Design and Interoperability Testing of a Network IED: a Manufacturer's Perspective

Design and Interoperability Testing of a Network IED: A Manufacturer's Perspective

Mark Adamiak
GE Power Management
Malvern, PA, USA

Drew Baigent
GE Power Management
Markham, Ontario, Canada

Abstract
This paper describes the evolution of communications in Intelligent Electronic Devices (IEDs), the drive for standardization early on in the process, the platform required to fuel this migration, and the issues raised in testing for interoperability among these new devices.

Introduction
Data Communications in Intelligent Electronic Devices (IEDs) has taken the leap into the next generation with the migration to Ethernet as the primary communications medium. In an effort to achieve interoperability early on in this migration process, the Electric Power Research Institute (EPRI) and a group known as the "Utility Initiative" have worked together to proffer a common solution for utility enterprise communications known as the Utility Communication Architecture or UCA. UCA describes a "suite" of solutions to cover all communications aspects of the utility enterprise. UCA provides a "network" solution to the interconnection of data sources – similar to the web solution used throughout the world to interconnect computers.

A recent focus of this effort has been communications in the utility substation where the application of a common protocol and peer-to-peer communications can be shown to have demonstrable savings. For example, integration systems today often require gateways to "commonize" the various protocols and data elements found in today's IEDs into a common database of values. Implementation of a common protocol eliminates the need for gateway solutions. In the area of protection wiring, all signaling between devices is performed via point to point wiring. Peer-to-peer communications can provide a flexible, low cost alternative.

Communication Profile
In creating the next generation communication profile, it was decided to base the model on both the International Standards Organization (ISO) and Internet communication models (figure 1). These models are commonly portrayed as 7 layer and 5 layer models respectively. For simplicity, however, the model can be broken down into 3 primary categories, namely, the application layer, the network layers, and the physical layers. These layers perform communication functions as follow:

Application Layer
The application layer is a set of services for moving and operating on data. The application layer can be compared to the system functions that are a part of FORTRAN, "C" and other languages. In these languages, there are "system calls" to perform such function as "Open File", "Read File", "Write File", etc. that communicate between the user program and the operating system. The application layer performs these kinds of services but communicating between devices over a network. As such, one can speak of reading or writing data and other services among devices not only on the local network but also through a Wide Area Network (WAN).

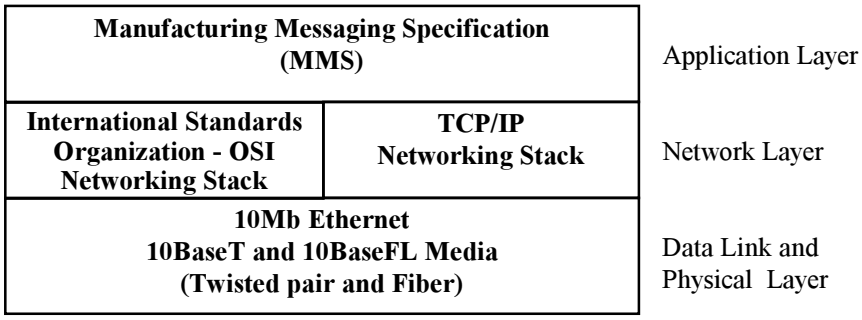

Figure 1
Substation Network Profile

The application layer chosen for the utility profile is the Manufacturing Messaging Specification (MMS). MMS provides a rich set of some 87 services for this function, however, it was determined that only a small subset of these services were necessary to meet the functional requirements spelled out by the industry [1]. The required generic services have been defined in the Common Application Service Module (CASM) document [2] and subsequently mapped to the appropriate MMS services.

There are a number of key services (besides read and write) that facilitate the operation and integration of a network relay in an enterprise, namely:

- Get Object Definition: This service, when issued by any host / client computer, downloads a definition of every variable known to the IED. This service can be equated to meeting a stranger and asking the question "who are you?". Implementation of this service provides automatic creation / update of the host database for that relay. As the software in an IED is often upgraded in the field, this feature automatically keeps the Host database up to date. Note that the ISO Network protocol will automatically detect a new device on the network. As such, the Host computer can automatically create and maintain a list of all the data objects available in the substation. Note that this function is also available remotely over a network.

- Named Variable Lists: Today's IED contain hundreds of present value measurements. The manufacturer typically provides a pre-configured "present value" command that fetches a factory defined set of data. In general, however, utilities typically have their own definition of what they would like to see in a present value message. MMS provides a service that allows the user to define a particular set of data to be retrieved and assigns a name to that data set. For example, the billing agent for a client would need to collect the kilowatt-hour usage for a particular line or set of lines. A "name list" could be established that retrieved only that data on request. Furthermore, the IED could be set-up with security access such that the billing data could appropriately restricted. Typical "name lists" would include: SCADA Data, Power Quality, Outage Report, Demand Data, and Equipment Health.

- Unsolicited Event Notification: Event collection in a substation today is performed on a polled basis, that is, some master controller sends a request for data and a list of events are then transmitted as requested. MMS supports "unsolicited" event collection, that is, the event is automatically transmitted upon change of state. This concept is extended to the transmittal of other data in the substation where data transmission can be initiated by the change of an analog value outside of some bound or change of state of a status indication.

- File Transfer: Upon request, MMS will transfer files from a "server" to the requesting client. Large blocks of data are automatically segmented, transferred block by block, re-assembled in the client machine, and written onto an organized storage media. This function can be used to transfer both file data such as demand data, oscillography, and events as well as program and configuration files.

Network Layer

As it was deemed desirable to be able to access data from any device from anywhere in the corporate enterprise, a complete Network communication layer (the software that handles getting data from here to there) was included in the profile. Two solutions were adopted for the Network layer - TCP/IP and the International Standards Organization -Open System Interconnect.

TCP/IP stands for Transmission Control Protocol / Internet Protocol which is the ubiquitous transport/network layer used over the Internet. The inclusion of TCP/IP in the substation allows access to IED data through the Internet or an intranet. TCP/IP is a streaming protocol which means that transmission of a packet of data waits for a "stream" of data (such as that from a teletype terminal) to fill a buffer before the buffer is transmitted. This mode of operation could potentially slow down the communication of small packets of data. It should be noted, however, that there are controls available on the size and delays times of sending a packet of data. In addition to the streaming aspect, TCP/IP has built in congestion control that will drop packets of data if the network is deemed too busy. This feature is not desirable in the delivery of real time data.

The other Network layer included is the ISO-OSI network layers. ISO is the International Standards Organization which has established the Open System Interconnect (OSI) seven layer model. This model is implemented through a number of standard protocols in the Network layer and does not suffer from the need to wait until a buffer is full before transmitting. Both network layers support the concept of "broadcasting" a

message for all devices on the bus to hear. This feature is very desirable for functions such as data capture triggering, time synchronization, and even control messages to multiple devices.

Physical / Data Link layer

Ethernet was chosen as the Physical / Data Link layer inside the substation due to its predominance in the marketplace and the subsequent availability of low-cost implementations and associated network hardware (such as bridges and routers). In addition, Ethernet's fiber implementations are very desirable in the substation environment and the scalability of Ethernet is well defined with 100Mb implementations being fairly common and 1Gb Ethernet well on its way into vogue. Processors are available today with multiple 10 Mb Ethernet ports integrated into the chip and next generation designs are due out shortly that include 100 Mb ports.

Use of Object Models

Having put in place a system to communicate data, the question arises as to what data and how is it to be organized. This solution to this part of the communication model is solved by what has become known as the 8th layer or the "User Layer". A particular implementation of the user layer is found in the concept of object modeling. An object model is a representation of a physical object or abstract concept. For example, a relay makes measurements of voltage, current, and power on a monitored transmission line. The measurements made by the relay can be organized in a "measurement model" containing all the elements mentioned above. If additional measurements such as power quality and power factor are added at a later date, the original model is easily expanded to accommodate this data.

Why use object models? First of all, modeling of the data creates an independent representation of the data that is not linked to a physical location or storage method inside the relay. Representation of the data in models make it easy to visualize what happens to data in its local environment as well as its interaction with other elements of the modeled device. Physical representation has now been standardized under a Unified Modeling Language (UML). As such, object models can easily be shared with others.

Primary in this implementation, however, is that modeling provides a way to standardize information exchange between other models / devices. Such an object standardization has been created under UCA which is known as the General Object Model for Substation and Field Equipment (GOMSFE) [3]. GOMSFE contains models for metering, protection elements, control, security, and a host of other items. The models are based on what was perceived to be the common elements found in an IED. Once standardized, users can issue requests to the IED for "standard" object values. For example, a utility SCADA system can automatically request Volts, Amps, Watts, Vars, and Status from an IED without having any knowledge of the manufacturer or of the IED. Note that it is almost impossible to standardize on all possible objects in an IED as there are many "vendor specific" objects. These objects serve as differentiators between vendors and make up part of the total object space (figure 2).

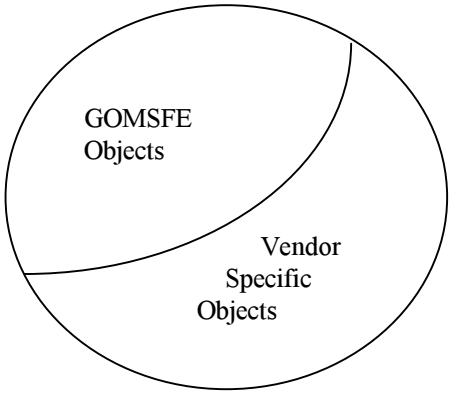

Figure 2
IED Object Space

Design of a Network IED

The primary enabler of the Network IED has been the exponential increase in microprocessor performance and subsequent integration of communication interfaces onto the microprocessor chip – the "engine" of a Network IED. Additionally, price/performance ratios have decreased to the point where the performance requirements of a distance relay and the cost effective requirements of a feeder relay can be met by the same microprocessor and digital technology.

Recognizing that the "engine" of a Network IED is going to continue to increase in horsepower, the platform that houses the engine must be designed to accommodate the future changes. An excellent model to observe for this purpose is the Personal Computer or PC. The PC has become a general-purpose tool that can be used for numerous tasks by running different application

programs on the same platform. Additionally, the basic platform can be upgraded as new CPUs become available and expanded by the addition of special purpose hardware modules to perform special functions as required. Another aspect of the PC that has fostered its acceptance has been the common look and feel of the Human-Machine interface on an international basis. As such, employee training is minimized – a major expense in any industry.

It is desirable to emulate the PC in the design of a universal Network IED, that is, an IED that is modular in both hardware and software and a common look and feel in a user interface. The primary functional building blocks required in such an IED include:

A. Algorithmic and control logic processing, usually performed by the main 'protection' microprocessor. Note that most digital relays have multiple processors for different functions.

B. Power system current and voltage acquisition with interposing current and voltage transformers and an analog-to-digital converter that is tightly integrated with a dedicated digital signal processor (DSP).

C. Digital inputs and outputs for control interfaces, usually required to handle a variety of current and voltage ratings as well as actuation speed, actuation thresholds and different output types (e.g. Form-A, Form-C, Solid-State).

D. Analog inputs and outputs for interfacing to transducer and SCADA systems, usually required to sense or output dcmA currents.

A. Communications to station computers or SCADA systems, usually requiring a variety of physical interfaces (e.g. RS485, Fiber Optical, etc.) as well as a variety of protocols (e.g. Modbus, DNP, IEC-870-5, UCA 2.0, etc.)

B. Local HMI for local operator control and device status annunciation.

C. Power supply circuitry for control power, usually required to support a wide range of AC and DC voltage inputs (e.g. 24-300 VDC, 20-265 VAC).

The design of a Network IED requires an architecture that can accommodate all of the above functional blocks in a modular manner and allow for scalability, flexibility, and upgradability in a cost effective manner for all applications.

Hardware Architecture

The architecture which best implements hardware modularity is that of a plug-in card system similar to that found in programmable logic controllers (PLCs) as well as PCs. Key to the performance of such a system is the high-speed parallel bus which provides the modules with a common power connection and high-speed data interface to the master processor (CPU) as well as to each other. Figure 3 shows such a system with all the core functional blocks implemented as modules. Modularity can also be extended to the HMI where the front of the IED can be configured as needed with indicating lights, displays, and keypad.

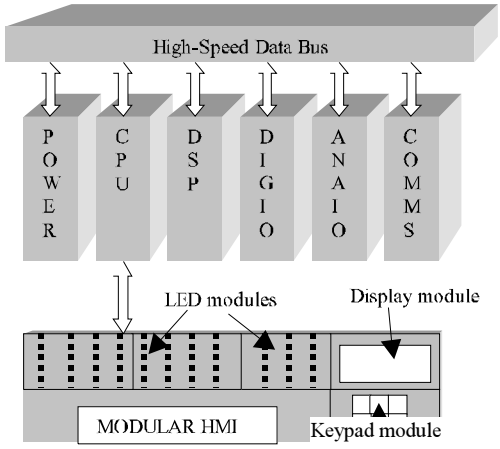

Figure 3
Modular Architecture Design

Software Architecture

A modular architecture which provides scalability and flexibility from a hardware perspective requires software that supports the same features. In fact, the software has its own form of modularity based on functionality:

- Protection elements
- Programmable logic and I/O control
- Metering
- Data and Event capture/storage
- Digital signal processing
- HMI control
- Communications

The key advancement in software engineering which has become predominant in the software industry is Object Oriented Programming and Design (OOP/OOD). This involves the use of *'objects'* and *'classes'*. An object is defined as: "*a logical entity that contains both data and*

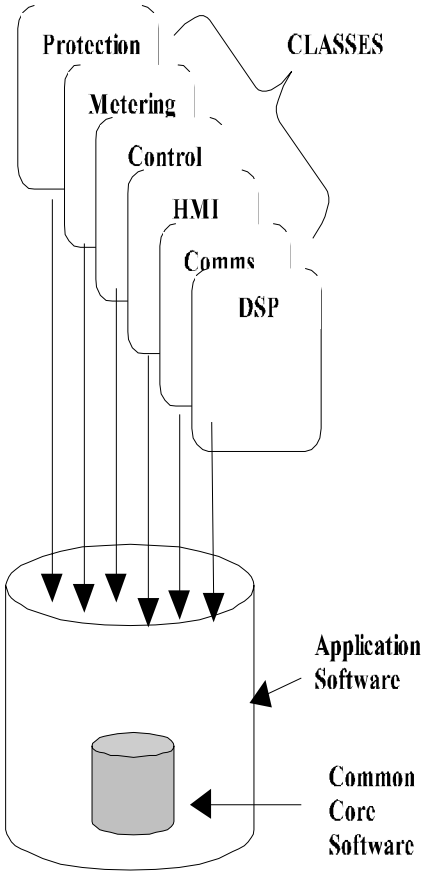

Figure 4b
Relay Code Creation

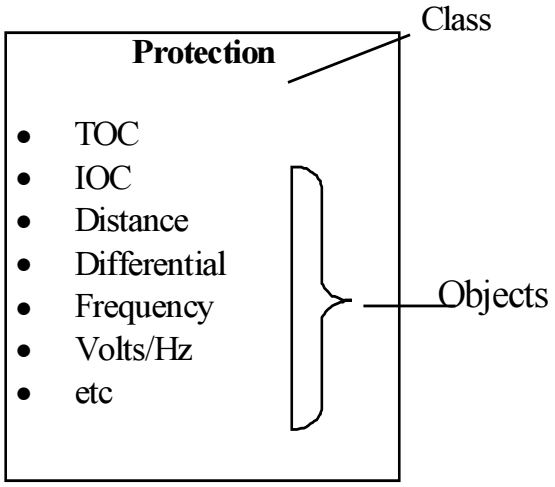

Figure 4a
Class Concept

code that manipulates that data". A class is the general form of the object. By using this concept one can create a ***protection class*** and objects of the class such as **Time Overcurrent , Instantaneous Overcurrent , Current Differential, Under Voltage, Over Voltage, Under Frequency, Distance Mho, Distance Quadrilateral, etc.** These represent software modules that are completely self-contained or *'encapsulated'* which is the term used in the industry. The same can be done for metering,

programmable logic, and I/O control functions, HMI and communications or for that matter any functional entity in the system.

By employing OOP/OOD in the design of the software architecture of the universal relay we have been able to achieve the same features as the hardware architecture: modularity, scalability, and flexibility. Figure 4a shows the concept of a *protection class* with the protection elements as *objects of the class*. The application software of the universal relay (i.e. feeder protection, transformer protection, distance protection etc.) is constructed by combining objects from each of the classes (Figure 4b).

Network Solution

Given a network IED, one can now configure a substation network architecture. Figure 5 illustrates a network architecture of such a system. In this implementation, operation of the IEDs, the Network, and the Host computers / Operator Interfaces is totally separated. In other words, failure of the host computers would have no effect on the inherent operation of the system. All IEDs on the network respond to requests from any other IED on the network. "Next Generation" SCADA is effected as a Bridge or Router interface onto the utility WAN. All data available in the connected IEDs (including the object definitions) become available to any networked device. User defined information, through the implementation of user defined Name Lists, can now be selectively delivered.

Network Solution Features

It is understood that the transition from present SCADA to next generation SCADA will not take place overnight. Nevertheless, the illustrated architecture accommodates legacy SCADA interface through the use of SCADA Gateways. These gateways act as protocol translators from the MMS objects available on the LAN to the

traditional SCADA data required by the remote SCADA Master. Additionally, it is recognized that many substations will contain "legacy" IEDs whose data would be desired in an integrated environment. As such, a similar gateway function can effected by the Host computer or any other independent computer. Ultimately, data retrieved from the legacy IEDs can be made MMS accessible.

Peer-to-Peer Communications

The peer to peer communication environment opens up new vistas for protection applications in the electrical plant. Traditional protection schemes used hard wires and wired logic to implement the various protection schemes. Peer to Peer communications now allows for information transfer through the use of Remote Inputs (RIs) and Remote Outputs (ROs). Any device can define a RI that is linked to an object in another IED (either local or literally anywhere on the network). Linkage would be specified by IED address, object name, object type, and security. The requesting device gets access to the desired object either on request, on change of state (or deadband),
or periodically. Since plant control requires a high degree of reliability, provision is made to implement redundant communications from the IEDs and subsequently, support for a redundant LAN.

The GOMSFE document provides a mechanism for efficient transfer of digital messages through the use of a connection-less multicast message. The format of the message is specifically defined and is known as the Generic Object Oriented Substation Event or GOOSE. GOOSE messages are periodically launched upon the change of state of any of the digital elements and are periodically re-transmitted to confirm delivery.

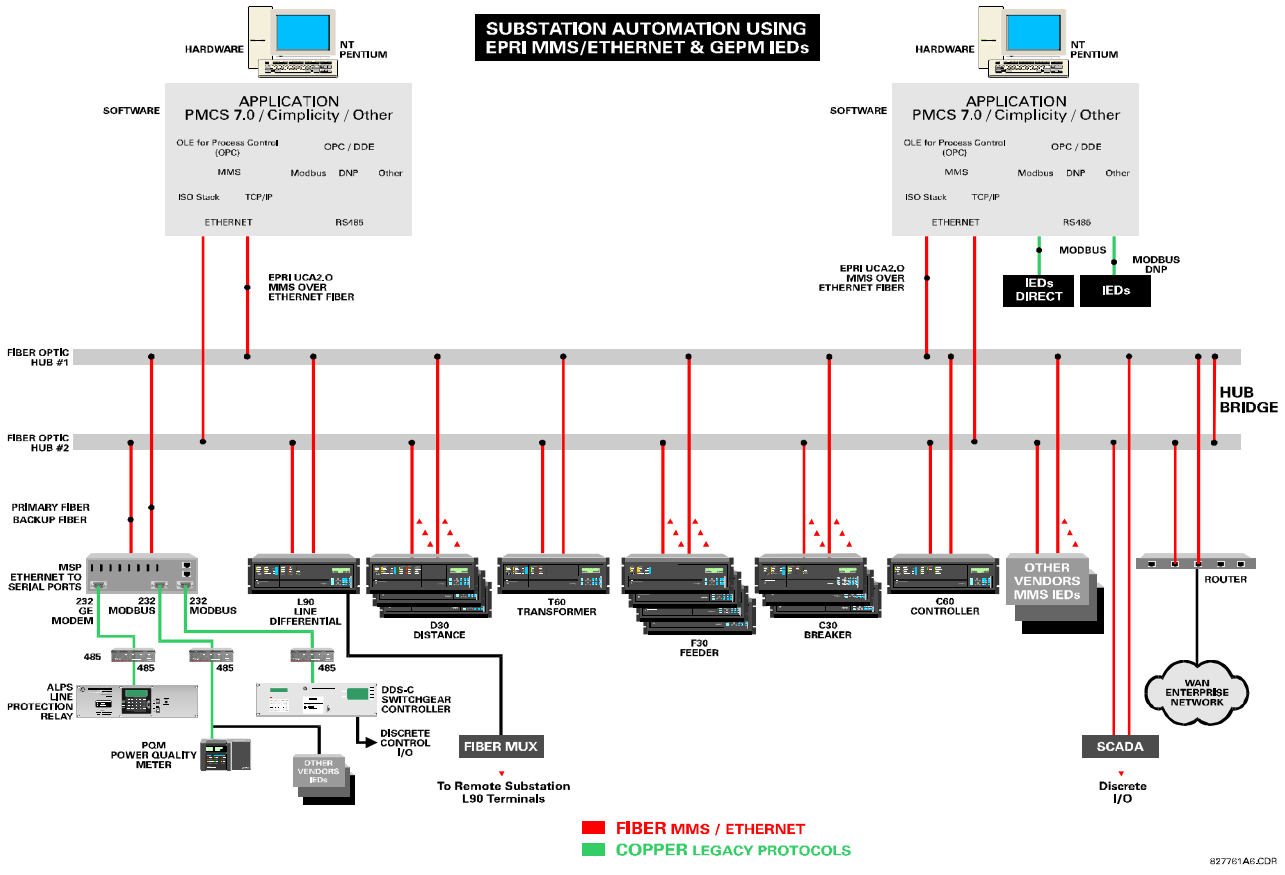

Figure 5
Substation Network Architecture

Interoperability Testing

Communications among a system of Network IEDs can be broken down into three primary areas, namely, host to IED, IED to IED via multicast (local network only), and general IED to IED (both intra and inter substation). As such, interoperability testing in such a system must take place over these three fronts – each with some similarities but also different functionality and performance requirements.

Host to IED Communications

One of the possible network configurations incorporates a host computer located on the network for functions such as user interface, data logging, legacy SCADA interface, PC Control, etc. In this configuration, the host needs to be able to establish a database of all variables from all IEDs in the network and subsequently be able to refresh this database in less than 1 second. The interface with the various IEDs is established on a "connection oriented" basis, that is, there is a request and response based on a user assigned address.

Testing of the host/IED interoperability involves validating operation in four areas as discussed below:

1. **Conformance to CASM and appropriate mapping into MMS.** As stated earlier, CASM is a generic application layer. The implementer needs to make sure that the MMS services installed in the IED completely overlay the CASM services. As most implementations will use commercially available MMS software, this task is done primarily by the primary software vendor and only validated by the implementer.

2. **Proper functionality of the MMS services**. Given that the proper services have been included in the MMS package, the question now is whether the service is interoperable with other manufacturers' implementation. Again, this primarily falls under the scope of the primary software supplier. The IED manufacturer is obliged to do some testing with other manufacturers' MMS clients, however, this function primarily falls under the scope of independent testing labs.

3. **Proper mapping of the GOMSFE and Vendor Specific objects**. The manufacturer is responsible for first correlating the GOMSFE objects with the internal objects of the IED. In most cases, the basic object will need to be extended. Once mapped, the mapping needs to be checked against the GOMSFE document to make sure all mandatory objects have been instantiated and that any GOMSFE objects used have been spelled properly. This process is done manually today and is a candidate for automation in the near future.

4. **Proper mapping of values into the GOMSFE and Vendor Specific objects.** Part of the implementation process is mapping a pointer to the value of the GOMSFE variable. Again, this falls under the purview of the implementer. As a manual process, a known quantity (such as an input voltage) needs to be verified to be in the proper location in the appropriate GOMSFE model. Similarly, GOMSFE objects for settings need to be validated against factory settings and verified to change when changed in the primary location.

Multicast IED Communication

As discussed earlier, high speed peer-to-peer communication *within the substation* is performed via a connectionless mechanism known as GOOSE. The GOOSE contains two parts: a pre-defined set of 32 data items such as "Trip", "Close", "Lockout", etc. and up to 96 "user defined" remote outputs. Testing of the GOOSE message includes checking for proper bit mapping (i.e. – receiving a lockout message when a lockout message was sent) but also measuring performance under heavy network loading conditions. All pre-defined data items (if supported) must be tested. Additionally, all positions of the user-defined bits must be tested for proper transmission and receipt.

As the source of GOOSE messages could be digital inputs or internal Virtual Inputs, timing of the messages should be checked over two different timing paths. One path should be from issuance of a digital input to the closing of a contact output. This path includes the digital input debounce delay, stack processing time, logic processing time, and output relay operate time. The second timing path should be the internal messaging time – independent of the input and output delays. This timing is typically available from the event recorder inside the IED. Set-up for this test is facilitated by the use of IRIG-B time stamping that can be used to synchronize the event clocks in the IEDs under test.

Client / Server Based IED to IED Communication

This third mode of communication is a connection oriented service which permits IED data sharing outside the confines of the local network. This type of communication would need to be transactionally set up by the user. As such, testing of this mode of operation

needs to be done by the user. Testing would include establishing the condition(s) for the transmission and verifying that the requested message is properly received by the client. Note that the condition(s) for transmission could be triggered either at the client side or at the server side as established by previous agreement (e.g. – change of state of a variable). At this time, the IED to IED exchange parameters have not been established within the substation documents, however, the pieces are in place to proceed once agreement is reached on "how".

External Test Equipment

In the test scenarios described above, the IED was an integral part of the test equipment. There are other operational and performance measures that require additional equipment in order to quantify. In particular, basic Ethernet information such as LAN loading, peak loading, failed packets, collision count, trace recording, etc. are required. There is off the shelf equipment that can be purchased that measure these quantities and numerous others. These tools allow manufacturers to share communication messages as a means of validating interoperability. For example, the issuance of a GOOSE message to trip a breaker can be captured by one manufacturer, E-Mailed to another, and played back to the other manufacturers' IED to verify proper execution of the GOOSE message. It is expected that in the near future, libraries of such recording will be made available as part of interoperability validation.

In addition to the standard Ethernet test equipment, MMS Data Analyzers are starting to appear. An analyzer not only captures the raw data packet but also decodes the MMS messages contained within the data packets thereby providing both the developer and the user extensive debug capabilities.

Conclusions

The hardware and software technology to create a "Network" IED is ready now. The roadmap to a networked substation automation system has been drawn. The utilities of the world are waiting for vehicles to drive down today's automation highway and they expect a vehicle that will be upgradable to drive down tomorrow's automation highway. In all cases, the buyer needs to make sure that the manufacturer has properly road tested the vehicle and he also needs to be aware of the field tests required by each IED.

Bibliography

[1] Substation Integrated Protection, Control, and Data Acquisition Phase 1, Task 2 Requirements Specification; EPRI – RP3599-01

[2] Common Application Service Models (CASM) and Mapping to MMS; ftp://sisconet.com/epri/UCA2.0/CASM_15.ZIP

[3] General Object Model for Substation and Field Equipment (GOMSFE); ftp://sisconet.com/epri/UCA2.0/GOMSFE9.zip