guest editorial

John D. McDonald

substation automation

IED integration and availability of information

ELECTRIC UTILITY DEREGULATION, economic pressures forcing downsizing, and the marketplace pressures of potential takeovers have forced utilities to examine their operational and organizational practices. Utilities are realizing that they must shift their focus to customer service. Customer service requirements all point to one key element: information, i.e., the right amount of information to the right person or computer within the right amount of time. The flow of information requires data communication over extended networks of systems and users. In fact, utilities are becoming among the largest users of data and are the largest users of real-time information.

The advent of industry deregulation has placed greater emphasis on the availability of information, the analysis of this information, and the subsequent decision-making to optimize system operation in a competitive environment. Intelligent electronic devices (IEDs) being implemented in substations today contain valuable information, both operational and nonoperational, needed by many user groups within the utility. The challenge facing utilities is determining a standard integration architecture that meets the utility's specific needs, can extract the desired operational and nonoperational information, and deliver this information to the users who have applications to analyze the information.

This issue of *IEEE Power & Energy Magazine* focuses on substation integration and automation. My Guest Editorial provides an overview of substation integration and automation fundamentals and focuses on best practices. It also includes a list of:

- ✔ further reading material for those who require more information on the same subject
- ✔ acronyms and abbreviations for those readers who are not familiar with the terminology.

Three feature articles follow with more specific information on:

- ✔ a business case methodology for expanding the implementa-

©DIGITAL VISION

Utilities must determine a standard integration architecture that meets their secific needs in extracting desired opertaional and nonoperational data and delivering it to the users.

1540-7977/03/$17.00©2003 IEEE

tion of substation automation technologies at MidAmerican Energy Company

- ✔ a pilot project at Omaha Public Power District to integrate data from various devices within two substations and a simulator
- ✔ a generic architecture that applies the multiagent systems methodology to the field of substation automation.

Open Systems

An open system is a computer system that embodies supplier-independent standards so that software may be applied on many different platforms and can interoperate with other applications on local and remote systems. An open system is an evolutionary means for a substation control system that is based on the use of nonproprietary, standard software and hardware interfaces. Open systems enable future upgrades available from multiple suppliers at lower cost to be integrated with relative ease and low risk.

The concept of open systems applies to substation automation. It is important to learn about the different de jure (legal) and de facto (actual) standards and then apply them so as to eliminate proprietary approaches. An open systems approach allows the incremental upgrade of the automation system without the need for complete replacement, as happened in the past with proprietary systems. There is no longer the need to rely on one supplier for complete implementation. Systems and IEDs from competing suppliers are able to interchange and share information. The benefits of open systems include longer expected system life, investment protection, upgradeability and expandability, and readily available third-party components.

Levels of Integration and Automation

Substation integration and automation can be broken down into five levels, as shown in Figure 1. The lowest level is the power system equipment, such as transformers and circuit breakers. The middle three levels are IED implementation, IED integration, and substation automation applications. All electric utilities are implementing IEDs in their substations. The focus today is on the integration of the IEDs. Once this is done, the focus will shift to what automation applications should run at the substation level. The highest level is the utility enterprise, and there are multiple functional data paths from the substation to the utility enterprise.

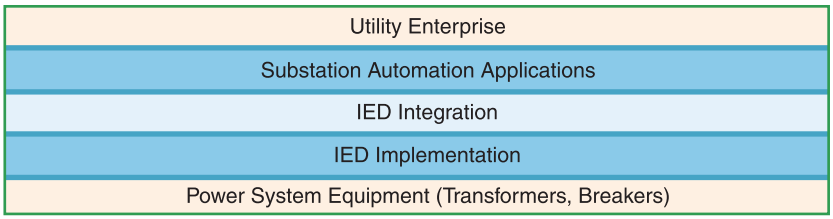

figure 1. Five levels of substation integration and automation.

Since substation integration and automation technology is fairly new, there are no industry standard definitions, except for the definition of an IED. The industry standard definition of an IED is given below, as well as definitions for substation integration and substation automation.

- ✔ *IED*: Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers). An example of a relay IED is shown in Figure 2.
- ✔ *Substation integration*: Integration of protection, control, and data acquisition functions into a minimal number of platforms to reduce capital and operating costs, reduce panel and control room space, and eliminate redundant equipment and databases.
- ✔ *Substation automation*: Deployment of substation and feeder operating functions and applications ranging from supervisory control and data acquisition (SCADA) and alarm processing to integrated volt/var control in order to optimize the management of capital assets and enhance operation and maintenance (O&M) efficiencies with minimal human intervention.

figure 2. Example of a relay IED.

Architecture Functional Data Paths

There are three primary functional data paths from the substation to the utility enterprise, as shown in Figure 3. The most common data path is conveying the operational data (e.g., volts, amps) to the utility's SCADA system every 2 to 4 s. This information is critical for the utility's dispatchers to monitor and control the power system. The most challenging data path is conveying the nonoperational data to the utility's data warehouse. The challenges associated with this data path include the characteristics of the data (waveforms rather than points), the periodicity of data transfer (not continuous, on demand), and the protocols used to obtain the data from the IEDs (not standard, IED supplier's proprietary protocols). Another challenge is whether the data

A corporate data warehouse enables users to access substation data while maintaining a firewall to substation control and operation functions.

is pushed from the substation into the data warehouse, pulled from the data warehouse, or both. The third data path is remote access to an IED by passing through or looping through the substation integration architecture and isolating a particular IED in the substation.

Data Warehouse

The corporate data warehouse enables users to access substation data while maintaining a firewall to substation control and operation functions. Both operational and nonoperational data is needed in the data warehouse. To size the data warehouse, the utility must determine who the users of the substation automation system data are, the nature of their application, the type of data needed, how often the data is needed, and the frequency of update required for each user. Examples of user groups within a utility are substation design engineering, protective relay engineering, protective relay technicians, substation metering, substation operations, control center operations, engineering planning, transmission and distribution engineering, power quality, substation test, substation maintenance, predictive maintenance, communications engineering, SCADA, feeder automation, and information technology.

SA System Functional Architecture Diagram

The functional architecture diagram in Figure 4 shows the three functional data paths from the substation to the utility enterprise, as well as the SCADA system and the data warehouse. The operational data path to the SCADA system utilizes the communication protocol presently supported by the SCADA system. The nonoperational data path to the data warehouse conveys the IED nonoperational data from the SA system to the data warehouse, either being pulled by a data warehouse application from the SA system or being pushed from the SA system to the data warehouse based on an event trigger or time. The remote access path to the substation utilizes a dial-in telephone connection. The global positioning system (GPS) satellite clock time reference is shown, providing a time reference for the SA system and IEDs in the substation. The PC provides the graphical user interface (GUI) and the historical information system for archiving operational and nonoperational data. The SCADA interface knows which SA system points are sent to the SCADA system, as well as the SCADA system protocol. The local area network (LAN) enabled IEDs can be directly connected to the SA LAN. The non-LAN enabled IEDs require a network interface module (NIM) for protocol and physical interface conversion. The IEDs can have various applications, such as equipment condition monitoring (ECM) and relaying, as well as direct (or hardwired) input/output (I/O).

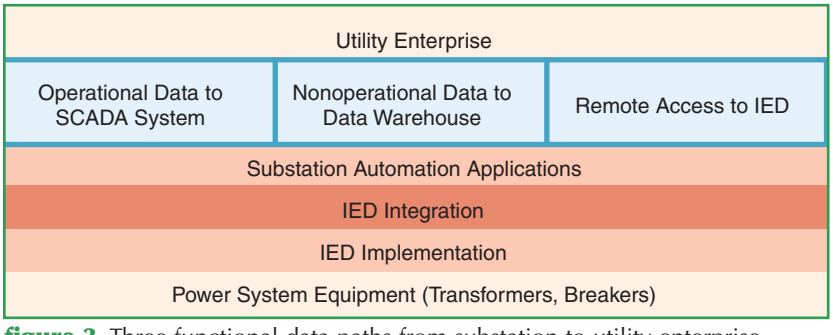

figure 3. Three functional data paths from substation to utility enterprise.

New Versus Existing Substations

The design of new substations has the advantage of starting with a blank sheet of paper. The new substation will typically have many IEDs for different functions, and the majority of operational data for the SCADA system will come from these IEDs. The IEDs will be integrated with digital two-way communications. The small amount of direct input/output (hardwired) can be acquired using programmable logic controllers (PLCs). Typically, there are no conventional remote terminal units (RTUs) in new substations. The RTU functionality is addressed using IEDs, PLCs, and an integration network using digital communications.

In existing substations, there are several alternative approaches, depending on whether or not the substation has a conventional RTU installed. The utility has three choices for their existing conventional substation RTUs:

- ✔ Integrate RTU with IEDs: Many utilities have integrated IEDs with existing conventional RTUs, provided the RTUs support communications with downstream devices and support IED communication protocols. This integration approach works well for the operational data path but does not support the nonoperational and remote-access data paths. The latter two data paths must be done outside of the conventional RTU.
- ✔ Integrate RTU as another substation IED: If the utility desires to keep its conventional RTU, the preferred approach is to integrate the RTU in the substation integration architecture as another IED. In this way, the RTU can be retired easily as the RTU hardwired direct input/output transitions to come primarily from the IEDs.

- ✔ Retire RTU and use IEDs and PLCs as with a new substation: The RTUs may be old and difficult to support, and the substation automation project may be a good time to retire these older RTUs. The hardwired direct input/output from these RTUs would then come from the IEDs and PLCs as with a new substation.

Equipment Condition Monitoring

Many electric utilities have employed ECM to maintain electric equipment in top operating condition while minimizing the number of interruptions. With ECM, equipment-operating parameters are automatically tracked to detect the emergence of various abnormal operating conditions. This allows substation operations personnel to take timely action when needed to improve reliability and extend equipment life. This approach is applied most frequently to substation transformers and high voltage electric supply circuit breakers to minimize the maintenance costs of these devices, as well as improve their availability and extend their useful life. Figure 5 shows an ECM IED installed on a substation transformer.

Equipment availability and reliability may be improved by reducing the amount of offline maintenance and testing required, as well as reducing the number of equipment failures. To be truly effective, equipment condition monitoring should be part of an overall condition-based maintenance strategy that is properly designed and integrated into the regular maintenance program.

ECM IEDs are being implemented by many utilities. In most implementations, the communication link to the IED is via a dial-up telephone line. To facilitate integrating these IEDs into the substation architecture, the ECM IEDs must support at least one of today's widely used IED protocols: Modbus, Modbus Plus, or Distributed Network Protocol version 3 (DNP3). In addition, a migration path to utility communications architecture version 2 (UCA2) manufacturing message specification (MMS) protocol is desired. If the ECM IEDs can be integrated into the substation architecture, the operational data will have a path to the SCADA system, and the nonoperational data will have a path to the utility's data warehouse. In this way, the users and systems throughout the utility that need this information will have access to it. Once the information is brought out of the substation and into the SCADA system and data warehouse, users can share the information in the utility. The "private" databases that result in islands of automation will go away. Therefore, the goal of every utility is to integrate these ECM IEDs into a standard substation integration architecture so that both operational and nonoperational information from the IEDs can be shared by utility users.

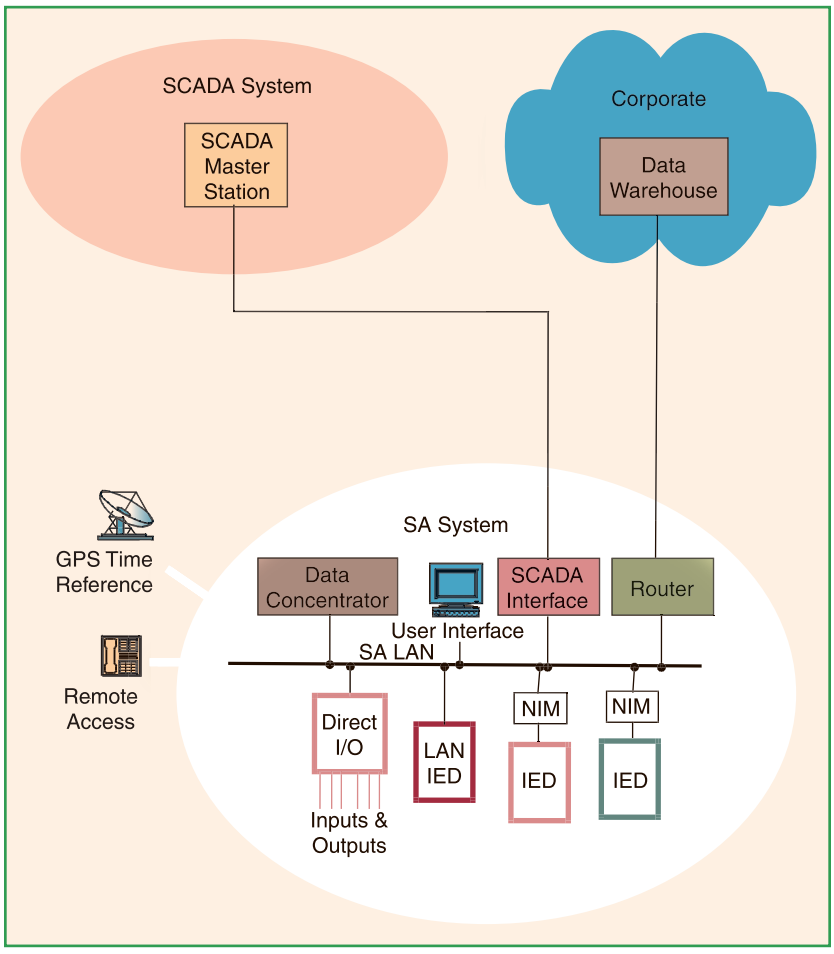

figure 4. SA system functional architecture diagram.

Substation Automation Training Simulator

One of the challenges for electric utilities when implementing substation automation for the first time is to create

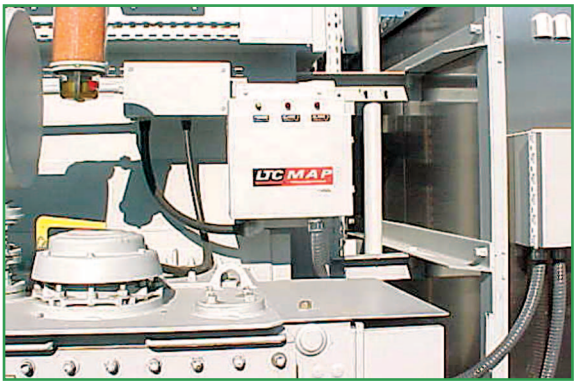

figure 5. ECM IED installed on substation transformer.

figure 6. Substation automation training simulator.

"buy-in" for the new technology within the utility. The more people know about a subject the more comfortable they feel and the better the chance they will use the technology. It is much easier and less stressful to learn about substation automation technology in a training environment, away from the substation, than on a system installed in an energized substation. For these reasons, many utilities purchase a substation automation training simulator (SATS), which is an identical configuration to that installed in substations. The main difference is that the SATS includes at least one of every kind of IED installed in all substations. In addition to training, SATS is used for application development and testing of new IEDs. An example of a SATS presently installed at an electric utility is shown in Figure 6.

Protocol Fundamentals

A communication protocol allows communication between two devices. The devices must have the same protocol (and version) implemented. Any protocol differences will result in communication errors.

If the communication devices and protocols are from the same supplier, i.e., where a supplier has developed a unique protocol to utilize all the capabilities of the two devices, it is unlikely the devices will have trouble communicating. By using a unique protocol of one supplier, a utility can maximize the device's functionality and see a greater return on its investment; however, the unique protocol will constrain the utility to one supplier for support and purchase of future devices.

If the communication devices are from the same supplier but the protocol is an industry-standard protocol supported by the device supplier, the devices should not have trouble communicating. The device supplier has designed its devices to operate with the standard protocol and communicate with other devices using the same protocol and version. By using a standard protocol, the utility may purchase equipment from any supplier that supports the protocol and, therefore, can comparison-shop for the best prices.

Industry-standard protocols typically require more overhead than a supplier's unique protocol. Standard protocols often require a higher speed channel than a supplier's unique protocol for the same efficiency or information throughput. However, high-speed communication channels are more prevalent today and may provide adequate efficiency when using industry-standard protocols. UCA2 MMS is designed to operate efficiently over 10 Mb/s switched or 100 Mb/s shared or switched Ethernet. If a utility is considering UCA2 MMS as its protocol of choice, a prerequisite should be installation of high-speed communications. If the utility's plan is to continue with a communication infrastructure operating at 1,200 to 9,600 b/s, the better choice for an industry-standard protocol would be DNP3.

A utility may not be able to utilize all of a device's functionality using an industry standard protocol. If a device was designed before the industry standard protocol, the protocol may not thoroughly support the device's functionality. If the device was designed after the industry standard protocol was developed, the device should have been designed to work with the standard protocol such that all of the device's functionality is available.

The substation integration and automation architecture must allow devices from different suppliers to communicate (interoperate) using an industry-standard protocol. The utility has the flexibility to choose the best devices for each application, provided the suppliers have designed their devices to achieve full functionality with the protocol. Though devices from different suppliers can operate and communicate under the standard protocol, each device may have capabilities not supported by the other device. There is also a risk that the protocol implementations of the industry-standard protocol by the two suppliers in each device may have differences. Factory testing will verify that the functions of one device are supported by the protocol of the other device and vice versa. If differences and/or incompatibilities are found, they can be corrected during factory testing.

Protocol Considerations

There are two capabilities a utility considers for an IED. The primary capability of an IED is its standalone capabilities, such as protecting the power system for a relay IED. The secondary capability of an IED is its inte-

gration capabilities, such as its physical interface (e.g., RS-232, RS-485, Ethernet) and its communication protocol (e.g., DNP3, Modbus, UCA2 MMS).

Today utilities typically specify the IEDs they want to use in the substation rather than giving a supplier a turnkey contract to provide the supplier's IEDs only in the substation. However, utilities typically choose the IEDs based on the IED's standalone capabilities only, without considering the IED's integration capabilities. Once the IEDs are installed, the utility may find in the future, when they want to integrate the IEDs, that the IEDs were purchased with the IED supplier's proprietary protocol and with a physical interface not desired (RS-485 purchased when Ethernet is desired). When purchasing IEDs, the utility must consider both the standalone capabilities in the choice of the IED and the integration capabilities when ordering the IED, even if the IEDs will not be integrated in the near future.

Today, the most common IED communication protocols are Modbus, Modbus Plus, and DNP3. The UCA2 MMS protocol is becoming commercially available from more IED suppliers and being implemented in more utility substations. However, the implementations may not be optimal (adding a separate box for the UCA2 MMS protocol and Ethernet networking) and may result in poor performance (data latency due to the additional box) rather than the supplier incorporating the new functionality into the existing IED. The utility must be cautious when ordering an IED with other than the IED supplier's target protocol, often supplier proprietary, used in the design of the IED. Some IED functionality may be lost when choosing other than the IED supplier's target protocol.

The most common IED networking technology today in substations is serial communications, either RS-232 or RS-485. As more and more IEDs become available with Ethernet ports, the IED networking technology in the substation will be primarily Ethernet.

Utility Communication Architecture

The use of international protocol standards is now recognized throughout the electric utility industry as a key to successful integration of the various parts of the electric utility enterprise. One area addresses substation integration and automation protocol standardization efforts. These efforts have taken place within the framework provided by the Electric Power Research Institute's (EPRI's) UCA.

UCA is a standards-based approach to utility data communications that provides for wide-scale integration from the utility enterprise level (as well as between utilities) down to the customer interface, including distribution, transmission, power plant, control center, and corporate information systems. UCA version 1.0 specification was issued in December 1991 as part of EPRI Project RP2949, Integration of Utility Communication Systems. While this specification supplied a great deal of functionality, industry adoption was limited, due in part to a lack of detailed specifications about how the specified protocols would actually be used by applications. For example, the MMS (ISO/IEC 9506) protocol was specified for real-time data exchange at many levels within a utility, but specific mappings to MMS for exchanging power

Acronyms and Abbreviations

DNP	distributed network protocol
ECM	equipment condition monitoring
EPRI	Electric Power Research Institute
GOMSFE	generic object models for substation and feeder equipment
GPS	global positioning system
ICCP	inter-control center communications protocol
IEC	International Electrotechnical Commission
IED	intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers, Inc.
I/O	input/output
ISO	International Standards Organization
IT	information technology
LAN	local area network
Mb/s	megabits per second
MMS	manufacturing messaging specification
NIM	network interface module
O&M	operations and maintenance
PES	IEEE Power Engineering Society
PLC	programmable logic controller
PSRC	IEEE PES Power Systems Relaying Committee
RF	radio frequency
RFP	request for proposal
RTU	remote terminal unit
SA	substation automation
SATS	substation automation training simulator
SCADA	supervisory control and data acquisition
TC	technical committee
TCP/IP	transmission control protocol and Internet protocol
UCA	utility communication architecture
var	volt ampere reactive
WAN	wide area network
WG	working group

Benefits of open systems include longer expected system life, investment protection, upgradeability and expandability, and readily available third-party components.

system data and schedules or for communicating directly with substation or distribution feeder devices was lacking, resulting in continuing interoperability problems.

The UCA (MMS) Forum was started in May 1992 to address these UCA application issues. Six working groups were established to consider issues of MMS application in power plants, control centers, customer interface, substation automation, distribution feeder automation, and profile issues. The MMS Forum served as a mechanism for utilities and suppliers to build the technical agreements necessary to achieve a wide range of interoperability using UCA MMS. Out of these efforts came the notion of defining standard power system objects and mapping them onto the services and data types supported by MMS and the other underlying standard protocols. This heavily influenced the definition of the UCA2 specification issued in late 1996, which endorses ten different protocol profiles, including transmission control protocol and Internet protocol (TCP/IP) and inter-control center communications protocol (ICCP), as well as a new set of common application service models for real-time device access.

The EPRI UCA Substation Automation Project began in the early 1990s to produce industry consensus regarding substation integrated control, protection, and data acquisition and to allow interoperability of substation devices from different manufacturers. The Substation Protocol Reference Specification recommended three of the ten UCA2 profiles for use in substation automation. Future efforts in this project were integrated with the efforts in the Utility Substations Initiative.

In mid-1996, American Electric Power hosted the first Utility Substations Initiative meeting, as a continuation of the EPRI UCA Substation Automation Project. Approximately 40 utilities and 25 suppliers are presently participating, having formed supplier/utility teams to define the supplier IED functionality and to implement a standard IED protocol (UCA2 profile) and LAN protocol (Ethernet).

Generic object models for substation and feeder equipment (GOMSFE) are being developed to facilitate suppliers in implementing the UCA Substation Automation Project substation and feeder elements of the power system object model. New IED products with this functionality are now commercially available. The Utility Substations Initiative meets three times each year, in January, May, and September, immediately following the IEEE PES Power System Relaying Committee (PSRC) meetings and in conjunction with the UCA Users Group meetings. Every other meeting includes a supplier interoperability demonstration. The demonstration in September 2002 involved approximately 20 suppliers with products interconnected by a fiber Ethernet LAN interoperating with the UCA2 MMS protocol, the GOMSFE device object models, and Ethernet networks.

The UCA Users Group is a nonprofit organization whose members are utilities, suppliers, and users of communications for utility automation. The mission of the UCA Users Group is to enable utility integration through the deployment of open standards by providing a forum in which the various stakeholders in the utility industry can work cooperatively together as members of a common organization to:

- ✔ influence, select, and/or endorse open and public standards appropriate to the utility market based on the needs of the membership
- ✔ specify, develop, and/or accredit product/system-testing programs that facilitate the field interoperability of products and systems based upon these standards
- ✔ implement educational and promotional activities that increase awareness and deployment of these standards in the utility industry.

The UCA Users Group was first formed in 2001 and presently has 34 corporate members, including 17 suppliers, 14 electric utilities, and three consultants and other organizations. The UCA Users Group organization consists of a Board of Directors, with the Executive Committee and Technical Committee reporting to the board. The Executive Committee has three committees reporting to it: Marketing, Liaison, and Membership. The Technical Committee has a number of committees reporting to it, including Substation, Communications, Products, Object Models (IEC 61850/GOMSFE), and Test Procedures. The Web site for the UCA Users Group is www.ucausersgroup.org. The group meets three times each year, in January, May and September, immediately following the IEEE PES PSRC meetings and in conjunction with the Utility Substations Initiative meetings. In addition, the UCA Users Group will meet at the IEEE PES Substations Committee Annual Meeting 27-30 April 2003 in Sun Valley, Idaho. This meeting will include a supplier interoperability demonstration with 20 to 25 suppliers demonstrating the implementation of the UCA2 MMS protocol and Ethernet networking technology into their IEDs and products and interoperating with the other suppliers' equipment.

IEC 61850

The UCA2 substation automation work has been brought to IEC Technical Committee (TC) 57 Working Groups

(WGs) 10, 11, and 12, who are developing IEC 61850, the single worldwide standard for substation automation communications. IEC 61850 is based on UCA2 and European experience and provides additional functions such as substation configuration language and a digital interface to nonconventional current and potential transformers.

Distributed Network Protocol

The development of DNP was a comprehensive effort to achieve open, standards-based interoperability between substation computers, RTUs, IEDs, and master stations (except inter-master-station communications) for the electric utility industry. DNP is based on the standards of the IEC TC 57, WG 03. DNP has been designed to be as close to compliant as possible to the standards as they existed at the time of development with the addition of functionality not identified in Europe but needed for current and future North American applications (e.g., limited transport layer functions to support 2K block transfers for IEDs, radio frequency (RF), and fiber support). The present version of DNP is DNP3, which is defined in three distinct levels. Level 1 has the least functionality, for simple IEDs, and Level 3 has the most functionality, for SCADA master-station communication front-end processors.

The short-term benefits of using DNP are:

- ✔ interoperability between multi-supplier devices
- ✔ fewer protocols to support in the field
- ✔ reduced software costs
- ✔ no protocol translators needed
- ✔ shorter delivery schedules
- ✔ less testing, maintenance, and training
- ✔ improved documentation
- ✔ independent conformance testing
- ✔ support by independent user group and third-party sources (e.g., test sets, source code).

In the long term, further benefits can be derived from using DNP, including:

- ✔ easy system expansion
- ✔ long product life
- ✔ more value-added products from suppliers
- ✔ faster adoption of new technology
- ✔ major operations savings.

DNP was developed by Harris, Distributed Automation Products, in Calgary, Alberta, Canada. In November 1993, responsibility for defining further DNP specifications and ownership of the DNP specifications was turned over to the DNP User Group, a group composed of utilities and suppliers who are utilizing the protocol. The DNP User Group is a forum of over 300 users and implementers of the DNP3 protocol worldwide. The major objectives of the group are to:

- ✔ maintain control of the protocol and determine the direction in which the protocol will migrate
- ✔ review and add new features, functions, and enhancements to the protocol
- ✔ encourage suppliers and utilities to adopt the DNP3 protocol as a standard
- ✔ define recommended protocol subsets
- ✔ develop test procedures and verification programs
- ✔ support implementer interaction and information exchange.

The DNP User Group has an annual general meeting in North America, usually in conjunction with the DistribuTECH Conference in February/March. The Web site for DNP and the DNP User Group is www.dnp.org. The DNP User Group Technical Committee is an open volunteer organization of industry and technical experts from around the world. This committee evaluates suggested modifications or additions to the protocol and then amends the protocol description as directed by the User Group members.

Choosing the Right Protocol

There are several factors to consider when choosing the right protocol for your application. First, determine the system area with which you are most concerned, e.g., the protocol from a SCADA master station to the SCADA RTUs, a protocol from substation IEDs to an RTU or a PLC, or a LAN in the substation. Second, determine the timing of your installation, e.g., six months, 18 to 24 months, or three to five years. In some application areas, technology is changing so quickly that the timing of your installation can have a great impact on your protocol choice. If you are implementing new IEDs in the substation and need them to be in service in six months, you could narrow your protocol choices to DNP3, Modbus, and Modbus Plus. These protocols are used extensively in IEDs today. If you choose an IED that is commercially available with UCA2 MMS capability today, then you may choose UCA2 MMS as your protocol.

If your timeframe is one to two years, you should consider IC 61850 and UCA2 MMS as the protocol. Monitor the results of the Utility Substation Communication Initiative utility demonstration sites. These sites have implemented new supplier IED products that are using UCA2 MMS as the IED communication protocol and Ethernet as the substation local area network.

If your timeframe is near term (six to nine months), make protocol choices from suppliers who are participating in the industry initiatives and are incorporating this technology into their product's migration paths. This will help protect your investment from becoming obsolete by allowing incremental upgrades to new technologies.

Communication Protocol Application Areas

There are various protocol choices depending on the protocol application area of your system. Protocol choices vary with the different application areas. Different application areas are in different stages of protocol development and industry efforts. The status of development efforts for different applications will help determine realistic plans and schedules for your specific projects.

Selecting the right supplier ensures that you stay informed about industry developments and trends and allows you to access new technologies with the least impact on your current operation.

Within the Substation

The need for a standard IED protocol dates back to the late 1980s. IED suppliers acknowledge that their expertise is in the IED itself, not in two-way communications capability, the communications protocol, or added IED functionality from a remote user. Though the industry made some effort to add communications capability to the IEDs, each IED supplier was concerned that any increased functionality would compromise performance and drive the IED cost so high that no utility would buy it. Therefore, the industry vowed to keep costs competitive and performance high as standardization was incorporated into the IED.

The IED supplier's lack of experience in two-way communications and communication protocols resulted in crude, primitive protocols and, in some cases, no individual addressability and improper error checking (no select-before-operate). Each IED required its own communication channel, but only limited channels, if any, were available from RTUs. SCADA system and RTU suppliers were pressured to develop the capability to communicate to IEDs purchased by the utilities. Each RTU and IED interface required not only a new protocol but a proprietary protocol not used by any other IED.

It was at this point that the Data Acquisition, Processing and Control Systems Subcommittee of the IEEE Power Engineering Society (PES) Substations Committee recognized the need for a standard IED protocol. The subcommittee formed a task force to examine existing protocols and determine, based on two sets of screening criteria, the two best candidates. *Trial Use Recommended Practice for Data Communications Between Intelligent Electronic Devices and Remote Terminal Units in a Substation* (IEEE Standard 1379) was published in March 1998. This document did not establish a new communication protocol. To quickly achieve industry acceptance and use, it instead provided a specific implementation of two existing communication protocols in the public domain, DNP3 and IEC 870-5-101.

For IED communications, if your implementation timeframe is six to nine months, select from protocols that already exist: DNP3, Modbus, and Modbus Plus. However, if the implementation timeframe is one year or more, consider UCA2 MMS as the communications protocol. Regardless of your timeframe, evaluate each supplier's product migration plans. Try to determine if the system will allow migration from today's IED with DNP3 to tomorrow's IED with UCA2 MMS without replacing the entire IED. This will leave open the option of migrating the IEDs in the substation to UCA2 in an incremental manner, without wholesale replacement. If you choose an IED that is commercially available with UCA2 MMS capability today, then you may want to choose UCA2 MMS as your IED protocol.

Substation to Utility Enterprise

This is the area of traditional SCADA communication protocols. The Data Acquisition, Processing, and Control Systems Subcommittee of the IEEE PES Substations Committee began developing a recommended practice in the early 1980s in an attempt to standardize master/remote communications practices. At that time, each SCADA system supplier had developed a proprietary protocol based on technology of the time. These proprietary protocols exhibited varied message structures, terminal-to-data circuit terminating equipment (DCE) and DCE-to-channel interfaces, and error detection and recovery schemes. The *IEEE Recommended Practice for Master/Remote Supervisory Control and Data Acquisition (SCADA) Communications* (IEEE Standard 999-1992) addressed this nonuniformity among the protocols, provided definitions and terminology for protocols, and simplified the interfacing of more than one supplier's RTUs to a master station.

The major standardization effort undertaken in this application area has taken place in Europe as part of the IEC standards-making process. The effort resulted in the development of the IEC 870-5 protocol, which was slightly modified by GE (Canada) to create DNP. This protocol incorporated a pseudo transport layer, allowing it to support multiple master stations. The goal of DNP was to define a generic standards-based (IEC 870-5) protocol for use between IEDs and data concentrators within the substation, as well as between the substation and the SCADA system control center. Success led to the creation of the supplier-sponsored DNP User Group that currently maintains full control over the protocol and its future direction. DNP3 has become a de facto standard in the electric power industry and is widely supported by suppliers of test tools, protocol libraries, and services.

Cyber Security

When today's control systems were designed, information and system security was not a priority. SCADA and other control systems were designed as proprietary, stand-alone systems, and their security resulted from their physical and logical isolation and controlled access to them. As information technology becomes increasingly advanced, substation automation continues to move to open, standards-based net-

working technologies and/or the Internet to bring the benefits of information sharing to operations. All suppliers have the capability to implement Web-based applications to perform monitoring, control, and remote diagnostics. This, however, leads to control system cyber vulnerabilities. Existing information technology (IT) can protect substation control systems from traditional IT vulnerabilities, but they are not designed to protect control systems against vulnerabilities unique to control systems.

A security policy and a mechanism for its enforcement should be developed for the substation. A minimum list of questions to be addressed before attaching the SA system (or SCADA system) to the network include the following.

- ✔ Which network users and applications require control system access?
- ✔ What do they need access to?
- ✔ What type of remote access does the user require (e.g., dial-up, telnet, ftp, X-sessions, PCAnywhere, etc.)?
- ✔ What are the security risks associated with each type of access?
- ✔ Is the information required worth the security risk?
- ✔ Is the password capable of being changed?
- ✔ How often should it be changed?
- ✔ Who is the system administrator?

Make Decisions with the Future in Mind

As we look to the future, it seems the time between the present and the future is shrinking. When a PC bought today is made obsolete in six months by a new model with twice the performance at less cost, how can you protect the investments in technology you make today? Obviously, there is no way you can keep up on a continuous basis with all the technology developments in all areas. You must rely on others to keep you informed, and who you select to keep you informed is critical. With every purchase, you must evaluate not only the supplier's present products but also its future product development plans.

- ✔ Does the supplier continuously enhance and upgrade products?
- ✔ Is the supplier developing new products to meet future needs?
- ✔ Do existing products have a migration path to enhanced and new products?

Selecting the right supplier will ensure you stay informed about new and future industry developments and trends and will allow you to access new technologies with the least impact on your current operation.

Further Reading

Fundamentals of Supervisory Systems, IEEE Tutorial 94 EH0392-1 PWR, 1994.

IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control, IEEE Standard C37.1-1994.

IEEE Standard Electrical Power System Device Function Numbers and Contact Designations, IEEE Standard C37.2-1996.

Communication Protocols, IEEE Tutorial 95 TP 103, 1995.

Trial Use Recommended Practice for Data Communications Between Intelligent Electronic Devices and Remote Terminal Units in a Substation, IEEE Standard 1379-1997.

Advancements in Microprocessor-Based Protection and Communication, IEEE Tutorial 97TP120-0, 1997.

C. Newton, "Keys to an automated future: Decision maker series interview of John McDonald," *T&D World*, pp. 68-71, Feb. 1999.

J.D. McDonald, "Substations," in *Electric Power Engineering Handbook*. Boca Raton, FL: CRC Press, 2000, ch. 5.

J.D. McDonald and Southern Engineering, *Automating a Distribution Cooperative, from A to Z*, National Rural Electric Cooperative Association (NRECA) Cooperative Research Network (CRN), 1999.

J.D. McDonald and T.L. Saxton, "Understanding today's protocol standardization efforts," *Utility Automation*, pp. 32-36, Sep./Oct. 1997.

J.D. McDonald, J.T. Robinson, and L.T. Swartz, "Substation communication and protocols: Field trials and international standards," presented at 1998 CEPSI Conf., Pattaya, Thailand, 1998.

J.D. McDonald, D.G. Caceres, S.H. Borlase, and M.C. Janssen, "Standardized design of transmission substation automation systems," Congresso del Centro de Argentino de Ingenieros 1998, Buenos Aires, Argentina, 1998.

J.D. McDonald, D.G. Caceres, S.H. Borlase, M.C. Janssen, and J.C. Olaya, "ISA embraces open architecture," *T&D World*, Oct. 1999.

J.D. McDonald, "Industry activities in substation protocol standardization," EPRI Substation Equipment Diagnostics Conf. IX, New Orleans, LA, Feb. 2001.

J.D. McDonald, M. Doghman, and B. Dahl, "Present and future integration of diagnostic equipment monitoring at OPPD," EPRI Substation Equipment Diagnostics Conf. IX, New Orleans, LA, Feb. 2001.

Biography

John D. McDonald received his B.S. and M.S. degrees in electrical engineering from Purdue University and an MBA from the University of California at Berkeley. As senior principal consultant and manager of Automation, Reliability, and Asset Management for KEMA Consulting, he assists electric utilities in substation integration and automation, distribution management systems, distribution SCADA systems, and communication protocols. He is a Fellow of the IEEE, secretary of the IEEE PES, past-chair of the IEEE PES Substations Committee, and recipient of the IEEE Millennium Medal in 2000 and the IEEE PES Award for Excellence in Power Distribution Engineering in 2002. He gives tutorials and seminars in substation automation, distribution SCADA, and communications for various IEEE PES local chapters as an IEEE PES Distinguished Lecturer. He was editor of the "Substations" chapter and a coauthor for the book *The Electric Power Engineering Handbook*, cosponsored by the IEEE PES and published by the CRC Press in 2000. He is editor-in-chief and author of the "Substation Integration and Automation" chapter for the book *The Electric Power Substation Engineering Handbook*, to be published by the CRC Press in 2003.