More Than Communication – the Engineering Approach of IEC 61850

Tim Tibbals and Dave Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
2nd International Conference on Advanced Power System Automation and Protection
Jeju, Korea
April 24–27, 2007

More Than Communication – the Engineering Approach of IEC 61850

Tim Tibbals and Dave Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—IEC 61850 is a very large standard with many functions and services within it. End users implement different combinations of the functions and services for the different features they provide. The IEC 61850 standard Parts 3 and 4 provide methods of developing best engineering practices for substation protection, integration, control, monitoring, metering, and testing in order to effectively use what is available in the products and tools in the market.**

When designing and implementing an IEC 61850-based substation automation system (SAS), it is important to not only specify the use of IEC 61850, but also what parts of the standard are to be used and, more importantly, the system performance. In addition to the details of the standard, there are also implementation details left to the discretion of the vendors that are not dictated by the standard and need to be documented as requirements in order to attain the required system functionality. The following is a sample of these details:

- **Quantity of client/server associations to the device**
- **Quantity of peer-to-peer messages the device will publish or transmit**
- **Quantity of peer-to-peer messages the device will subscribe to or receive**
- **Number of characters allowed in the device name**
- **Run-time device diagnostics**
- **Configuration of the device via SCL (substation configuration language) XML files instead of settings**

I. Engineering Requirements

The engineering requirements of an SAS are independent of the protocol selection. The protocols and methods used for communication within an SAS should be chosen to achieve the system requirements. Because of this, it is imperative to create the definition of the SAS as a first step. The automation system is a collection of hardware and Intelligent Electronic Devices (IEDs) that are connected via communications to the SAS as shown in Fig. 1.

The requirements of the communications are based on the functions defined by the users of the SAS in addition to the users of the IEDs. The two typical categories of users of the SAS within a utility are the protection engineers and the automation engineers. There may also be others. The SAS design and implementation must accommodate all users to be successful. The detailed discussion of the engineering process is best done using examples. For the purposes of this paper, the system described in the one-line diagram of Fig. 2 shall be used.

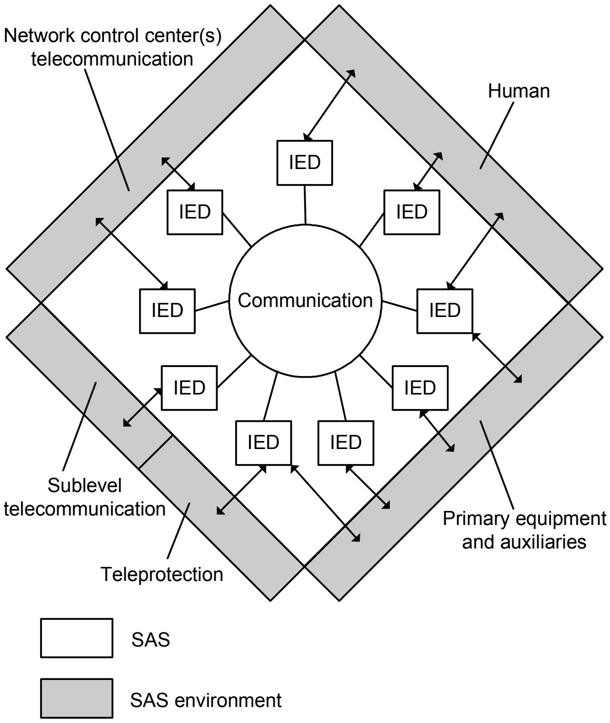


Fig. 1. Structure of the SAS and its environment

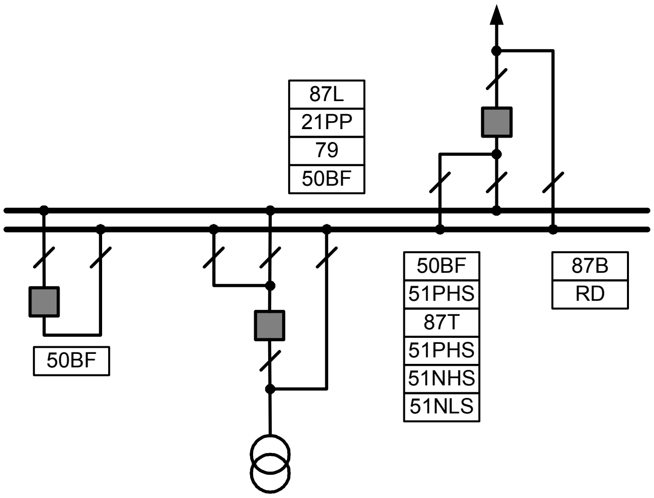


Fig. 2. Substation protection requirements

A. Flexibility and Expandability

The example substation is part of the associated transmission network to a wind farm and, in the first stage, will be a 34.5/230 kV step-up substation. One hundred wind generators in groups of 20 will be connected to the 34.5 kV bus. In 230 kV, a main bus/auxiliary bus arrangement will connect the wind farm to the national grid. The one-line diagram of the 230 kV side is displayed in Fig 2.

The following are the requirements for the system:

1. Ensure interoperability between protection and control devices.
2. Comply with functionality of user protection specification.
3. Comply with functionality of automation specification.
4. Design for interchangeability of main IEDs at the communications interface.
5. Connect IEC 61850 bay control and protection devices to the Ethernet; allow no data concentrators for local operation.
6. Perform bay control interlocks between bays using GOOSE messages.
7. Communicate with two master stations using redundant SCADA gateways with legacy protocols.
8. Provide two local HMIs.

B. *Flexibility and Expandability*

The SAS design for interchangeability utilizes IEDs from multiple vendors. The IEDs are selected and matched based on protection and data functionality as modeled in IEC 61850. The system integrator defines the rules for logical devices, logical nodes, controls, and data mapping with customer input. The system integrator is also responsible for defining HMI and gateway databases. The customer defined master station databases that the gateway databases must support. Tables I–V list the protection requirements for each protection panel.

TABLE I
230 KV LINE PROTECTION PANEL

Description	Function
Bay Control	Local Control and Data Acquisition
Main Distance Protection Directional Overcurrent	21/67
Main Line Current Differential Directional Overcurrent	87L/67
Breaker Failure/Synchronism Check	50 BF/25/27
Reclosing	79

TABLE II
230 KV TRANSFORMER PROTECTION PANEL

Description	Function
Bay Control	Local Control and Data Acquisition
Main Transformer Protection	87
High Side Overcurrent Protection	50/51 HS
Breaker Failure/Synchronism Check	50 BF/25/27
Low Side Overcurrent Protection	50/51 LS
Neutral Overcurrent Protection	50/51 N
Tertiary Overcurrent Protection	50/51 TZ

TABLE III
230 KV TIE BREAKER PROTECTION PANEL

Description	Function
Bay Control	Local Control and Data Acquisition
Breaker Failure/Synchronism Check	50 BF/25/27

TABLE IV
230 KV BUS DIFFERENTIAL PROTECTION PANEL

Description	Function
Bus Differential	87B

TABLE V
AUXILIARY BAY PANEL

Description	Function
Backup Bay Control	Local Control and Data Acquisition
Backup Line Current Differential Backup Distance Protection	21/87L
Backup Transformer Protection	87

C. *Scalability*

1) New Substation Technology: Bay Control, SCADA Gateway, and IEC 61850

In addition to using the new IEC 61850 standard, the SAS design often incorporates products that the customer has not used before. All of the protective relays must be approved for use by the customer on their system regardless of their support of IEC 61850 protocols. This SAS final design relies heavily on several relays that the customer previously approved and used in other integration systems that use other protocols and now also support IEC 61850. Other IEDs, such as the bay control units, were approved by the customer for use on this system. Fig. 3 illustrates the front-panel HMI on the bay control unit used in the 230 kV tie breaker protection panel.

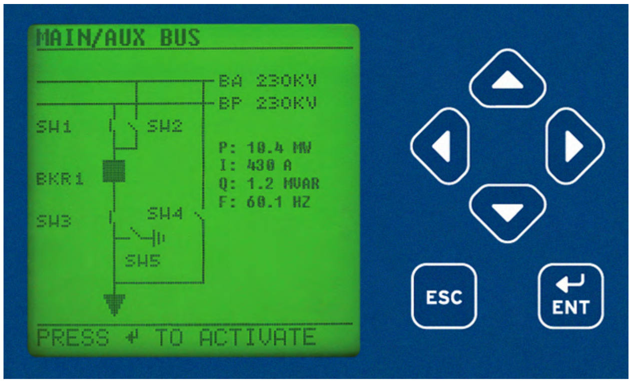


Fig. 3. Front-panel HMI on the bay control unit used in the 230 kV tie breaker protection panel

The SAS design requires that the system integrator work with every IED from each vendor to understand and implement the IEDs, each with different IEC 61850 capabilities, into the communications architecture.

New work is being done by the IEC Technical Committee (TC) Working Group (WG) 57 to extend use of the protocols within the IEC 61850 standard to outside the substation.

Presently they are not used outside the substation, and the designs still rely on traditional and in-service SCADA protocols. The customer needed to support existing DNP3 links as well as the bit-oriented Conitel 2020 protocol. A rugged computer was deployed as a gateway to act as a client, collect and concentrate data from the IEDs via IEC 61850 protocols, convert these data into SCADA protocols, and serve them to the existing SCADA consoles. Therefore, in addition to acting as a protocol gateway, the rugged computer is a data concentrator and a client/server. Fig. 4 illustrates an example SCADA console similar to the ones in the project. The data collected via IEC 61850 protocols are converted into DNP3 and Conitel 2020 and transferred over established SCADA links. The operators are unaware of the fact that the substation protocols are different than previous designs that used DNP3 and other protocols in the substation. Even though this example substation used DNP3 and Conitel 2020, this SAS design can accommodate virtually any SCADA or control center protocol.

Fig. 4. Typical SCADA console user unaffected by choice of protocol within the substation

The major impact of using IEC 61850 in this project and then converting it into traditional and legacy protocols is the dramatic increase in complexity of the new IEC 61850 protocols. Because some of the new IEC 61850 protocols are more functional, they have more features and attributes that do not exist in other protocols like DNP3 and Conitel 2020. Therefore, it is difficult to convert simple DNP3 messages to perform actions that are more elaborate in the IEC 61850 protocols. One such example is commanded control. IEC 61850 protocols require six or more attributes to be set before an IED will act on it. The simple DNP3 command structure requires only two. Therefore, there is not a one-to-one correspondence of necessary protocol attributes to complete client/server transactions. This eliminates the opportunity to automatically map configuration between the protocols and creates the need for much manual configuration of the protocol translation. This translation effort can be the most time consuming part of the system integration activity. Additionally, commands and other message transactions via IEC 61850 methods benefit from object-oriented data structures; however, some of these data structures include data types that are not available within the other protocol methods. Therefore, not only must missing data attributes somehow be created, existing data attributes often must be converted from one type to another.

2) *New Software Automatically Creates Communications Settings and Configuration*

New IEC 61850 configuration methods work in conjunction with previously existing IED application configuration software to create designs and set relays and other IEDs to perform logic, interlocks, and protection. The best practice method mentioned in the standard relies on the creation of a configured IED description (CID) file, which uses SCL to describe all of the IEC 61850 protocol configurations, and is then downloaded directly into the IED. When the IED starts up, it finds the CID file and performs self-configuration. This file is locally or remotely transferred into the IED without impacting any other functionality in the IED. Because this configuration is an IEC 61850 communications configuration file only, there is no opportunity to inadvertently impact protection or automation settings. Therefore, the communication is configured, tested, and commissioned without impacting the other applications within the IED. Furthermore, this CID file is also retrieved directly from memory within the IED to definitively verify what configuration is being used by the IED. Fig. 5 shows an approach when a software tool used to combine information from all IED CID files is combined with visualization information to create a system file or system configuration description (SCD) file.

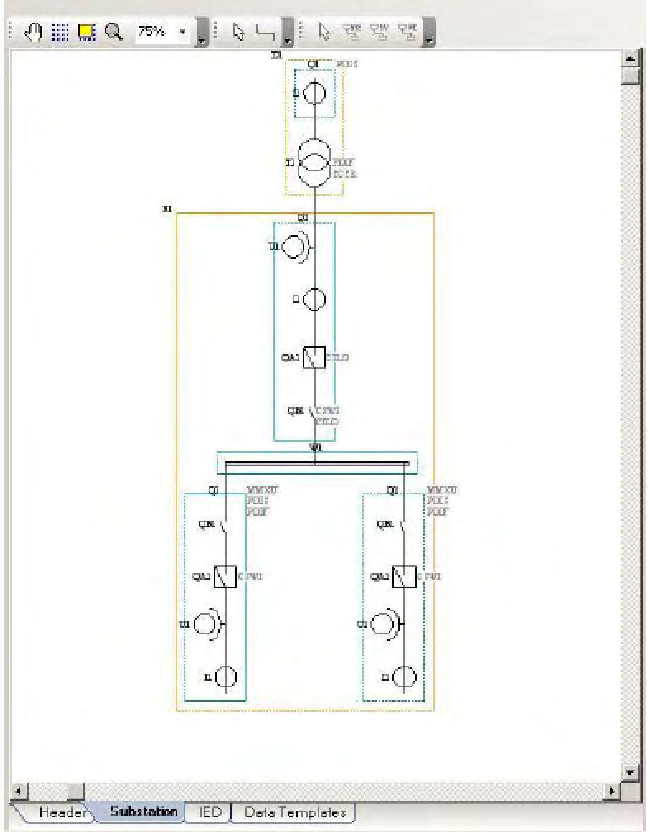


Fig. 5. Example substation drawing and configuration tool

Because the IEC 61850 standard does not specify a single way to perform configuration, several vendors chose to add IEC 61850 configuration as settings among the existing protection and automation settings within their IED. For these IEDs, the protection-settings software is used to create and download all the settings into the IED. Care must be taken to preserve, test, and commission all affected, or possibly affected, settings. The upper portion of Fig. 6 illustrates the relationship between IEC 61850 configurations via designs saved as files to be distributed using traditional file transfer means, like FTP, and directly loaded into local or remote IEDs. The lower portion of Fig. 6 illustrates protection and automation settings being created and the IED being set with a separate, special-purpose software application.

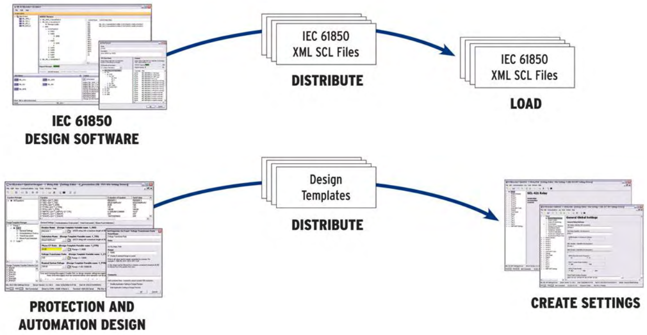


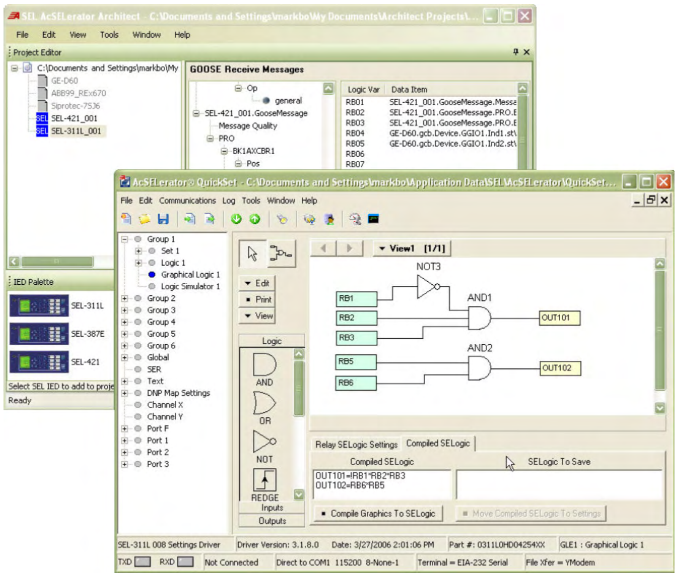
Fig. 6. File configuration of IEC 61850 and protection and automation settings configuration

For those IEDs that support the necessary SCL files and the standardization of their format, configuration software from any vendor should be able to view data descriptions within the SCL files that represent the system needs and IED capabilities. This allows the designer to visualize and logically connect data among IEDs from any vendor.

Using the methods described in the standard, IEC 61850 configuration software allows the designer to create data groups and reporting methods that identify what data are sent, how they are sent, when they are sent, and under what conditions.

Once the IEC 61850 configuration software imports files representing the capabilities of IEDs, designers make use of these capabilities to exchange data among the IEDs. After the configuration files or settings are installed in the IEDs, they report data to SCADA gateways, engineering workstations, sequential events recorders (SERs), etc., as well as to each other. Once an IED is configured to receive data from another IED via the IEC 61850 protocol GOOSE, the IED has access to that information as a logical status with the value of a binary one or zero. To the IED, this is now the same as a binary status received any other way, such as the mirror of the state of a bit in another relay via a peer-to-peer serial protocol, a commanded change of state via a SCADA command, a front-panel operator command, a remote engineering console command, or a local hardwire contact input.

In Fig. 7, the window in front illustrates combining several IED digital logic variables into a graphical Boolean expression. These digital logic variables are used freely without restriction based on their source, e.g., hardwire input contacts, GOOSE, serial peer-to-peer, or front-panel or remote command. The window behind illustrates the association of contents of received GOOSE messages to digital logic variables in an IED. In this case, Logic Bits RB01 through RB03 are received from other IEDs via GOOSE messages and then combined. RB04 and RB05 are received from another IED via a GOOSE message and then combined with RB06, which can be updated from any of the possible data sources.



Logic Var	Data Item
RB01	SEL-421_001.GooseMessage.Messa
RB02	SEL-421_001.GooseMessage.PRO.E
RB03	SEL-421_001.GooseMessage.PRO.E
RB04	GE-D60.gcb.Device.GGIO1.Ind1.st\
RB05	GE-D60.gcb.Device.GGIO1.Ind2.st\
RB06	
RB07	

Compiled SELogic

```
OUT101=!RB1*RB2*RB3
OUT102=RB6*RB5
```

```
SEL-311L 008 Settings Driver   Driver Version: 3.1.8.0   Date: 3/27/2006 2:01:06 PM   Part #: 0311L0HD04254XX   GLE1 : Graphical Logic 1
TXD   RXD   Not Connected   Direct to COM1  115200  8-None-1   Terminal = EIA-232 Serial   File Xfer = YModem
```

Fig. 7. Mapping of GOOSE contents to IED logic variables and use of these variables within a graphical logic editor

D. SAS Communications Architecture

The wind farm SAS design called for the devices to be directly connected to the Ethernet LAN, and no data concentration was to be allowed for data exchange among the IEDs, local HMIs, and protocol gateways. Vendors submitted product designs that performed direct transmission and receipt of IEC 61850 protocols. As mentioned previously, data concentration was initially allowed only for the SCADA gateway function that converted IEC 61850 protocols into DNP3 and Conitel 2020.

The substation LAN is configured in a ring topology with Ethernet switches installed in each cabinet. Because of the short distances and the fact that all the IEDs are inside one cabinet, the bay IEDs are connected to the switch using copper cables. Longer switch-to-switch connections between bays are accomplished via fiber optics that support the ring topology as seen in Fig. 8. This topology provides redundant ring communications at the switch level; however, IED connections within the same bay cabinet do not warrant redundant communications at the IED level based on past experience. Also, the use of internal switches within the IEDs connected in a ring is not allowed because it dramatically decreases reliability and increases complexity for the sole purpose of overcoming a cable failure.

Two local computers provide the operation HMI to the user for local control and visualization. Redundant SCADA protocol gateways provide the interface to the SCADA master in DNP3 and Conitel 2020.

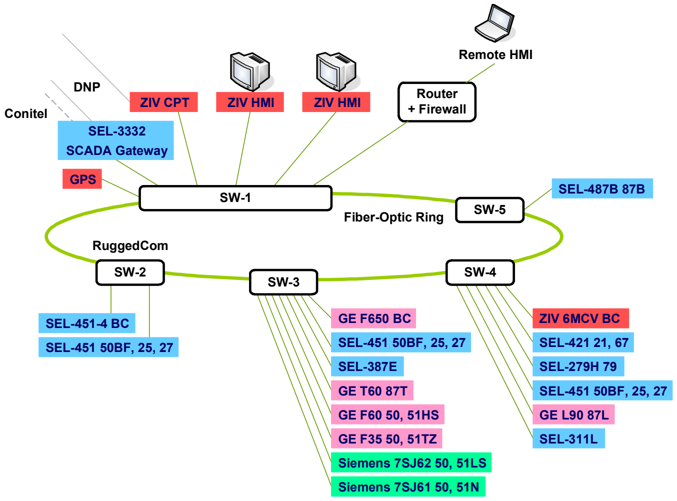


Fig. 8. Various connections to the substation fiber-optic Ethernet ring

As mentioned, each bay panel has its own Ethernet switch, regardless of the number of IEDs. This was done for several reasons: robust communications, ease of field installation, and ease of future maintenance. IEDs connected in a star fashion with the switches connected in a fiber-optic ring provide the most reliable and dependable substation LAN. Because each panel has its own switch, none of the bay communications cabling needed to be disrupted or retested between factory acceptance testing (FAT) and field installation. Each panel was complete and tested during the FAT. Once delivered on-site, the switches were reconnected in a ring, and the network was quickly reconfigured, regardless of their eventual distance from one another. Future Ethernet troubleshooting and maintenance has been simplified by inclusion of a switch in each bay instead of multidrop connections between IEDs or long-distance cable runs to a distant switch.

E. Communications Implementation Considerations

The IEC 61850 standard requires timestamp resolution to the microsecond. Therefore, the recommended best practice for time synchronization remains IRIG-B because it is the only method that provides this accuracy. SNTP (simple network time protocol) can be used but will not provide the accuracy required. IEC 61850 Part 5 identifies the requirements for the time-synchronization accuracy classes. The T1 accuracy class for ± 1 ms time tagging of events requires the time-synchronization source to be one order of magnitude more accurate (± 0.1 ms) to achieve the required timestamp accuracy. SNTP provides time-synchronization accuracy in milliseconds, which is not sufficient to support the T1 accuracy class. Future changes to the IEC 61850 standard may recommend a method over Ethernet once one is available. The IEEE is working on a standard, referred to as IEEE 1588, that may provide microsecond time-synchronization accuracy over Ethernet. However, until then, some vendors suggest that customers use SNTP, which is convenient because it travels over Ethernet and does not require a second connection like IRIG-B. The accuracy of SNTP is at best several milliseconds and varies as the network traffic varies.

The customer agreed to implement time synchronization via SNTP or IRIG-B because of different implementations among all the vendors. The customer asked that the vendors provide useful descriptive naming of the IEC 61850 data and groups, such as logical node names, and avoid generic names. However, many of the vendors used generic naming. These generic names are conformant with the standard; however, they are not very useful to the end user and are actually counterproductive to creating the SCL and self-description. By using generic naming, the vendors eliminate the ability to perform automatic configuration and require the integrator to refer to documentation to see which generic IEC 61850 value represents the needed phase voltage or breaker position.

As shown in Fig. 8, each IED must serve data to six clients, perhaps simultaneously. These six include the two dual-primary redundant HMIs, two dual-primary redundant protocol gateways, one local engineering access connection, and one remote engineering access connection. For each client connection, the design called for separate binary-state data set buffered reports and measurement data set unbuffered reports.

1) Match Existing Device Naming Methods

The customer planned to continue using the naming convention developed within their organization. All of the databases that receive substation data—protocol gateway, engineering, SCADA, HMI, and documentation—use the name of the source IED. The customer naming convention requires 12 characters, XXX YYYYY ZZZZ. These 12 characters represent the aggregate name, where XXX identifies the substation (e.g., LVD), YYYYY is the breaker identifier associated with the device (e.g., 97010), and ZZZZ identifies the IED function (e.g., MCAD, the acronym for bay control). This combines to be LVD97010MCAD and represents the bay control for tie breaker 97010 in station LVD.

Some vendors did not support 12 characters in their IED description within their IEC 61850 configuration. Though this is not defined by the standard, it has been common for many years via many protocols to provide enough characters for end users to uniquely name each IED based on their established internal naming conventions, and it became a problematic "local issue." Local issue is the term used within the standard to refer to important implementation details that are not addressed by the standard and must be resolved locally—within the implementation of the IED. However, because many local issues result in differences that impact integration among vendors' IEDs, the connotation has come to mean issues local to the substation where the integrator must make things work. Because character length is a local issue, out of scope of the standard, IEDs were included that do not support the customer's naming convention. Discovering this local issue so late in the project resulted in a tremendous amount of rework and testing because each element in each database that referred to data from these IEDs had to be changed to the shorter name and retested. Furthermore, the customer was not able to maintain their established naming convention.

2) Logical Devices, Functions

This customer, like other customers, would like the opportunity to replace IEDs from one vendor with those of another vendor that perform the same function and would like to have each IED support the same communications interface capabilities. This is a useful consideration, but even though communications via IEC 61850 protocols can be standardized, they can only be standardized to the features that overlap within every product (the lowest common denominator). Also, keep in mind that even though IEC 61850 IEDs communicate similarly, they do not perform protection or automation the same, and the standard does not specify how they perform these functions. To allow interchangeability at the communications level for this project, IEC 61850 logical devices within the IEDs were defined for each required function. Only the specified logical nodes were allowed to exist inside each logical device. Examples of the logical devices include:

- CTRL1 for bay control – LVD97010MCADCTRL1
- PRO for main protection – LVD97010MCADPRO
- MET for metering – LVD97010MCADMET

The left view in Fig. 9 illustrates browser software finding several IEDs (physical devices) on the network, including the physical device bay control LVD97010MCAD. The right view shows the detail within the MCAD that exposes each logical device and the logical nodes inside the CTRL1 logical device.

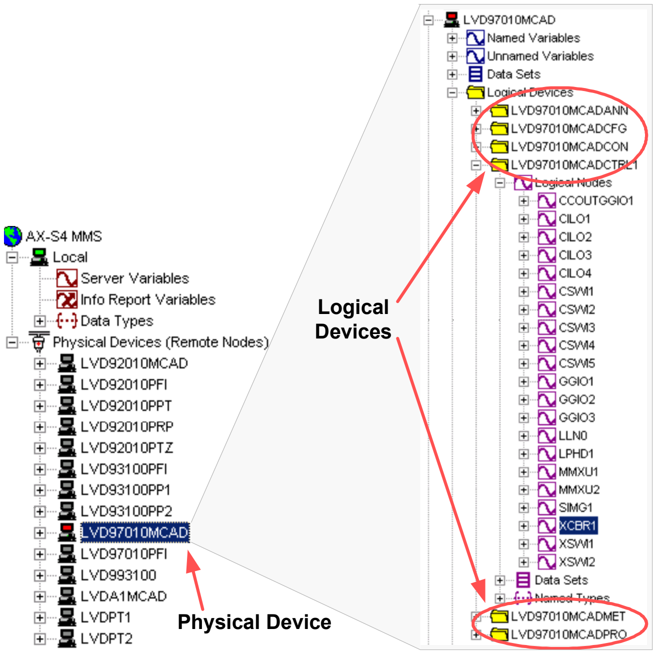


Fig. 9. Browsing on physical devices, logical devices, and logical nodes

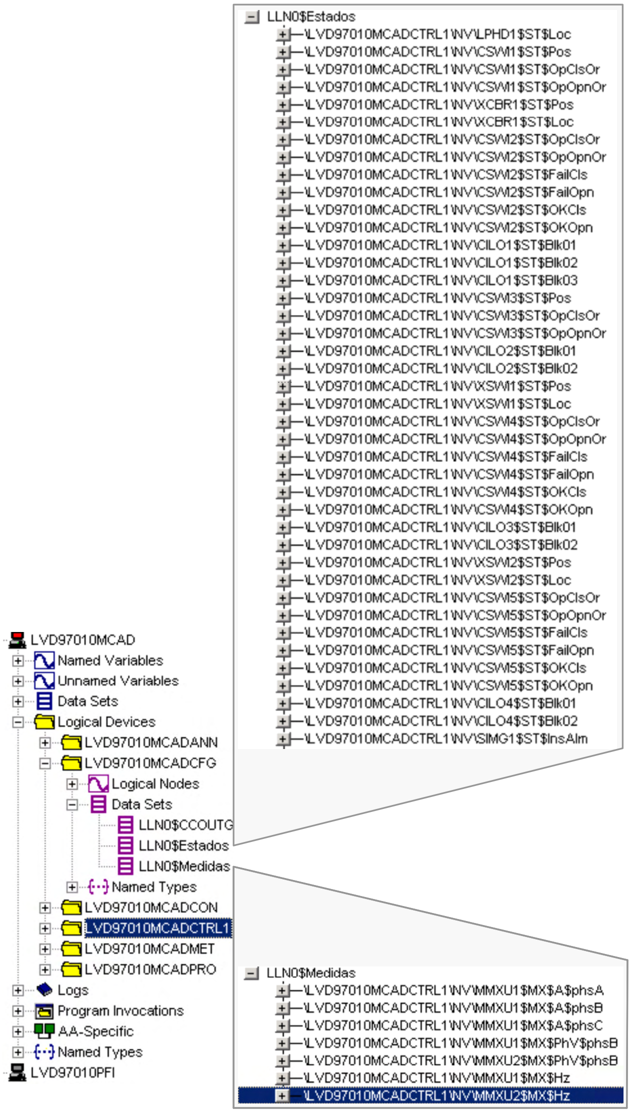
3) IED Data Sets

Inside each logical device, only the logical nodes required for the project were allowed to be communicated within the data sets. This was accomplished by some vendors through the use of configurable data sets that were easily modified to support this. Also, several default logical devices and nodes were left in the IED in case of future needs, but they were not reported in the data sets developed for the in-service design. The customer requested data sets for binary data states (*estados*), analog measurements (*medidas*), and GOOSE bits (GOOSE) as summarized in Table VI.

TABLE VI
DATA SETS

Name	Association	Report Type
Estados	Binary Status	Buffered
Medidas	Measurements	Unbuffered
GOOSE	GOOSE Bits	GOOSE Messages

The contents of the digital state and measurement data sets are illustrated in Fig. 10.



LLN0$Estados
\LVD97010MCADCTRL1\NV\LPHD1STLoc
\LVD97010MCADCTRL1\NV\CSWI1STPos
\LVD97010MCADCTRL1\NV\CSWI1STOpClsOr
\LVD97010MCADCTRL1\NV\CSWI1STOpOpnOr
\LVD97010MCADCTRL1\NV\XCBR1STPos
\LVD97010MCADCTRL1\NV\XCBR1STLoc
\LVD97010MCADCTRL1\NV\CSWI2STOpClsOr
\LVD97010MCADCTRL1\NV\CSWI2STOpOpnOr
\LVD97010MCADCTRL1\NV\CSWI2STFailCls
\LVD97010MCADCTRL1\NV\CSWI2STFailOpn
\LVD97010MCADCTRL1\NV\CSWI2STOKCls
\LVD97010MCADCTRL1\NV\CSWI2STOKOpn
\LVD97010MCADCTRL1\NV\CILO1STBlk01
\LVD97010MCADCTRL1\NV\CILO1STBlk02
\LVD97010MCADCTRL1\NV\CILO1STBlk03
\LVD97010MCADCTRL1\NV\CSWI3STPos
\LVD97010MCADCTRL1\NV\CSWI3STOpClsOr
\LVD97010MCADCTRL1\NV\CSWI3STOpOpnOr
\LVD97010MCADCTRL1\NV\CILO2STBlk01
\LVD97010MCADCTRL1\NV\CILO2STBlk02
\LVD97010MCADCTRL1\NV\XSWI1STPos
\LVD97010MCADCTRL1\NV\XSWI1STLoc
\LVD97010MCADCTRL1\NV\CSWI4STOpClsOr
\LVD97010MCADCTRL1\NV\CSWI4STOpOpnOr
\LVD97010MCADCTRL1\NV\CSWI4STFailCls
\LVD97010MCADCTRL1\NV\CSWI4STFailOpn
\LVD97010MCADCTRL1\NV\CSWI4STOKCls
\LVD97010MCADCTRL1\NV\CSWI4STOKOpn
\LVD97010MCADCTRL1\NV\CILO3STBlk01
\LVD97010MCADCTRL1\NV\CILO3STBlk02
\LVD97010MCADCTRL1\NV\XSWI2STPos
\LVD97010MCADCTRL1\NV\XSWI2STLoc
\LVD97010MCADCTRL1\NV\CSWI5STOpClsOr
\LVD97010MCADCTRL1\NV\CSWI5STOpOpnOr
\LVD97010MCADCTRL1\NV\CSWI5STFailCls
\LVD97010MCADCTRL1\NV\CSWI5STFailOpn
\LVD97010MCADCTRL1\NV\CSWI5STOKCls
\LVD97010MCADCTRL1\NV\CSWI5STOKOpn
\LVD97010MCADCTRL1\NV\CILO4STBlk01
\LVD97010MCADCTRL1\NV\CILO4STBlk02
\LVD97010MCADCTRL1\NV\SIMG1STInsAlm

LLN0$Medidas
\LVD97010MCADCTRL1\NV\MMXU1MXA$phsA
\LVD97010MCADCTRL1\NV\MMXU1MXA$phsB
\LVD97010MCADCTRL1\NV\MMXU1MXA$phsC
\LVD97010MCADCTRL1\NV\MMXU1MXPhV$phsB
\LVD97010MCADCTRL1\NV\MMXU2MXPhV$phsB
\LVD97010MCADCTRL1\NV\MMXU1MXHz
\LVD97010MCADCTRL1\NV\MMXU2MXHz

Fig. 10. Required IED data sets and their contents

4) New IEC 61850 Data Objects

Based on previous design experience, the project manager had recommended the use of new data objects not yet a part of the standard. The project manager had already submitted a proposal to be added to the standard so that all users could benefit from their future use. Even though they were not yet a formal part of the standard, some vendors were able to implement them because the IEC 61850 standard defines the methods necessary to extend the logical nodes and data objects to include new and unanticipated contents.

One such data object is the open and close order activation information, or ACT. This is a status that represents that the IED received a control action command. The control switch logical node, CSWI, was extended to include both an open order ACT (CSWI\OpOpnOr) and a close order ACT (CSWI\OpClsOr).

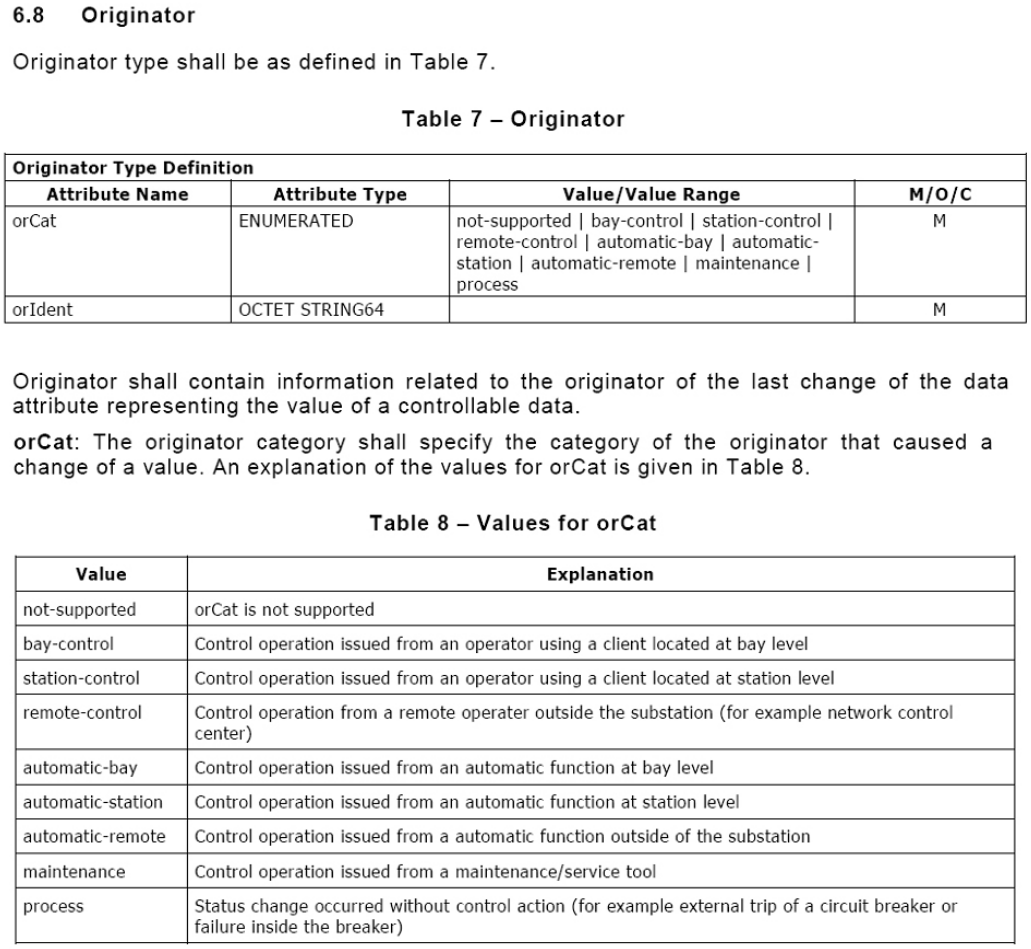
5) Controls Filtered by Origin

The project design also required control functionality where the status was mandatory within the standard, but the function was left undefined. Origin category (orCat) and other features became local issues not expected by the vendors and required additional development during the project. It was determined to use orCat to filter the controls based on what the client sent them, or the "control origin category." This control origin, the originator category, is illustrated in Fig. 11, an excerpt from the standard. As can be seen, the standard does not address the behavior or use of this attribute. These are left to be addressed as a local issue.

The customer requested that the IEDs accept or deny control execution based on the source of control that is the orCat attribute for circuit breakers, control switches, and sectionalizer switches. In this way, the IEDs are configured to accept or deny control commands by comparing the origin to the present state of permission for that client. Addressing it as a local issue, the integration design team defined its behavior to satisfy the customer's requirements. As designed, an IED can be set for remote control only and act on only commands with the origin associated with a remote SCADA client and deny local HMI commands. Conversely, when the IED is expected to perform in local mode, it can filter out all remote SCADA commands based on their origin and accept only commands from a local HMI. This filtering is useful to assure that the communications are configured correctly on a trusted network. However, it should not be considered a method to satisfy cybersecurity requirements because the origin is simply a setting and is not authenticated in any way. The IEC 62351 standard is under development and when complete will provide cybersecurity methods for IEC 61850 substations.

Logical node implementations for breakers, control switches, and sectionalizer switches are filtered as listed below:

- Breaker – XCBR\POS\origin
- Control switch – CSWI\POS\origin
- Sectionalizer switch – XSWI\POS\origin



6.8 Originator

Originator type shall be as defined in Table 7.

Table 7 – Originator

Originator Type Definition			
Attribute Name	**Attribute Type**	**Value/Value Range**	**M/O/C**
orCat	ENUMERATED	not-supported | bay-control | station-control | remote-control | automatic-bay | automatic-station | automatic-remote | maintenance | process	M
orIdent	OCTET STRING64		M

Originator shall contain information related to the originator of the last change of the data attribute representing the value of a controllable data.

orCat: The originator category shall specify the category of the originator that caused a change of a value. An explanation of the values for orCat is given in Table 8.

Table 8 – Values for orCat

Value	Explanation
not-supported	orCat is not supported
bay-control	Control operation issued from an operator using a client located at bay level
station-control	Control operation issued from an operator using a client located at station level
remote-control	Control operation from a remote operater outside the substation (for example network control center)
automatic-bay	Control operation issued from an automatic function at bay level
automatic-station	Control operation issued from an automatic function at station level
automatic-remote	Control operation issued from a automatic function outside of the substation
maintenance	Control operation issued from a maintenance/service tool
process	Status change occurred without control action (for example external trip of a circuit breaker or failure inside the breaker)

Fig. 11. Excerpt from IEC 61850 standard defining the originator type and orCat values

II. SAS Communications Integration Project Challenges

A. *Local Issues Undefined by the Standard*

By and large, the complications encountered in this project resulted from local issues left unresolved by the standard. Many of these local issues cannot, and will not, be addressed by the standard but are essential to a successful implementation. Throughout the design, the communications integration team documented a list from these local issues and the chosen solutions as a guideform specification to aid other users of the standard. The most arduous task was actually representing specific customer data requirements within the noncustomer specific international standard methods of IEC 61850.

The previously mentioned request to support customer-specific IED names and logical device names was not unusual. However, it was unexpected by a few vendors. The primary IED vendor anticipated these requests because of years of experience supporting UCA2, which uses all of the same messaging specifications and data transfer methods. Thus, the flexibility of configuration of IEDs from this vendor's IEDs easily supported the customer's desires. However, several of the IEDs from other vendors did not. In some instances product development provided the solution; in others, the final design was modified to match the IED capabilities.

B. *Unnecessary and Unexpected Use of Generic Data References*

The choice of several vendors to use generic data references instead of specific naming for commonly used information was a surprise. Though not mandatory, it was definitely expected that vendors would provide logical node and data object names that reflected the source and purpose of the data.

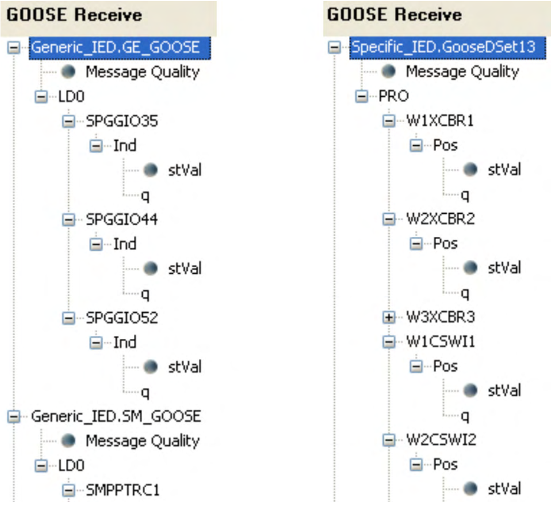


Fig. 12. Specific naming versus generic naming for a switch status

Fig. 12 illustrates an example of specific naming versus generic naming for a switch status. In the generic example on the left, the contents of a data set published in a GOOSE message represent the position of an apparatus as a generic data object (indicator, Ind) associated with a generic logical node (single point generic process input/output, SPGGIO35). The more descriptive example on the right shows the contents of a data set where each of three windings are associated with a separate circuit breaker. Winding one circuit breaker logical node is W1XCBR1, and the position is identified as Pos rather than a generic indication. Therefore, with a little experience, it can be observed that W1XCBR1.Pos.stVal refers to the value of the position of the circuit breaker associated with winding one. It is not possible from the generic description to know what SPGGIO35.Ind.stVal refers to.

Without specific naming within the IED, separate documentation must be used to identify what the generic data objects represent. This eliminates the possibility of self-description and automatic configuration. Generic naming is defined in the standard for use when data that cannot be anticipated, such as results of customer and/or site-specific logic, are incorporated in a system. This feature should be used sparingly to improve self-description but is a useful method to incorporate data at the time of installation that would otherwise be unavailable. If these data are common to other applications, they may become mapped to new or existing logical nodes as the products evolve.

The fact that devices from nine different product developments from six different vendors were combined for the first time in any project was also a difficult challenge, but this would be true regardless of the protocol chosen. Engineers that participated in the engineering of this project were located across seven time zones (United States, Mexico, Spain, Germany). Several communications tests were staged over the Internet between remotely located engineers and products so that work could begin before all products were collected at the site of the FAT. It quickly became evident that the vendors were in different stages of completeness of their IEC 61850 implementations. Some development continued until the beginning of the FAT, which in some cases allowed the vendors to incorporate some of customer's local issue requests.

Time was also a concern because delivery was initially required four months after the contract award for the team to design, build, and test all the protection panels and integration systems. This, in concert with the fact that some IEDs were the result of product development completed during the design stage, resulted in a lot of integration rework during the FAT.

III. Factory Acceptance Test

Overall, the FAT took six weeks. The project management team and system integrators were involved in the total length of the testing. Other IED vendors were involved in the configuration and testing of their devices. The process started with initial network setup, switch configuration, and initial communications tests. This part of the process went quickly but also brought to attention the following issues:

1. Some manufacturers were not able to meet some of the IEC 61850 requirements for the project. Below is a list of limitations found during this process:
    a. Physical device name limited to eight characters. This made the project management team redefine

the database naming and meant reconfiguration of databases for all the clients.

b. Logical device name was not configurable. This limited the overall goal of device interchangeability.

c. No mapping flexibility meant that the IED did not allow for mapping any desired IED digital value to a specific data object in a logical node. Therefore, the team used more generic nodes than what was expected in the design stage.

d. Some IEDs did not support the six clients required by the project.

Most of these limitations exist because of IED limitations and were not possible to overcome, requiring the design team to change databases and naming conventions for the devices with limitations.

2. After these problems were addressed, HMIs and SCADA gateways were reconfigured in order to start functional testing. During this second part of testing, new issues were discovered:

   a. Report control block names were not configurable for some of the IEDs.

   b. Writing to report control block named components OptFlds and TrgOps was a challenge because values defined in the design stage were not accepted by all the IEDs.

   c. Double point indication for breakers and sectionalizers caused problems when mapped to DNP3 and Conitel 2020.

   d. Some IEDs did not support the origin attribute to report back to the HMI. The HMI uses orCat to discriminate from which level the control was executed and to log the control origin.

   e. IEDs must use orCat as a filter to allow controls from different control levels.

      i. Local

      ii. HMI

      iii. Control center

3. After status, measurements, and controls were tested, GOOSE messages for interlocks were tested. The following two issues were addressed:

   a. Control block reference (CBR) cannot exceed 32 characters for some IEDs. CBR is configured by adding the physical name, logical name, logical node, and data set. Because of the naming convention used, this limitation was exceeded most of the time in several IEDs, and the customer was not able to use the CBR that they originally chose.

   b. Configuration software from some vendors will import SCL files from other vendors but will not respect all the configuration parameters. As a result, the device is not allowed to subscribe to the GOOSE messages from the other devices.

   After these issues were addressed, the testing of interlocks between bay controls was fast and easy, showing the real advantages of GOOSE.

4. Confirming the successful use of GOOSE messages for protection was the last part of the FAT. The customer wanted to perform detailed testing in order to gain confidence in the new technology.

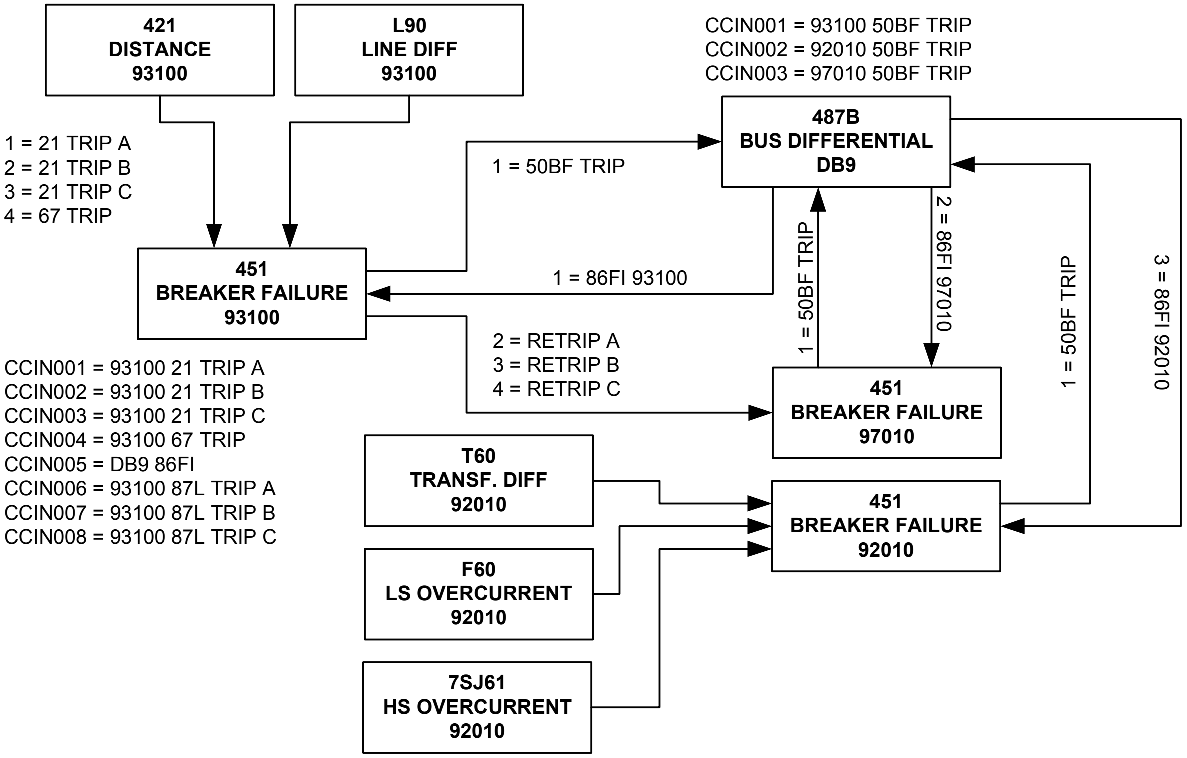


Fig. 13. Breaker failure protection scheme using GOOSE

The complete breaker failure protection scheme was implemented using both traditional wiring and GOOSE. The operation sequence of the breaker failure scheme is presented below. Fig. 13 illustrates the process.

a. Trip of protection relay—the relay detects the fault, operates, and at the same time, sends a GOOSE message to the breaker failure relay.

b. Retrip of breaker failure relay—breaker failure relay receives the GOOSE message and sends the retrip signal to the associated breaker.

c. Trip of breaker failure protection—in the case when a breaker failure timer expires, a breaker failure trip GOOSE message is sent to the bus differential relay to start the bus isolation.

d. Bus differential relay receives the GOOSE message, identifies feeders connected to the bus with the breaker failure, and sends a GOOSE message to trip the required breakers through their associated breaker failure scheme.

Fig. 14 shows an event report from the breaker failure relay 93100 for a retrip operation. IN101 represents the trip signal from the distance protection relay using a hardwired contact; CCIN001 represents the trip signal from the same relay using GOOSE. The time difference between hardwired and GOOSE is about 12 ms because of the time introduced by the physical output of the distance protection relay and the debounce timer of the breaker failure relay. Because of this delay, the retrip operation using GOOSE was 12 ms faster than the hardwired operation. This difference might be reduced using high-speed output contacts.

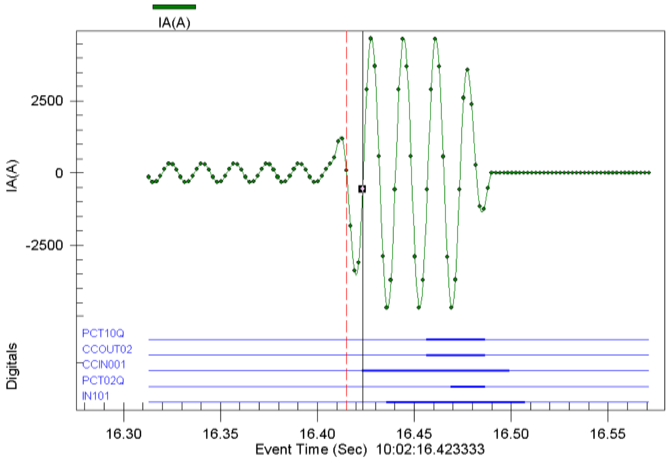


Fig. 14. An event report from the breaker failure relay 93100 for a retrip operation

Fig. 15 shows an event report for the breaker failure relay 97010. In this case, the hardwired trip comes into IN103, and after about 200 ms, BFTR1 represents the output contact to the 86FI lockout relay that will distribute the trip to all breakers in the bus. The GOOSE trip comes into CCIN003, the same 200 ms apply, and another GOOSE (CCOUT001) is sent to the bus differential relay that determines which breakers to trip and sends another GOOSE message (CCIN005). Fig. 15 shows that the GOOSE scheme is 8 ms faster, without considering that the wiring scheme still has to go through the lockout relay.

Additional tests were performed, increasing traffic in the network and obtaining the same results. In this specific project, Ethernet switches with VLAN (virtual LAN) priority tagging and store-and-forward technology to avoid collisions were used in order to guarantee the results.

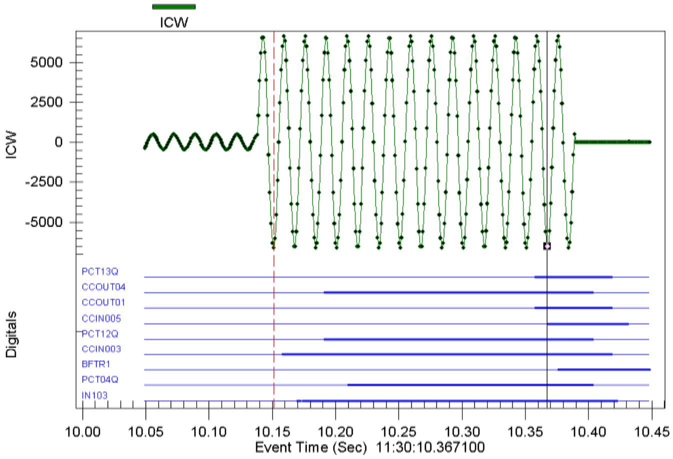


Fig. 15. An event report for breaker failure relay 97010

IV. Lessons Learned

Much was learned during the project because it was the first to integrate so many different vendor IEDs into one system and prove interoperability. Success was possible because of the skills and years of experience of the design team working with the messaging and methods of the new standard. The vendor that supplied the bulk of the IEDs has been providing this technology for six years as UCA2 and recently upgraded their implementation to incorporate SCL. However, most of the lessons that can and should be taken from this paper are the resolution of local issues documented as a guideform specification. These local issues were not solved in the past because other IEC 61850 system designs were created with a handful of IEDs from the same vendor or perhaps two different vendors. The design team for this project offers the following list of lessons learned.

A. Design Stage

- Be aware of desired IED name length and restrictions within the IEDs.
- As early as possible, identify optional parts of the standard that you will require in order to increase the likelihood that each vendor will support them. Be prepared to compromise if your IED of choice does not support these requirements.
- Choose IEDs that support configuration flexibility so that any IED data available to the communications interface can be presented and so that logical devices and logical nodes can be extended to incorporate new and unanticipated data.
- Choose vendors that will support your requirements and desires to implement nonmandatory elements of

the standard as well as your selection of resolutions to local issues.

- Test new product communications as much as possible prior to the FAT.
- Use IRIG-B for better timestamp accuracy.
- Use substation-grade communications equipment.
- Use Ethernet switches that support VLAN and priority tagging.
- Preferably, use IEDs that support direct loading of SCL configuration files over devices that require proprietary software.
- Choose IEDs that support the required number of clients (recommend six).
- Choose IEDs that support the appropriate GOOSE parameters.
  - GOOSE subscriptions (recommend 24)
  - Logic variable associations for bay control (recommend 128)
  - Logic variable associations for protection (recommend 16 or 128, depending on application complexity)
  - GOOSE publications (recommend eight)

B. *Communications Interface Testing*

- Be prepared to understand and test communications at the manufacturing messaging specification (MMS) level.
- Be aware that, because of the anonymity of Ethernet, messages are interleaved from multiple sources.
  - This complicates troubleshooting and eliminates straightforward functional testing.
  - One must trust software test tools rather than hardware connections and diagnostics, such as LEDs, to provide communications information.
- Choose IEDs that respond to commands to identify what configuration file is loaded within the IED and in use.
- Choose IEDs that respond to commands to identify the status of their configured outgoing GOOSE message publications.
- Choose IEDs that respond to commands to identify the status of subscription to expected incoming GOOSE message.

C. *Functional Testing*

- Document everything.
- Keep your Ethernet analyzer recording at all times. You cannot troubleshoot what was not captured by an analyzer.
- Recognize that part of the simplicity and speed in using GOOSE is that permissive logic is done in the relay logic rather than auxiliary relays because so much information can be received quickly from many sources.

D. *Software*

At this time, not all vendors have IEC 61850 configuration software available. Some still edit files at the XML level. For this project, only three vendors had an IEC 61850 configuration tool available. Engineering software tools (SCL software) that can import ICD files from the different IEDs and create CID files for the IEDs, SCADA gateways, and HMIs will help to reduce configuration time as well as complexity.

Fig. 16. Construction of the wind farm

V. Guideform Specification

In order to confirm that IEDs that support IEC 61850 are successfully integrated into a substation system, the following details also need to be met. Some of these details are not mandatory for IEC 61850 conformance but are necessary to satisfy integrated communications. Therefore, IEDs offered for inclusion in a system to satisfy this specification need to be IEC 61850 conformant and support the following itemized functionalities:

- Each IED shall support the appropriate protocols within the IEC 61850 standard.
  - Reporting, poll response, controls, and self-description shall be performed via MMS protocol.
  - Configuration shall be performed via XML-based SCL files.
  - Peer-to-peer messaging shall be performed via IEC 61850 GOOSE messages.
- Each IED shall have a native Ethernet port that supports each of the IEC 61850 protocols mentioned previously as well as essential engineering access connections over the same Ethernet port. Specifically,

each IED Ethernet port shall support, at a minimum, the following:

- IEC 61850 reporting via MMS
- IEC 61850 polling MMS
- IEC 61850 controls via MMS
- IEC 61850 self-description via MMS
- IEC 61850 GOOSE messaging
- IEC 61850 configurations via XML-based SCL files loaded directly into the IED (preferred)
- Engineering access via standard TCP/IP mechanisms
- Event report collection via standard TCP/IP mechanisms
- Non-IEC 61850 settings transfer via standard TCP/IP mechanisms (e.g., protection and logic settings)

In order to support varied future and additional installations, each IED shall also support a SCADA protocol in addition to IEC 61850 via the Ethernet port.

Each IED shall support the origin category (orCat) for controls and filter permission to execute a received command based on the command origin.

Each IED shall support the data object ACT to represent the open and close order activation information. This status represents that the IED received a control action command.

Each IED shall support a descriptive name of up to 16 characters in order to provide the ability for the end user to uniquely name the IEDs within their system based on new or established naming practices.

Each IED shall be capable of supporting six simultaneous client-server associations. This number is necessary to support the possible network requirement of two redundant SCADA gateway connections, two redundant HMI connections, and two redundant engineering access connections.

Each IED shall support six default preloaded buffered reports and six preloaded unbuffered reports. These reports shall be preconfigured and capable of being used without customization. However, the IED shall also support customization of the reports and data sets.

Each IED shall have the ability to freely rename data sets, logical devices, and logical nodes.

Each IED shall have the ability to add and remove logical nodes to and from each logical device.

Each IED shall use specific naming for commonly used information rather than generic data references.

Changes to data sets and reporting configuration shall be done via ease-of-use configuration software. The resulting SCL CID file shall be downloaded directly into the IED as described within the standard. This is necessary to confirm that future IEDs from multiple vendors can be used and configured with one software tool.

Each IED shall support remote loading of the CID file via Ethernet using standard TCP/IP mechanisms in order to accommodate engineers designing and technicians configuring IEDs remotely from each other because of geography and/or time.

It is of utmost importance that the IEDs support stations and applications with different data requirements, have the ability to accommodate data that were not recognized to be necessary until after contract award, and represent customer-specific data and IED logic values as appropriate IEC 61850 logical nodes and data objects. Therefore, flexible configuration of data sets shall be required as well as the ability to create new logical devices, logical nodes, and their contents. To support this, it shall be possible to create different ICD (IED capability description) and CID files that map any and all available IED data for specific customer applications. In this way, unique data sets and customer specific names shall be supported. Modification of the IED IEC 61850 capabilities shall be done without hardware or firmware changes to the IED.

Each IED shall allow the user to query it directly and to verify which IEC 61850 configuration file is active within the IED. This function is necessary to confirm correct configuration and identify what behavior should be expected from the IED in order to perform effective commissioning and troubleshooting.

In order to perform effectively in the anticipated communications designs, the IEC 61850 GOOSE implementation in each IED shall support the following requirements:

- Each IED shall be capable of publishing eight unique GOOSE messages.
- Each IED shall be capable of subscribing to 24 unique GOOSE messages.
- Each IED shall be capable of monitoring GOOSE message quality.
- Each IED shall be capable of processing incoming data elements and their associated quality.
- Each IED shall be capable of monitoring message and data quality as permissives prior to use of the incoming data. At the time of configuration, the end user can choose to ignore the possibly corrupted data—if the data or message quality fails—to prevent an unwanted operation.
- Each IED shall be capable of creating a GOOSE data set that includes both Boolean values and non-Boolean data types, such as analog values.
- Each IED shall be capable of accepting and processing data sets from other IEDs that contain Boolean and non-Boolean data types even though IEDs need only map and use Boolean data types.
- Each IED shall support priority tagging of GOOSE messages for optimizing latency through Ethernet switches.
- Each IED shall support VLAN identifiers to facilitate segregation of GOOSE traffic on the Ethernet network.
- Each IED shall support a preloaded default GOOSE message for use without custom configuration.
- Each IED shall support custom editing of the data sets published in the GOOSE messages so the user can send what they choose.

- Changes to data sets, GOOSE parameters, GOOSE publication, and GOOSE subscription shall be done via ease-of-use configuration software. The resulting SCL CID file shall be downloaded directly into the IED as described within the standard. This file shall not be converted into settings and downloaded via the conventional settings process. This difference is documented specifically and necessarily to confirm that future IEDs from multiple vendors can be used and configured with one software tool.
- The configuration software from the IED vendor shall import CID, ICD, and substation communications description (SCD) files in order to learn the available GOOSE publications and data sets from other IEDs. The software will use this information to configure the IED to subscribe to other vendor IEDs and use the data being broadcast.
- Each IED, while in service, shall allow the user to query it to learn communications diagnostics as well as status and/or error codes of GOOSE messages being sent and received.

In order to effectively configure the IED for use within the network, the ease-of-use configuration software provided with the IED shall be capable of the following requirements:

- The software shall be capable of importing configuration information about other IEDs from ICD, CID, or SCD files.
- The software shall validate the imported information to confirm that it complies with IEC 61850 parameters.
- The software shall provide error messages describing problems detected in imported files.
- The software shall support naming IEDs with up to 16 characters.
- The software shall support review and editing of IED data sets and report parameters.
- The software shall support review and editing of data sets and GOOSE parameters.
- The software shall support the mapping of any available data into the data sets.
- The software shall support the association of data quality with data elements.
- The software shall support visible end-user warnings to prevent incorrect data set editing as well as warning when editing a data set that is already in use. In this fashion, the end user can be warned not to disrupt an existing configuration and/or create a data set too large for its intended purpose.
- The configuration software shall support creation of eight GOOSE publications.
- The configuration software shall present the user with all available GOOSE messages and support up to 24 subscriptions.
- The configuration software shall support assigning VLAN and priority tags to GOOSE messages.
- The configuration software shall present the user with the entire data set for each potential GOOSE subscription and allow the user to browse for necessary data.
- The configuration software shall present the user with the entire data set for each potential GOOSE subscription and allow the user to map data from the incoming data sets into the IED. When this is done, the software automatically subscribes to the associated GOOSE message.
- The configuration software shall allow the user to choose message and data validation on incoming GOOSE data set contents.
- The configuration software shall allow the user to directly load the SCL file into the IED, or export it for storage or remote loading.
- The configuration software shall allow importing and exporting of SCL files without modification of the private regions of the original.
- The configuration software shall create files in XML format that can be modified by XML editors and tools to help resolve conflicts or errors in badly formed files.

IEC 61850-5 identifies several specific performance requirements for applications operating in the IEC 61850 series environment. Unfortunately, the IEC 61850 standard defines speed criteria that cannot be exactly measured. Therefore, it is not presently possible to test and verify the transmit time performance classes as described in the standard. Instead, it is possible to measure the transfer time, which includes the transmit time plus the time to process and timestamp the transmitted data. This transfer time represents the performance of communications in actual use. Data element state changes are timestamped and logged as sequential events records (SER). In IEDs with clocks synchronized to the same time reference and that create accurate timestamps, SER are used to calculate transfer time. The transfer time is described as the difference in time between the timestamped SER in the initiating IED and the timestamped SER in the receiving IED. For each IED, the measured GOOSE transfer time shall be provided with a description of how it was measured.

IEC 61850-10 defines other metrics to be measured within devices and documented by the vendors so that end users can compare multiple vendors. For each IED, timestamping accuracy will be identified and documented by providing the two following measures:

- Maximum clock synchronization error, which indicates the accuracy of the IED to synchronize its clock to the time reference
- Maximum timestamp delay error, which indicates the accuracy of the IED to timestamp the data when the event occurs

Product reliability metrics are essential because of the nature of networked IEDs being used to design systems of interoperable devices working in a coordinated fashion. IEC 60870-4 Telecontrol Equipment and Systems Part 4: Performance Requirements documents methods to measure and calculate the following [1]:

- Reliability
- Availability
- Maintainability
- Security
- Data integrity
- Time parameters
- Overall accuracy

These and other device performance measures are essential information for predicting performance, functionality, and reliability of designs executed by networked IEDs. No specific performance benchmarks are expected to be met; however, verification and publication of actual performance measures is necessary to be conformant. Using these published performance measures, system integrators can predict the performance of the interconnected IEDs and, thus, the performance of the system. Furthermore, system integrators will be able to identify suitable devices for specific applications.

Reliability measures should include, but not be limited to, specific product reliability metrics and a description of how the metrics are calculated or measured. Metrics that are mandatory include:

- Specific device mean time between failure (MTBF)
- Product family MTBF
- Specific product mean time between removals (MTBR)
- Product family MTBR

Reliability data should be based on the actual incidence of field failures for a large population of installed units. If the provided figures are based on actual data, the approximate size of each installed population used as a basis for each value should be indicated.

If insufficient field data are available to provide a meaningful MTBF, base the predicted MTBF on the parts-count procedure defined in Military Handbook, MIL-HDBK-217F, December 1991 [2]. Manufacturing quality and design quality can yield significantly better MTBF than predicted by MIL-HDBK-217F. The parts-count procedure does establish a pessimistic MTBF to support a minimum system availability calculation.

VI. References

[1] *Telecontrol Equipment and Systems Part 4: Performance Requirements*, IEC Standard 60870-4.

[2] *Military Handbook: Reliability Prediction of Electronic Equipment*, MIL-HDBK-217F, Department of Defense, Washington DC, December 1991.

[3] D. Dolezilek, "IEC 61850: What You Need to Know About Functionality and Practical Implementation," presented at the Western Power Delivery Automation Conference, Spokane, WA, 2005.

VII. Biographies

Timothy P. Tibbals received his BSEE from Gonzaga University in Spokane, Washington in 1989. After graduation, he joined Schweitzer Engineering Laboratories, Inc. as an applications engineer performing system studies and relay testing. He has experience in electric power protection, integration, automation, communications, and control design and implementation. He also has experience applying SEL products in SCADA and EMS systems. He has authored numerous technical papers and application guides. He served as the supervisor for Automation Services in SEL's Systems and Services Division for several years. He is a member of the IEEE, the IEEE Standards Society, the IEC Technical Committee 57, WG 10, and the UCA International Users Group tasked with upkeep and improvement of the IEC 61850 standard.

Dave Dolezilek is the technology director of Schweitzer Engineering Laboratories, Inc. He is an electrical engineer, BSEE Montana State University, with experience in electric power protection, integration, automation, communications, control, SCADA, and EMS. He has authored numerous technical papers and continues to research innovative technology affecting our industry. Dolezilek is a patented inventor and participates in numerous working groups and technical committees. He is a member of the IEEE, the IEEE Reliability Society, CIGRE working groups, and two International Electrotechnical Commission (IEC) technical committees tasked with global standardization and security of communications networks and systems in substations.

20070314
TP6278-01