.

Peer-to-peer communications are accomplished through direct physical connections or via a virtual direct connection passing through multiple network connections.

A station LAN with all IEDs on one segment and a multiple-segment process LAN design is shown in Figure 2. A merged station and process LAN is shown in Figure 3.

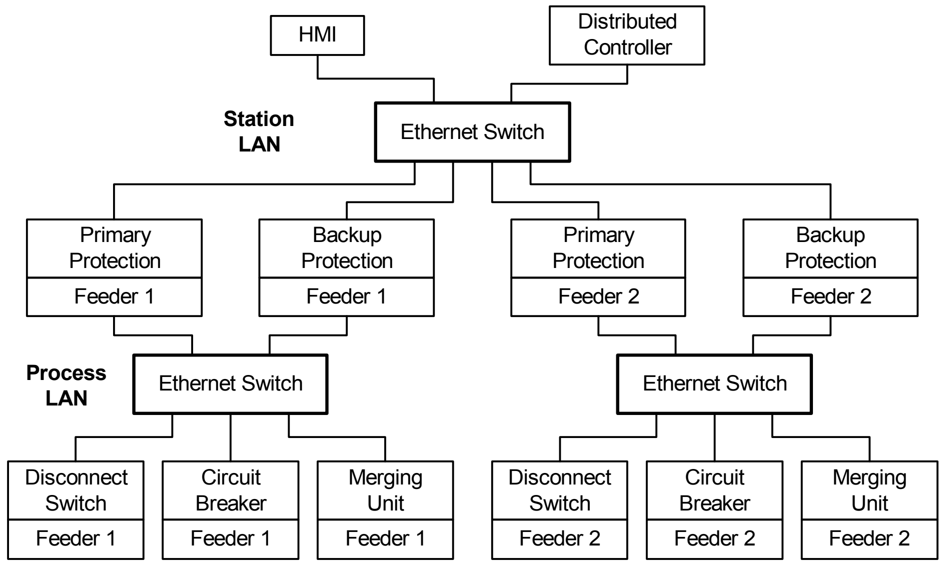

Figure 2 Station LAN and Multiple-Segment Process LAN Design

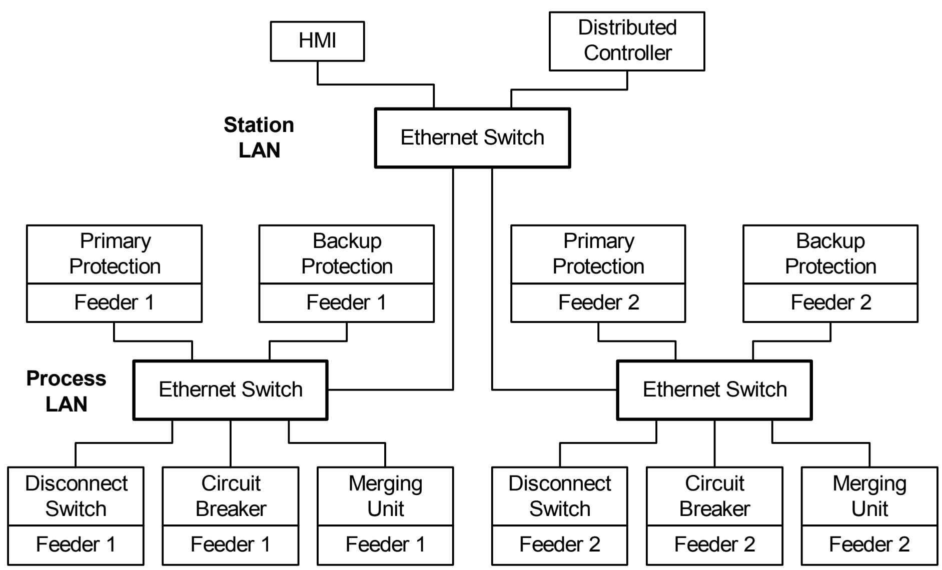

Figure 3 Merged Station and Process LAN Design

External Substation Connections

The IT products in the substation facilitate easy connection to other corporate systems through WAN or Internet connections. These connection possibilities highlight the importance of securing data access connections into the substation LAN. Figure 4 shows a previous substation network design with the addition of external connections.

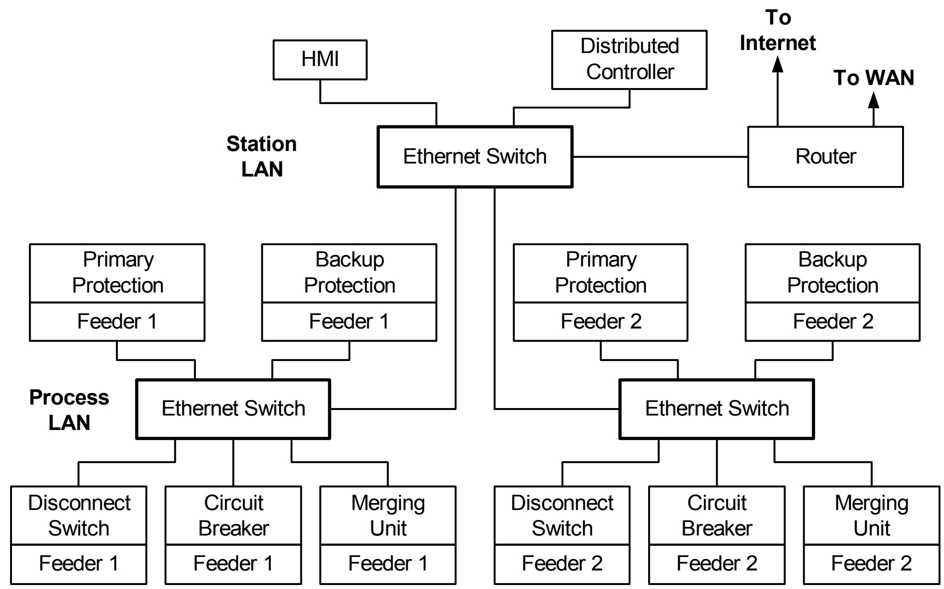

Figure 4 External Connections to Substation Communication Network

Logical Nodes, Logical Devices, and Physical Devices

A logical node (LN) is a collection of data objects, data-set objects, descriptive attributes, report-control objects, log-control objects, log objects, and a list of sampled values which define the boundaries of an entity and its state and behavior. The identification and description explicitly and uniquely identifies each data object within an IED in a standard way. In this way, data objects are uniformly defined by name and function across all IEDs. Logical node classes, data object classes, and their relationship in the context of substations and feeder equipment are defined and used to build the hierarchical names and groups that reference the objects in the IEDs. An example includes IEEE elements, such as LN "distance protection" with LN class name "PDIS" and IEEE number 21.

Peer-to-peer messaging is accomplished with two compliant messages that differ slightly. These two messages, GOOSE and GSSE, are collectively referred to as GSE.

Within IEC 61850, the abstract communications service interface (ACSI) was created to standardize the access to instrumented and calculated data stored in the LN logical groupings. The LNs were designed to represent monitoring and control of power system apparatus without regard for which IEDs, DAUs, and merging units they would reside in. This was done intentionally so that the IEC 61850 standard did not dictate the collection of IEDs required for each protection and monitoring application and ensured that multivendor solutions were possible. The ACSI describes how the data are collected but not where they reside. Therefore, a single multifunction IED can serve LNs for several applications, such as the following:

- protection for more than one feeder
- control of more than one feeder
- reclosing
- metering for more than one feeder

- station battery monitoring
- breaker monitoring for more than one feeder breaker

In this way, designers can choose any combination of IEDs so long as they collectively serve all the necessary LNs. Therefore, at the abstract data level, one solution with two multifunction IEDs can be made equivalent to another solution with five or more single-function IEDs. These can represent two solutions from one vendor, two solutions with one from each of two vendors, or even several solutions with each IED from a different vendor.

Also, the standard was designed to specifically include source IEDs, DAUs, and merging units that do not speak IEC 61850. These devices use various other methods to communicate data to server IEDs or gateways that do support IEC 61850 via the ACSI. These IEC 61850 ACSI server IEDs and gateways map the source data into the appropriate LNs. Server IEDs represent data from DAUs, merging units, or source IEDs as LNs in addition to the LNs they create for locally instrumented or calculated data. Gateways simply create and pass on LNs for the source IED data.

As shown in Figure 5, LNs may reside directly in the source IED, in a gateway, or in a combination of the two, known as a server IED. The LNs are the same, regardless of where they exist. However, if all of the LNs are in one server IED, they all share the same IP address.

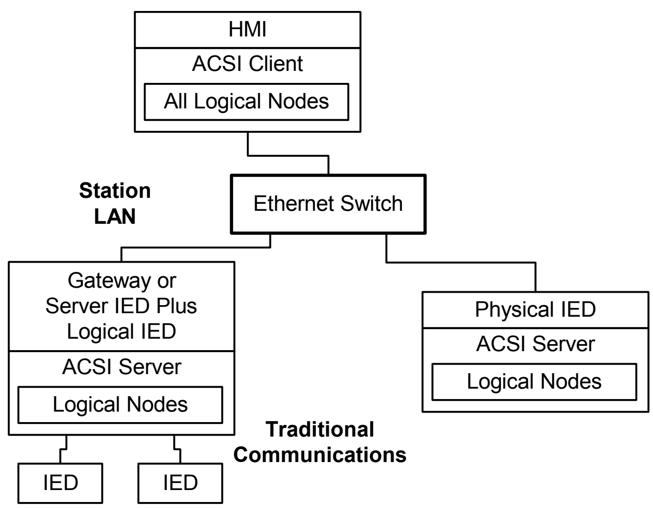

Figure 5 ACSI Server Locations

The standard is most powerful when used to design a system to serve a piece of power system apparatus. Often implemented as a bay, this design process includes the following steps:

- Specify bay application requirements.
- Specify bay integration requirements.
- Design systems of IEDs that satisfy application and integration requirements.
- Choose from several designs that meet application and integration requirements.

The standard is not intended to dictate functionality of IEDs. In light of the fact that each IED functions or performs differently, it is not feasible to use IEC 61850 to dictate IED functionality. However, in some cases, if the complete communications requirements are developed in advance of the system design, they can be used to specify IEDs to meet certain requirements. This design process includes the following steps:

- Specify bay application requirements.
- Specify IED IEC 61850 requirements.
- Identify IEDs that meet these IEC 61850 requirements.
- Design systems with these IEDs.
- Document application and integration capabilities of each design based on capabilities of IEDs.
- Choose design that meets majority of application requirements.

LEGACY SUBSTATIONS AND NONCOMPLIANT EQUIPMENT

Vendors and utilities alike recognize the need to continue use of IEDs that do not directly support the new communications functions described within the standards. There is a huge installed base of existing IEDs that still have value. The very important strategy of the IEC 61850 standard development to support IEDs that are noncompliant with IEC 61850 had a two-fold purpose. First, designers can leverage the investment of in-service and useful IEDs. Second, designers can choose new IEDs that best fit performance or cost criteria, regardless of whether or not they directly support IEC 61850, and incorporate them via compliant gateways or server IEDs. Figure 6 illustrates a hybrid Ethernet and serial LAN.

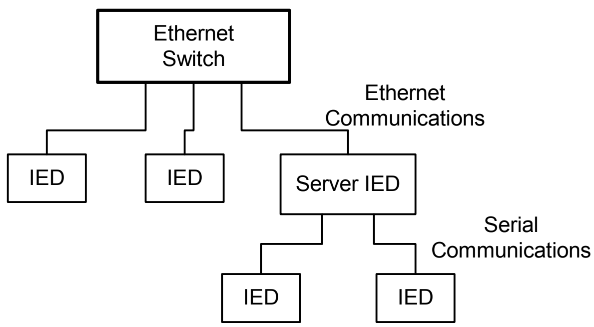

Figure 6 Hybrid Ethernet and Serial LAN

IEC 61850 LAN DESIGN OBSERVATIONS

Design Impact for Protection Communications

Network designers want to keep traffic to a minimum and reduce the number of messages to be processed, while IEDs consume and serve peer-to-peer GSE messages and serve up LNs. Further, consideration should be made to ensure that failed or attacked networks affect as few devices as possible. Finally, designers need to choose IEDs that will continue to function if they reside on a failed or attacked network.

Substation Configuration Language

Substation configuration language (SCL) files were created within the IEC 61850 standard as a means to standardize the method of describing communications capabilities within IEDs. This file simplifies some configuration between the IEC 61850 client and the IED, or IEC 61850 server, namely integration of LNs and GSE messages. Initially it was thought that these SCL files would be best collected directly from the IEDs, essentially a self-description method. However, it was quickly realized that system designers rarely have each specific IED at their disposal during the settings implementation phase. Designers work at their desks while the IEDs are at the panel shop or substation. Therefore, SCL files are distributed via a combination of electronic storage and email as well as directly from the IED.

Majority of Configuration Tasks Not Addressed

The SCL files do not accomplish the larger task of configuring the IED to perform its primary tasks. A common misconception exists that SCL files support automatic, total application configuration of multivendor IEDs as well as configuration of GSE communications. However, individual vendor settings software is still required to configure each IED via proprietary methods.

Another large part of network design involves interlocking, distributed protection and specialized automation. This task is also not addressed by the standard. Logic within the IEDs must be created and installed into each IED using unique vendor-specific software. No tool or standardization exists to aid in the design or creation of the distributed logic or associated GSE allocations.

Interoperability Among IEC 61850 Clients and Servers

One driving force behind the creation of IEC 61850 was to better accommodate interoperability among IEDs from multiple vendors. The standardization of GSE messages ensures interoperability directly between IEDs for protection, interlocking, and automation. Although the two messages are different, they can both exist on the network and provide interoperability between multiple devices that support GSSE and/or between multiple devices that support GOOSE or both. Further, the content of these messages is configurable to satisfy IED and system requirements. Therefore, even if two IEDs support the same message type, design and configuration must be performed to make the IEDs interoperable.

A second driving force behind the IEC 61850 was standardization of data acquisition and description methods to reduce the integration effort. Vendors can then support fewer standardized and proprietary communications methods and better focus on making the best IEDs possible to serve the electric power system. Network designers will find mapping consistently named values into database locations and operator displays much easier than understanding a unique method for each IED. The process of IEC 61850 clients discovering available LNs within locally connected IEC 61850 servers has even been automated.

However, an important detail to recognize is that the IEC 61850 standard addresses data acquisition and data description methods but does not dictate that the data exist in the IED ACSI. The majority of the LN content described within the IEC 61850 documentation is optional, may not exist, or may not be mapped. Also, IEC 61850 does not standardize which LNs must exist in the IED. Further, even if different IEDs support some or all of the same logical nodes, it does not standardize which data will be available. In other words, each IED may have a different collection of LNs and the same LN in different IEDs may have different amounts of data. Compliance is simply measured by verifying that the IED supports the LNs and data identified in its SCL.

This obviously presents several problems for the network designer:

- It may become necessary to acquire the SCLs, or descriptions thereof, well in advance of selecting IEDs.
- Although each IED may create and provide a wealth of information, the network designer only has access to the subset that is mapped into the LNs.
- IEC 61850 implementation, and therefore available data, will most likely differ between IEDs.

An additional challenge is file transfer. IEC 61850 supports both FTP and MMS file transfer. These two methods standardize the mechanism used to transfer files of data between clients and servers such as settings, event records, and lists. However, IEC 61850 does not standardize the contents. Therefore, it is not required nor expected that these files be consistent or interoperable among different vendors or different products from one vendor.

Interchangeability Among IEC 61850 Clients and Servers

The IEC 61850 standard was never intended to ensure interchangeability of IEDs because of their inevitable unique inner workings and performance. However, it has become apparent that utilities would like to see interchangeability at the ACSI level so that they can freely choose between IEDs and vendors with respect to integration. The observations listed in the previous section, namely that the standard does not specify LNs or contents to be supported, make interchangeability difficult or impossible. Interchangeability or interoperability will definitely not be ensured by the standard. Utilities can bring this about only by describing in advance the required LNs and contents. This in turn ensures interchangeability and interoperability at the ACSI level for that customer, for a specific application, and for a specific group of IEDs.

IEC 61850 LAN Practical Implementation Observations

Design Impact for Protection Communications

Serially integrated LANs are fast, reliable, and reduce IED message processing to a minimum because they physically isolate each IED from unnecessary traffic. Serially connected IEDs receive and process only messages sent directly to them.

In order to keep network message processing to an appropriate minimum and minimize the effect of failed or attacked networks, LANs are separated into connected yet separate segments. On these segments are the IEDs that serve a segment of the electric power system. These segments are designed to be as small as possible through physical or virtual means. For small stations, a single LAN is still appropriate, however, for larger systems LAN segment design has followed the natural progression toward serving a bay, or small collection of interrelated electric power system apparatus and functions. Because of their geographical proximity and logical association, integrated IEDs of a single bay are efficiently separated into physically isolated LAN segments. A segment is made up of a bay Ethernet switch and collections of IEDs performing monitoring, control, protection, and local operator interface. At a minimum, this usually consists of a bay control unit (BCU), bay monitoring unit (BMU), bay protection units (BPUs), and a bay Ethernet switch. More sophisticated automation systems include additional equipment monitors, station battery monitoring systems, weather stations, controllers, LTCs, and other IEDs. Communication design within the bay is done based on the capabilities of the chosen IEDs. Figure 7 illustrates multiple bay LAN segments.

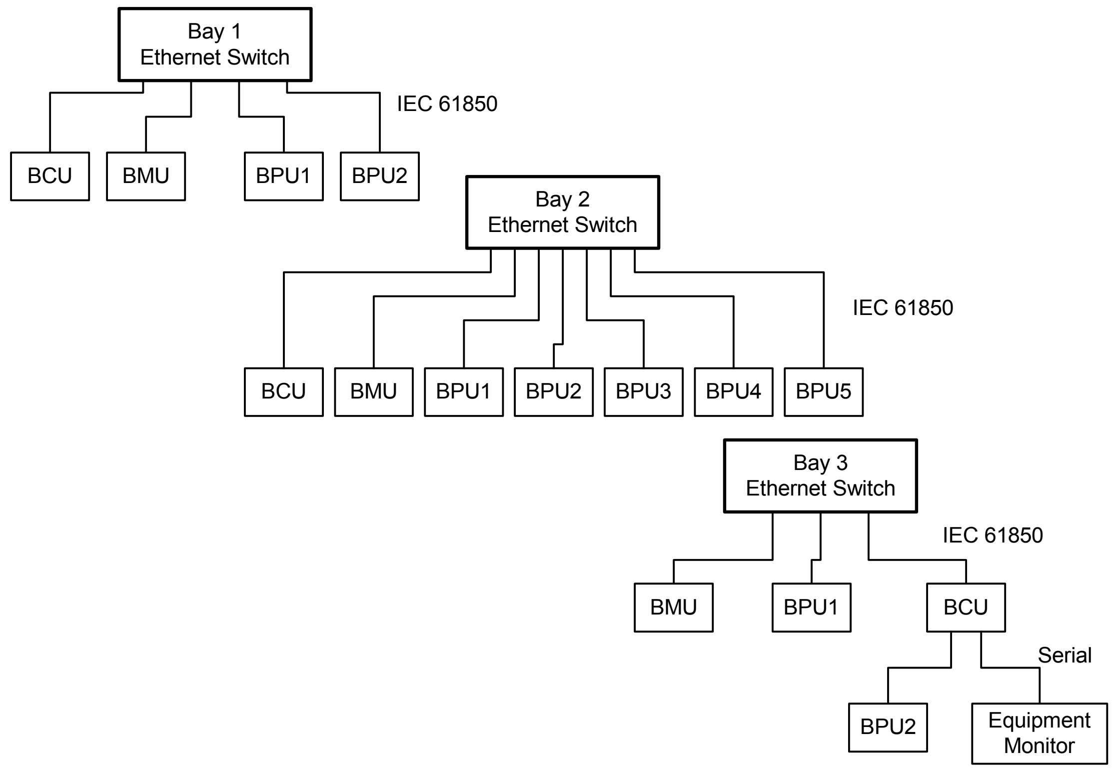

Figure 7 Multiple Bay LAN Segments

The station LAN is visualized as a station control unit (SCU), a station Ethernet switch, and connections to each bay Ethernet switch. Additional station-level devices may include protocol translators, engineering workstations, and web-based operator interfaces. Communications design between the SCU and each bay is done based on the functional requirements of managing the power system apparatus associated with the bay. Figure 8 illustrates the simplified logical view of a station comprised of the three bay LANs in Figure 7. Each of the three bay designs in the example can function differently or the same within the substation LAN. In the example where all three function the same, it can be seen that three different IEC 61850 compliant designs serve the same data, yet have different quantities of IP addresses and GSE messages.

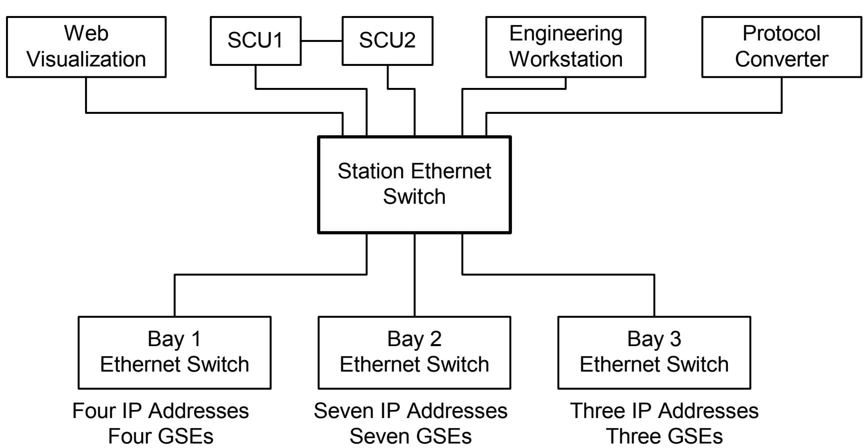

Figure 8 Logical View of Station LAN

Interoperability Among IEC 61850 Clients and Servers

Design of integration at the IED level is standardized yet still difficult to implement in practice. The IEC 61850 standard is most effective when used to design management of power system apparatus and then choose combinations of IEDs to serve that purpose. Choosing a specific collection of IEDs first restricts the power system apparatus management to what the IEDs can support. Further, if the requirements change, they can only be accommodated if the IEDs are modified through a vendor product development and upgrade process.

The migration toward bay-oriented LAN segments, each with their own Ethernet switch, simplifies multivendor interoperability at the bay level. Bay LAN segments are designed to manage corresponding power system apparatus such as distribution feeders, transmission terminals, and transformers. The end user not only defines the functional, performance, reliability, availability, and physical requirements, but also the IEC 61850 communications requirements. Vendors then design bay networks of IEDs and communications to satisfy the requirements. The end user is free to choose among the bay designs based on their chosen acceptance criteria. It is also possible, and in some cases required, to permit communications methods other than IEC 61850 within a bay hybrid LAN. Data from these non-IEC 61850 communications methods are mapped to LNs and GSE via a gateway or server IED and then transferred to the station LAN. The station network design can integrate bays from several different vendors, each with a standardized IEC 61850 interface.

Since each different bay LAN design may have different types and quantities of IEDs, each bay LAN will obviously have different distributions of LNs and GSE messages. Therefore, LNs and GSE messages between the station server and each different bay LAN design, and between bay LANs, will be compliant with IEC 61850 and yet different. Referring to a previous example (Figure 8), all of the LNs in a bay LAN with four multifunction IEDs (Bay 1) will have one of four IP addresses and there will be a minimum of four possible GSE messages. In a functionally equivalent bay with seven single-function IEDs (Bay 2), the same LNs will have one of seven different IP addresses and there will be a minimum of seven possible GSE messages.

Therefore, interchangeability at the bay level, rather than the IED level, will be much more useful and feasible.

Interoperability Between Existing Control Systems and Bay LANs

Utilities still use traditional telecontrol methods to send commands from the control center to the substation. Legacy SCADA protocols, DNP3, or IEC 60870 protocols need to be converted into IEC 61850 commanded control. This is presently done via an interface with the SCU that translates the SCADA command into an IEC 61850 message, which, in turn, is sent to the appropriate bay. Prior to passing on the command, the SCU checks the status of station level jurisdiction, permissions, tags, and interlocks to make sure the command is locally authorized. As with the other station data, the resulting status change is collected by the station server via an IEC 61850 LN and then translated into a SCADA message and sent to the control center.

Many utility designs require that remote control commands to the bay LAN be administered through the BCU rather than directly to the IED protecting the apparatus to be controlled. After receiving the commanded control from the SCU, the BCU performs a validation process, similar to the SCU, of bay-level jurisdiction, permissions, tags, and interlocks to make sure the command is locally authorized. The BCU then executes the command directly or passes a command message to an IED via IEC 61850, some other Ethernet protocol, or any number of other communications methods. This centralized bay LAN control authorization requires that the BCU communicate with the IEDs instead of, or in addition to, the IEDs communicating directly through the bay and station Ethernet switches to the SCU.

Interoperability and Interchangeability Between IEC 61850 Clients and Servers

Use of a global communications standard, like IEC 61850, provides the ability to predict how data will be moved and identified between clients and servers from any manufacturer. Again, the standard does not dictate which data will be present, but rather, if data do exist, how they will be moved and recognized. The most obvious benefit of this predictability is that the standard simplifies the integration effort in several ways.

- SCL file information uses standardized names and attributes to reduce the integration effort associated with creating a client database.
- Standardized SCL file format allows automated processing of portions of the client database.
- Integration between a client and multiple server IEDs with identical IEC 61850 interfaces will be the same and can be reused.
- Standardized LN nomenclature uses standardized names and attributes to reduce the integration effort associated with creating operator interfaces, logic, and control.
- Existing data within server IEDs, not previously mapped to LNs, can be easily exposed in compliance with IEC 61850 because IEC 61850 not only describes LNs but also describes standard methods to extend existing LNs to include new information and also how to create new LNs.
- When IEDs are modified, descriptions of their new IEC 61850 capabilities are available within a new SCL file.

VERIFICATION OF IED PERFORMANCE

The final part of IEC 61850 is Part 10, Conformance Testing. This part documents testing to verify that IEDs support the capabilities described within their SCL file. However, IEC 61850 LAN designers also need to be concerned about other IED performance characteristics not included in Part 10, such as the following:

- Time synchronization and time-stamp accuracy
- Control reaction time
- Operational and reliability criteria

These characteristics need to be requested from the IED vendor separately. This information is essential because of the nature of networked IEDs being used to design systems of interoperable devices working in a coordinated fashion. These, and other device performance measures, are essential information for predicting performance, functionality, and reliability of designs executed by networked IEDs.

It may not be possible, or necessary, for the end user to document specific performance benchmarks for each IED to meet, however, verification and delivery of the actual performance measures performed by the vendor need to be requested by the end user. In other words, the end user does not need to state what performance is required in advance, only that the performance is measured by the vendor and documentation of this is provided with the IED. Using these documented performance measures, design engineers can predict the performance of the interconnected IEDs and thus the performance of the system. Further, engineers will be able to identify suitable devices for specific applications.

This observation has already been proven to be true. In a recent demonstration, an IED that had passed certification was added to a demonstration IEC 61850 LAN comprised of IEDs from multiple vendors, and did not function as expected. This appeared to be caused by the unanticipated traffic patterns on the network. This simple example showed that the performance characteristics mentioned in this section, that are not included in IEC 61850 part 10, will determine the success of actual networks. The IED did pass the certification tests but did not perform the necessary functions on the LAN. Since true LAN performance is difficult to predict, understanding IED performance characteristics will be as important, or more so, than certification of specific data mapping attributes.

Time Synchronization and Time-Stamp Accuracy

Time-stamp accuracy documents the ability of the IED to communicate time-stamp information about an instrumented event. An accurate time stamp relies on several separate functions including accurately decoding the received signal, accurate synchronization of the IED clock to the received signal, timely IED detection of change-of-state, and accurate use of the IED clock value to time stamp data. However, to the end user, the most vital measure is how accurate the time stamp associated to the data record of the event is relative to the actual time of the event.

Control Reaction Time

The scope of this control reaction time measure is to verify the speed with which each IED is able to react to an incoming GSE or IEC 61850 commanded control (GCNTL) message or create an outgoing GSE or GCNTL message.

For incoming GSE and GCNTL messages, the documentation should identify the time latency between the IED receipt of the incoming message and a logical change of state in the IED and/or a physical contact output change of state. For outgoing GSE and GCNTL messages, the documentation should provide the time latency between the logical change of state in the device and/or a physical contact input change of state and the transmission of the associated GSE or GCNTL message.

Operational and Reliability Criteria

These performance measures document device reliability and operation characteristics. Network and application designers need reliability and operational information about monitoring, protection, control, and communications devices so that they may perform appropriate risk analysis and reliability design. Using these provided performance measures, designers can choose appropriate devices, specify appropriate redundancy, and identify appropriate communications technologies to satisfy network and application reliability and operational criteria.

Operational Criteria

Operational criteria determine whether the devices are appropriate for the environment in which they will be placed.

Operating Temperatures

For each device, the temperature range for normal operation shall be specified.

Suitability for Substation Environment

At a minimum, compliance or noncompliance to the following standards shall be specified.

IEEE C37.90.1: IEEE Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems

IEEE C37.90.2: IEEE Trial-Use Standard Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers

IEEE 1613: IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations

IEC 68-2-30 Damp heat, cyclic (12 + 12-hour cycle)

Humidity, 95% between 25° and 55°C

IEC 255-5 Impulse voltage test: 0.5 Joule, 5000 Volt

IEC 255-21-1 Vibration test (sinusoidal)

IEC 255-21-2 Shock and bump tests

IEC 255-22-1 Electrical disturbance tests for measuring relays and protection equipment

IEC 801-2 Electrical discharge requirements

IEC 801-4 Electrical fast transient/burst requirements

Reliability Criteria

Failure Rate

Observed failure rate is the quantity of each type of device that fails per year for a given population.

Mean Time Between Failure (MTBF)

MTBF is the measure of the verified hardware failure incidence for each IED. This is calculated as the accumulated years in service divided by the number of devices returned for component failure.

Mean Time Between Unscheduled Removals (MTBR)

MTBR is the measure of the unscheduled removal incidence for each IED. This is calculated as the accumulated years in service divided by the number of devices returned for confirmed component failure plus those returned with no problem found.

Reliability criteria are used to predict the performance of the resulting design and are used to perform the following:

- Identifying mission-critical components.
- Verifying device and system reliability.
- Assessing device and system risk.
- Investigating accidents/incidents.
- Evaluating design changes.
- Displaying the causes and consequences of events.
- Identifying common-cause failures.
- Predicting quantity of device failures over time.
- Predicting maintenance effort and cost over time.

CONCLUSIONS

Design Impact for Protection Communications

The standardization of GSE messages ensures interoperability directly between IEDs for protection, interlocking, and automation. Although the two messages, GOOSE and GSSE, are different, they both coexist on the network and provide interoperability between multiple devices that support GSSE, and/or between multiple devices that support GOOSE, or both.

Bay LAN segments keep network message processing to an appropriate minimum and minimize the effect of failed or attacked networks.

Interoperability Among IEC 61850 Clients and Servers

Designs created by defining strict IEC 61850 requirements at the IED level unnecessarily restrict the choice of IEDs and or the available functionality of the bay LAN.

Serially integrated LANs are fast and reliable, and reduce IED message processing to a minimum because they physically isolate each IED from unnecessary traffic. Serial connections to IEDs within a bay Ethernet LAN create a hybrid LAN. This hybrid LAN allows the network designer to choose from all new and in-service IEDs including BCUs, BMUs, BPUs, equipment monitors, weather stations, controllers, LTCs, meters, and battery monitoring systems. Therefore, installed investments can be leveraged and a wider selection of IEDs can be used to create substation automation systems.

Communications among IEDs within a hybrid bay LAN can be performed using IEC 61850, other Ethernet protocols, or other direct communications methods. This allows access to relevant IED data that are not presently exposed as part of the IED-IEC 61850 interface.

The migration toward bay-oriented LAN segments, each with their own Ethernet switch, simplifies multivendor interoperability at the bay level. IEC 61850 communications requirements defined at the bay level, permit use of the data modeling within the standard to satisfy application requirements associated with power system apparatus management.

Bay level interoperability allows end users to choose from bay LAN designs from multiple vendors based on functional, performance, reliability, availability, physical and communications acceptance criteria. These bay designs may be functionally equivalent, but still have different quantities of IEDs, LN addresses, and GSE messages.

Although initial IEC 61850 designs have focused on performing protection and SCADA replacement, more sophisticated future substation automation designs will likely require that the BCU communicate with the other bay IEDs and provide a centralized and concentrated data store and processing environment.

Data access security requirements may require other modifications to LAN segment design.

Reliability concerns virtually dictate that BCUs should support redundant, separate, physical Ethernet connections.

Interoperability Between Existing Control Systems and Bay LANs

Centralized bay LAN control authorization requires that the BCU communicate with the BMU, BPUs, and other IEDs instead of, or in addition to, the IEDs communicating directly through the bay and station Ethernet switches to the SCU.

IEC 61850 was designed for use within the substation and for IED quantities associated with a substation. Current implementations require that IEC 61850 be converted to legacy telecontrol protocols for communications to the remote control center.

Presently, substation LAN traffic is high enough that LAN segmentation is necessary. Therefore, even when high-speed Ethernet connections between the remote control center and substation are possible, the remote control center may not be capable of managing the process burden of communications directly to each IED. SCUs or BCUs will need to act as single points of contact to communicate data and control.

Interoperability and Interchangeability Among IEC 61850 Clients and Servers

The IEC 61850 standard is most effective when used to design bay LANs and when combinations of IEDs are then chosen to serve that purpose.

If the end user provides detailed IEC 61850 communications requirements in advance, vendors can develop the necessary IEC 61850-IED interface. This implementation satisfies the end user until new data requirements are recognized. This implementation may not satisfy other end user requirements and may need modification for each situation.

Existing data within server IEDs that are not presently mapped to LNs can be exposed to the IEC 61850 LAN when existing LNs are extended or new LNs created.

Standardized names and attributes enable standardized LN nomenclature to reduce the integration effort associated with creating operator interfaces, logic, and control. However, when one bay LAN is replaced with another containing different LN and GSE characteristics, the database, logic, and operator interfaces will need to be reconfigured. If the characteristics are the same, this integration effort can be reused.

Some end users intend to require that it be possible to replace any IED within a bay LAN with another IED from any manufacturer. This is referred to as interchangeability. Replacement of one IED by another may affect the function of the coordinated system because of the different operating principles used by different IED vendors. However, a hybrid LAN is capable of supporting interchangeability with many different IEDs at the IEC 61850 communications interface level. Appropriate LN and GSE interfaces are created in the new IED or within server IEDs on the LAN.

Realities of Moving From Design to Implementation

Communications traffic on actual substation Ethernet LANs will not be limited to the handful of protocols within the IEC 61850 standard. Substation LANs will also support traffic for web server applications in the IEDs and HMIs, nonstandard IED protocols such as vendor specific, Modbus IP, and DNP IP, email; Legacy SCADA protocols such as IEC 60870; vendor-specific IED configuration and diagnostic applications; network analyzer configuration and diagnostic applications; telephone and camera applications, etc.

The present certification method accomplishes only part of the necessary task to ensure a successful installation. The network designer must make sure that the IED supports the necessary data requirements and that the IED performance characteristics mesh with the other components to create a successful network. Finally, it seems clear that a flexible data mapping technology at the IED and bay level will make the physical application of an IEC 61850 network much easier to accomplish.

Reference

[1] Eric Udren, Steven Kunsman, Dave Dolezilek, "Significant Substation Communication Standardization Developments," Proceedings of the 2nd Annual Western Power Delivery Automation Conference, Spokane, WA, April 4-6, 2000.

Biography

David J. Dolezilek received his BSEE from Montana State University in 1987. He worked as project engineer and manager for the Montana Power Company and the California Department of Water Resources prior to becoming self-employed as a control system consultant. He joined Schweitzer Engineering Laboratories, Inc. in 1996 as their first system integration engineer. Dolezilek became the Director for North American Sales in 1997, R&D Engineering Manager for Automation and Communications Engineering in 1998, and Automation Technology Manager in 2000, to research and design automated systems. In 2003, Dolezilek became Sales and Customer Service Technology Director. He is the author of numerous technical papers and continues to research and write about innovative design and implementation affecting our industry. Dolezilek participates in numerous working groups and technical committees. He is a member of the IEEE, the IEEE Reliability Society, Cigre WG 35.16, and the International Electrotechnical Commission (IEC) Technical Committee 57 tasked with global standardization of communication networks and systems in substations. He holds US Patent number 6,655,835, titled "Setting Free Resistive Temperature Device (RTD) Measuring Module."