Substation Communication History and Practice

Daniel E. Nordell, P.E.
d.nordell@ieee.org

1. Introduction

Modern electric power systems have been dubbed "the largest machine made by mankind" because they are both physically large – literally thousands of miles in dimension – and operate in precise synchronism. In North America, for example, the entire West Coast, everything east of the Rocky Mountains, and the State of Texas operate as three autonomous interconnected "machines". The task of keeping such a large machine functioning without breaking itself apart is not trivial. The fact that power systems work as reliably as they do is a tribute to the level of sophistication that is built into them. Substation communication plays a vital role in power system operation. This paper provides a brief historical overview of substation communication, followed by sections which:

- Review functional and communication requirements
- Examine the components of both traditional and emerging Supervisory Control and Data Acquisition (SCADA) systems
- Review the characteristics of past, present, and future substation communication protocols
- Review the role of standards for substation communication
- Discuss the electromagnetic environment which substation communication devices must withstand
- Discuss security aspects of substation communications
- Discuss communication media options for substation communications

2. Supervisory Control and Data Acquisition (SCADA) Historical Perspective

Electric power systems as we know them began developing in the early 20th century. Initially generating plants ("generating stations") were associated only with local loads that typically consisted of lighting and electric transportation. If anything in the system failed – generating plant, power lines, or connections – the lights would quite literally be "out". Customers had not yet learned to depend on electricity being nearly 100% reliable, so outages, whether routine or emergency, were taken as a matter of course.

As reliance on electric power grew, so did the need to find ways to improve reliability. Generating stations and power lines were interconnected to provide redundancy and higher voltages were used for longer distance transportation of electricity. Points where power lines came together or where voltages were transformed came to be known as "substations". Substations often employed protective devices to allow system failures to be isolated so that faults would not bring down the entire system and operating personnel were often stationed at these important points in the electrical system so that they could monitor and quickly respond to any problems which might arise. They would communicate with central system dispatchers by any means available – often by telephone – to keep them apprised of the condition of the system. Such "manned" substations were normative throughout the first half of the 20th century.


If It's "Remote-Control"
Strowger Products
Will Do It

AUTOMATIC ELECTRIC COMPANY

Figure 1: October 31, 1932 Electrical World Advertisement

As the demands for reliable electric power became greater and as labor became a more significant part of the cost of providing electric power, technologies known as "Supervisory Control and Data Acquisition", or SCADA for short, were developed which would allow remote monitoring and even control of key system parameters. SCADA systems began to reduce and even eliminate the need for personnel to be on-hand at substations.

Early SCADA systems provided remote indication and control of substation parameters using technology borrowed from automatic telephone switching systems. As early as 1932 Automatic Electric was advertising "Remote-Control" products based on its successful line of "Strowger" telephone switching apparatus (See Figure 1). Another example (used as late as the 1960's) was an early Westinghouse REDAC

system that used telephone-type electromechanical relay equipment at both ends of a conventional "twisted-pair" telephone circuit. Data rates on these early systems were slow – data was sent in the same manner as rotary-dial telephone commands – ten bits per second - so only a limited amount of information could be passed using this technology.

Early SCADA systems were built on the notion of replicating remote controls, lamps, and analog indications at the functional equivalent of pushbuttons, often placed on a mapboard for easy operator interface. The SCADA masters simply replicated, point-for-point, control circuits connected to the remote, or slave, unit.

During the same timeframe as SCADA systems were developing, a second technology – remote teleprinting, or "Teletype" – was coming of age, and by the 1960's had gone through several generations of development. The invention of a second device – the "modem" (MOdulator / DEModulator) allowed digital information to be sent over wire pairs which had been engineered to only carry the electronic equivalent of human voice communication. With the introduction of digital electronics it was possible to use faster data streams to provide remote indication and control of system parameters. This marriage of Teletype technology with digital electronics gave birth to "Remote Terminal Units" (RTU's) which were typically built with discrete solid-state electronics and which could provide remote indication and control of both individual events and analog voltage and current quantities.

Beginning also in the late 1960's and early 1970's technology leaders began exploring the use of small computers (minicomputers at that time) in substations to provide advanced functional and communication capability. But early application of computers in electric substations met with industry resistance because of perceived and real reliability issues.

The introduction of the microprocessor with the Intel 4004 in 1971 (see http://www.intel4004.com for a fascinating history) opened the door for increasing sophistication in RTU design that is still continuing today. Traditional point-oriented RTU's that reported events and analog quantities could be built in a fraction of the physical size required by previous digital logic designs. More intelligence could be introduced into the device to increase its functionality. For the first time RTU's could be built which reported quantities in engineering units rather than as raw binary values. One early design developed at Northern States Power Company in 1972 used the Intel 4004 as the basis for a "Standardized Environmental Data Acquisition and Retrieval (SEDAR)" system which collected, logged, and reported environmental information in engineering units using only 4 kilobytes of program memory and 512 nibbles (half-bytes) of data memory.

While the microprocessor offered the potential for greatly increased functionality at lower cost, the industry also demanded very high reliability and long service life measured in decades that were difficult to achieve with early devices. Thus the industry was slow to accept the use of microprocessor technology in mission-critical applications. By the late 1970's and early 1980's integrated microprocessor-based devices were introduced which came to be known as "Intelligent Electronic Devices", or IED's,

Early IED's simply replicated the functionality of their predecessors – remotely reporting and controlling contact closures and analog quantities using proprietary communication protocols. Increasingly, IED's are being used also to convert data into engineering unit values in the field and to participate in field-based control algorithms. Many IED's are being built with programmable logic controller (PLC) capability and, indeed, PLC's are being used as RTU's and IED's to the point that the distinction between these different types of smart field devices is rapidly blurring.

Early SCADA communication protocols were usually proprietary in nature and were also often kept secret from the industry. A trend beginning in the mid-1980's has been to minimize the number of proprietary communication practices and to drive field practices toward open, standards-based specifications. Two noteworthy pieces of work in this respect are the International Electrotechnical Commission (IEC) 870-5 family of standards and the IEC 61850 standard. The IEC 870-5 work represents the pinnacle of the traditional point-list-oriented SCADA protocols, while the IEC 61850 standard is the first of an emerging approach to networkable, object-oriented SCADA protocols based on work started in the mid-1980's by the Electric Power Research Institute which became known as the Utility Communication Architecture (UCA).

3. SCADA Functional Requirements

Design of any system should always be preceded by a formal determination of the business and corresponding technical requirements that drive the design. Such a formal statement is known as a "Functional Requirements Specification". Functional requirements capture the intended behavior of the system. This behavior may be expressed as services, tasks or functions the system is required to perform.

In the case of SCADA it will contain such information as system status points to be monitored, desired control points, and analog quantities to be monitored. It will also include identification of acceptable delays between when an event happens and when it is reported, required precision for

analog quantities, and acceptable reliability levels. The functional requirements analysis will also include a determination of the number of remote points to be monitored and controlled. It should also include identification of communication stakeholders other than the control center, such as maintenance engineers and system planners who may need communication with the substation for reasons other than real-time operating functionality.

The functional requirements analysis should also include a formal recognition of the physical, electrical, communications, and security environment in which the communications is expected to operate. Considerations here include recognizing the possible (likely) existence of electromagnetic interference from nearby power systems, identifying available communications facilities, identifying functionally the locations between which communication is expected to take place, and identifying communication security threats which might be presented to the system.

It is sometimes difficult to identify all of the items to be included in the functional requirements, and a technique which has been found useful in the industry is to construct a number of example "use cases" which detail particular individual sets of requirements. Aggregate use cases can form a basis for a more formal collection of requirements.

4. SCADA Communication Requirements

After the functional requirements have been articulated, the corresponding architectural design for the communication system can be set forth. Communication requirements include those elements that must be included in order to meet the functional requirements.

Some elements of the communication requirements include:

- Identification of communication traffic flows – source/destination/quantity
- Overall system topology – eg, star, mesh
- Identification of end system locations
- Device/Processor Capabilities
- Communication Session/Dialog Characteristics
- Device Addressing schemes
- Communication Network Traffic Characteristics
- Performance Requirements

- Timing Issues
- Reliability/Backup/Failover
- Application Service Requirements
- Application Data Formats
- Operational Requirements (Directory, Security, and Management of the network)
- Quantification of electromagnetic interference withstand requirements

5. Components of a SCADA System

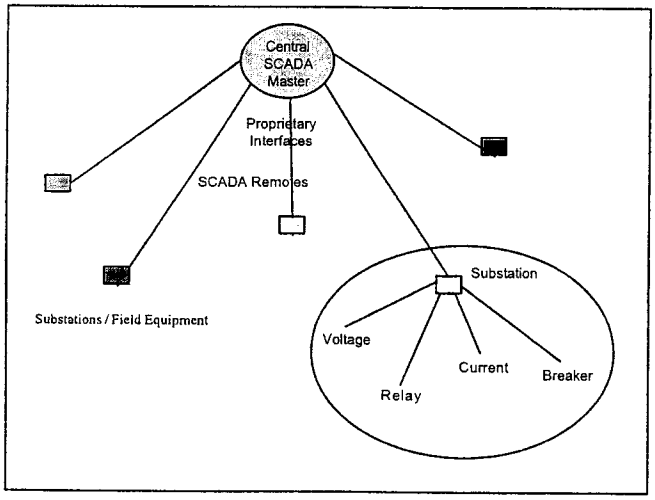


Figure 2: Traditional SCADA System Topology

Traditional SCADA systems grew up with the notion of a SCADA "master" and a SCADA "slave" or "remote". The implicit topology was that of a "star" or "spoke and hub", with the master in charge. In the historical context, the "master" was a hardwired device with the functional equivalent of indicator lamps and pushbuttons (see Figure 2).

Modern SCADA systems employ a computerized SCADA Master in which the remote information is either displayed on an operator's computer terminal or made available to a larger "Energy Management System" through networked connections. The substation RTU is either hardwired to digital, analog, and control points or frequently acts as a "sub-master" or "data concentrator" in which connections to intelligent devices inside the substation are made using communication links. Most interfaces in these systems are proprietary, although in recent years standards-based communication protocols to the remote terminal units have become popular. In these systems if other stakeholders such as engineers or system planners need access to the substation for configuration or diagnostic information, separate, often ad-hoc, provision is usually made using technologies such as dial-up telephone circuits.

With the introduction of networkable communication protocols, typified by the IEC 61850 series of standards, it is now possible to simultaneously

support communication with multiple clients located at multiple remote locations. Figure 3 shows how such a network might look. This

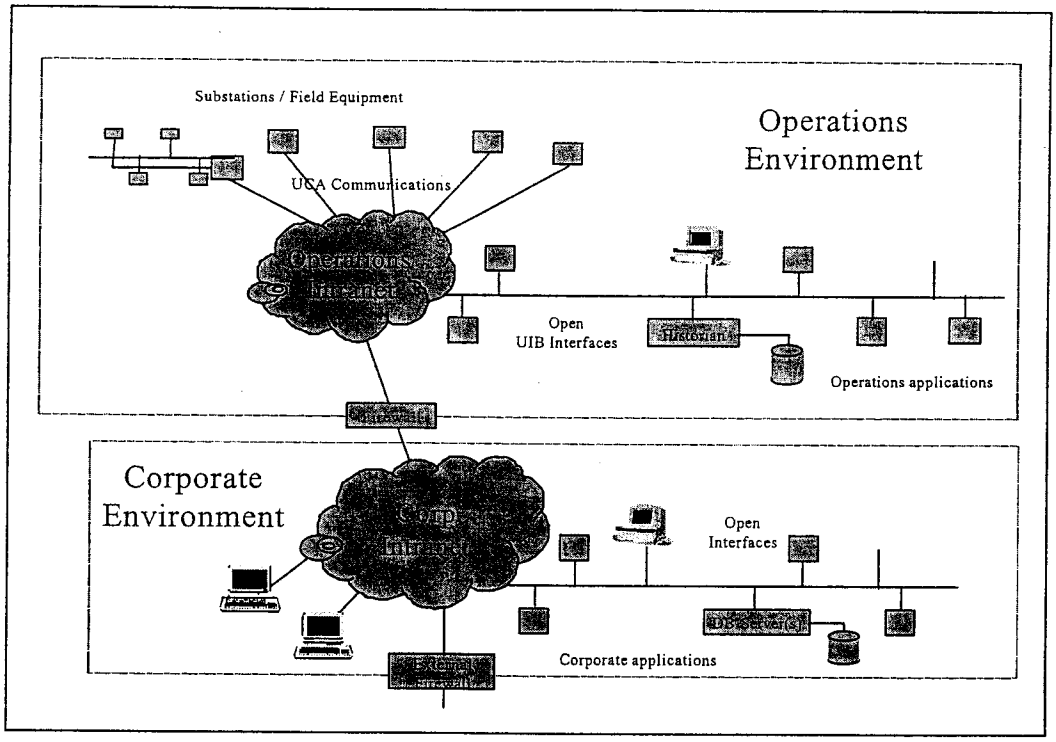


Figure 3: Networked SCADA Communications

configuration will support clients located at multiple sites simultaneously accessing substation devices for applications as diverse as SCADA, device administration, system fault analysis, metering, and system load studies.

SCADA systems as traditionally conceived report only real-time information. Another function shown on Figure 3 which may be included in a modern SCADA system is that of an historian which time-tags each change of state of selected status parameters or each change (beyond a chosen deadband) of analog parameters and then stores this information in an efficient data store which can be used to rebuild the system state at any selected time for system performance analyses.

6. SCADA Communication Protocols: Past, Present, and Future

As noted in the section on SCADA history, early SCADA protocols were built on electromechanical telephone switching technology. Signaling was usually done using pulsed direct-current signals at a data rate on the order of ten pulses per second. Analog information could be sent using "current loops", which are able to communicate over large distances (thousands of

feet) without loss of signal quality. Control and status points were indexed using assigned positions in the pulse train. Analog information was sent using "current loops" which could provide constant current independent of circuit impedance. Communications security was assured by means of repetition of commands or such mechanisms as "arm" and "execute" for control.

With the advent of digital communications (still pre-computer), higher data rates were possible. Analog values could be sent in digital form using analog-to-digital converters, and errors could be detected using parity bits and block checksums. Control and status points were assigned positions in the data blocks which needed to be synchronized between the remote and master devices. Changes of status were detected by means of repetitive "scans" of remote devices, with the "scan rate" being a critical system design factor. Communications integrity was assured by the use of more sophisticated block ciphers including the "cyclical redundancy check" which could detect both single- and multiple- bit errors in communications. Control integrity was ensured by the use of end-to-end "select-check-operate" procedures. Each manufacturer (and sometimes user) of these early SCADA systems would typically define their own communication protocol and the industry became known for the large number of competing practices.

Computer-based SCADA master stations, followed by microprocessor-based remote terminal units, continued the traditions set by the early systems of using points-list-based representations of control and status information. Newer, still-proprietary, communication protocols became increasingly sophisticated in the types of control and status information which could be passed. The notion of "report by exception" was introduced in which a remote terminal could report "no change" in response to a master station poll, thus conserving communication resources and reducing average poll times.

By the early 1980's the electric utility industry enjoyed the marketplace confusion brought by on the order of 100 competing proprietary SCADA protocols and their variants. With the rising understanding of the value of building on open practices, a number of groups began to approach the task of bringing standard practices to bear on utility SCADA practices. As shown in Figure 4, a number of different groups are often involved in the process of reaching consensus on standard practices. The process reads from the bottom to the top, with the "International Standards" level the most sought-after and also often the most difficult to achieve. Often the process starts with practices which have been found useful in the marketplace but which are, at least initially, defined and controlled by a particular vendor or, sometimes, end user. The list of vendor-specific SCADA protocols is long and usually references particular vendors. One

such list (from a vendor's list of supported protocols) reads like a "who's who" of SCADA protocols and includes:

> Conitel, CDC Type 1 and Type II, Harris 5000, Modicon MODBus, PG&E 2179, PMS-91, QUICS IV, SES-92, TeleGyr 8979, PSE Quad 4 Meter, Cooper 2179, JEM 1, Quantum Qdip, Schweitzer Relay Protocol (221, 251, 351), and Transdata Mark V Meter

Groups at the Institute of Electrical and Electronics Engineers (IEEE), the International Electrotechnical Commission (IEC), and the Electric Power Research Institute (EPRI) all started in the mid-1980's to look at the problem of the proliferation of SCADA protocols. IEC Technical Committee 57 (IEC TC57) working group 3 (WG 3) began work on it's

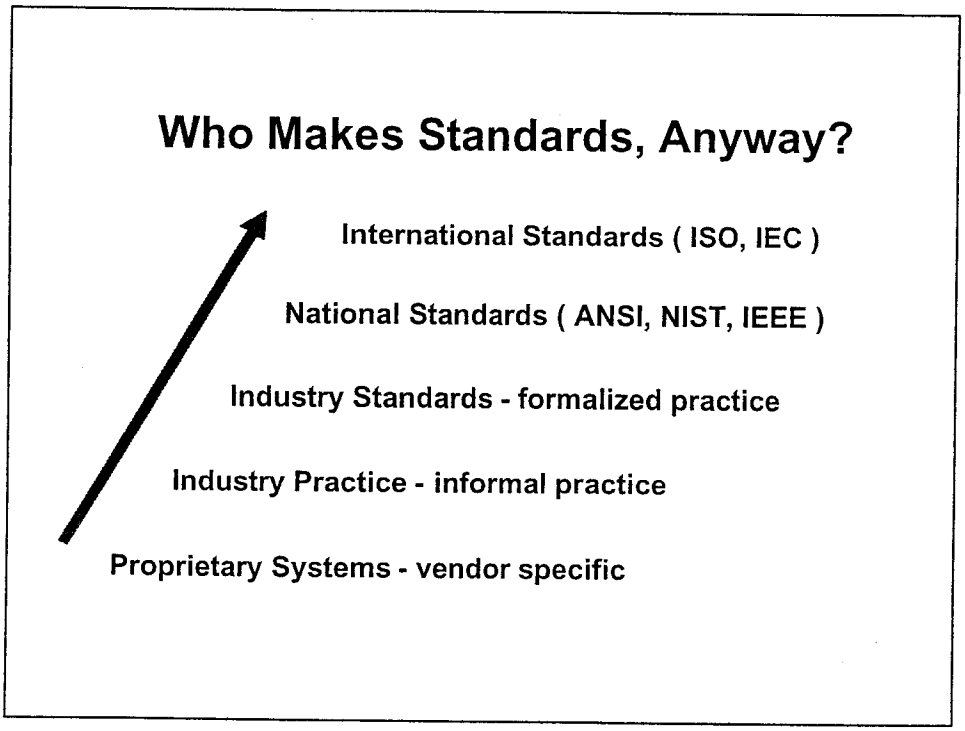


Figure 4: The Standards Process

"870" series of telecontrol standards. Groups within the IEEE Substations and Relay Committees began examining the need for consensus for SCADA protocols. And EPRI began a project which became known as the "Utility Communications Architecture" in an effort to specify an enterprise-wide, networkable, communications architecture which would serve business applications, control centers, power plants, substations, distribution systems, transmission systems, and metering systems.

6.1 DNP

With the IEC work partially completed, a North American manufacturer adapted the IEC 870-5-3 and 870-5-4 draft documents plus additional North American requirements to draft a new "DNP" protocol, which was

Limited to 16-bit address space (65,000 addresses)

TCP/IP - Limited to ~4 billion addresses. New IPG protocol will remove limits

On internet/intranet

released to the "DNP Users Group" (www.dnp.org) in November 1993. DNP3 was subsequently selected as a Recommended Practice by the IEEE Substation Committee C.2 Task Force for an RTU to IED Communications Protocol (IEEE Std 1379-1997 IEEE Trial-Use Recommended Practice for Data Communications Between Intelligent Electronic Devices and Remote Terminal Units in a Substation). DNP has enjoyed considerable success in the marketplace and represents the pinnacle of traditional points-list-oriented SCADA protocols.

6.2 IEC 870-5

The IEC TC57 WG3 continued work on its telecontrol protocol and has issued several standards in the IEC 60870-5 series (www.iec.ch) which collectively define an international consensus standard for telecontrol. IEC 870-5 has recently issued a new transport profile (104) which can be used over wide-area networks. 870-5 represents the best international consensus for traditional control center – to – substation telecommunication and, as noted above, is closely related to the North American DNP protocol.

6.3 UCA 1.0

The EPRI UCA project published its initial results in December of 1991. The UCA 1.0 specification outlines a communication architecture based on existing international standards. It specifies the use of the Manufacturing Message Specification (MMS: ISO 9506) in the application layer for substation communications.

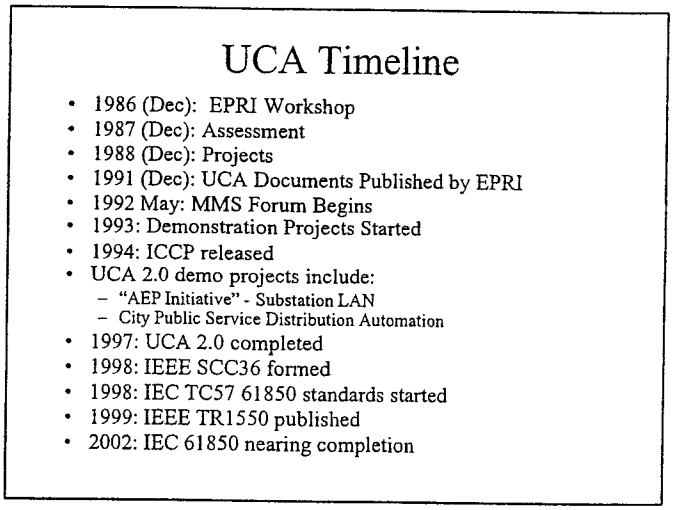


Figure 5: UCA Timeline

6.4 ICCP

The UCA 1.0 work became the basis for IEC 60870-6-503 (2002-04), entitled "Telecontrol equipment and systems - Part 6-503: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE.2 Services and protocol". Also known as ICCP, this specification calls for the use of MMS and was designed to provide standardized communication services between control centers, but has also been used to provide communication services between a control center and its associated substations.

6.5 UCA 2.0

Continuing work to develop the substation and IED communication portions of UCA was conducted in the MMS Forum beginning in 1992. This work resulted in the issuance of a UCA 2.0 report which was published as IEEE Technical Report 1550 (TR1550) (www.ieee.org) in December 1998.

6.6 IEC 61850

IEEE TR1550 became the basis for the new generation of IEC 61850 standards for communication with substation devices. The feature which distinguishes UCA and its IEC 61850 successor from traditional SCADA protocols is that they are networkable and are object-oriented so that a device can describe its attributes when asked. This allows the possibility of self-discovery and "pick-list" configuration of SCADA systems rather than the labor-intensive and more error-prone points-list systems associated with earlier SCADA protocols.

6.7 Continuing Work

Work is continuing in IEC TC57 WG13 and WG14 to define object-oriented presentation of real-time operations information to the business enterprise environment using best networking practices. TC57 has also recently commissioned a new Working Group 15 to evaluate and recommend security practices for the IEC protocols.

7. The Structure of a SCADA Communication Protocol

The fundamental task of a SCADA communications protocol is to transport a "payload" of information (both digital and analog) from the substation to the control center and to allow remote control in the substation of selected operating parameters from the control center. Other functions that are required but usually not included in traditional SCADA protocols include the ability to access and download detailed event files and oscillography and the ability to remotely access substation devices for administrative purposes. These functions are often provided using ancillary dial-up telephone-based communication channels. Newer, networkable, communication practices such as IEC 61850 make provision for all of the above functionality and more using a single wide area network connection to the substation.

From a communications perspective, all communication protocols have at their core a "payload" of information that is to be transported. That payload is then wrapped in either a simple addressing and error detection envelope and sent over a communication channel (traditional protocols) or is wrapped in additional layers of application layer and networking protocols which allow transport over wide area networks (routable object-oriented protocols like IEC 61850).

In order to help bring clarity to the several parts of protocol functionality, in 1984 the International Standards Organization (ISO) issued Standard

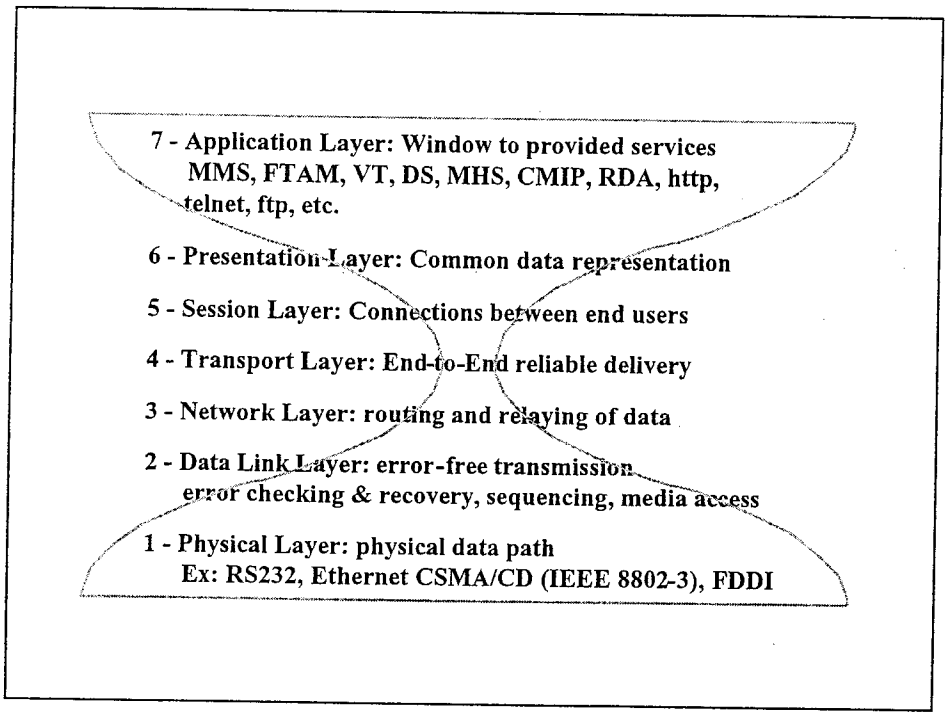


Figure 6: OSI Reference Model

ISO/IEC 7498 entitled "Reference Model of Open Systems Interconnection" or, simply, the OSI Reference Model. The model was updated with a 1994 issue date, with the current reference being "ISO/IEC 7498-1:1994 ", and available from "http://www.iso.org".

The OSI Reference Model breaks the communication task into seven logical pieces as shown in Figure 6. All communication links have a data source (application layer 7 information) and a physical path (layer 1). Most links also have a data link layer (layer 2) to provide message integrity protection. Security can be applied at layers 1 or 2 if networking is not required but must be applied at or above the network layer (3) and is often applied at the application layer (layer 7) to allow packets to be routed through a network. More sophisticated, networkable, protocols add one or more of layers 3-6 to provide networking, session management, and sometimes data format conversion services. Note that the OSI Reference Model is not, in and of itself, a communication standard. It is just a useful *model* showing the functionality that might be included in a coordinated set of communication standards.

Also note that Figure 6 as drawn shows a superimposed "hourglass". The hourglass represents the fact that it is possible to transport the same

information over multiple physical layers – radio, fiber, twisted pair, etc – and that it is possible to use a multiplicity of application layers for different functions. In the middle – the networking – layers, interoperability over a common network can be achieved if all applications agree on common networking protocols. For example, the growing common use of the Internet protocols TCP/IP represents a worldwide agreement to use common networking practices (common middle layers) to route messages of multiple types (application layer) over multiple physical media (physical layer – twisted pair, Ethernet, fiber, radio) in order to achieve interoperability over a common network (the Internet).

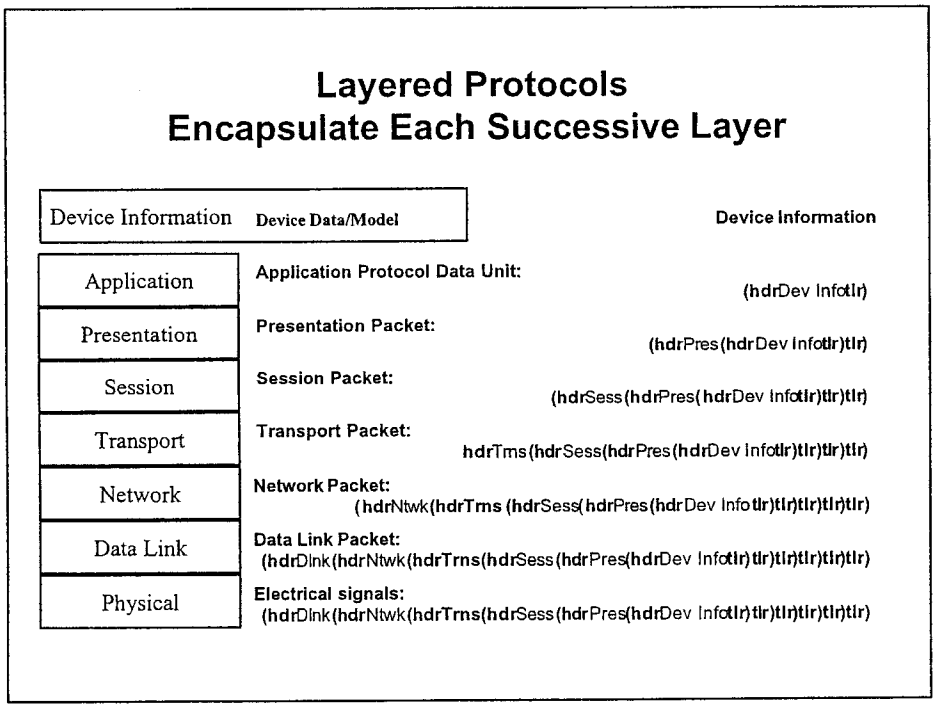


Figure 7: Layered Message Structure

Figure 7 shows how device information is encapsulated (starting at the top of the diagram) in each of the lower layers in order to finally form the data packet at the data link layer which is sent over the physical medium. The encapsulating packet – the header and trailer and each layer's payload – provide the added functionality at each level of the model, including routing information and message integrity protection. Typically the overhead requirements added by these wrappers are small compared with the size of the device information being transported. Figure 8 shows how a message can travel through multiple intermediate systems when networking protocols are used.

Traditional SCADA protocols, including all of the proprietary legacy protocols, DNP, and IEC 870-5-101, use layers 1, 2, and 7 of the reference model in order to minimize overheads imposed by the intermediate layers. IEC 870-5-104 and recent work being done with DNP add networking and transport information (layers 3 and 4) so that these

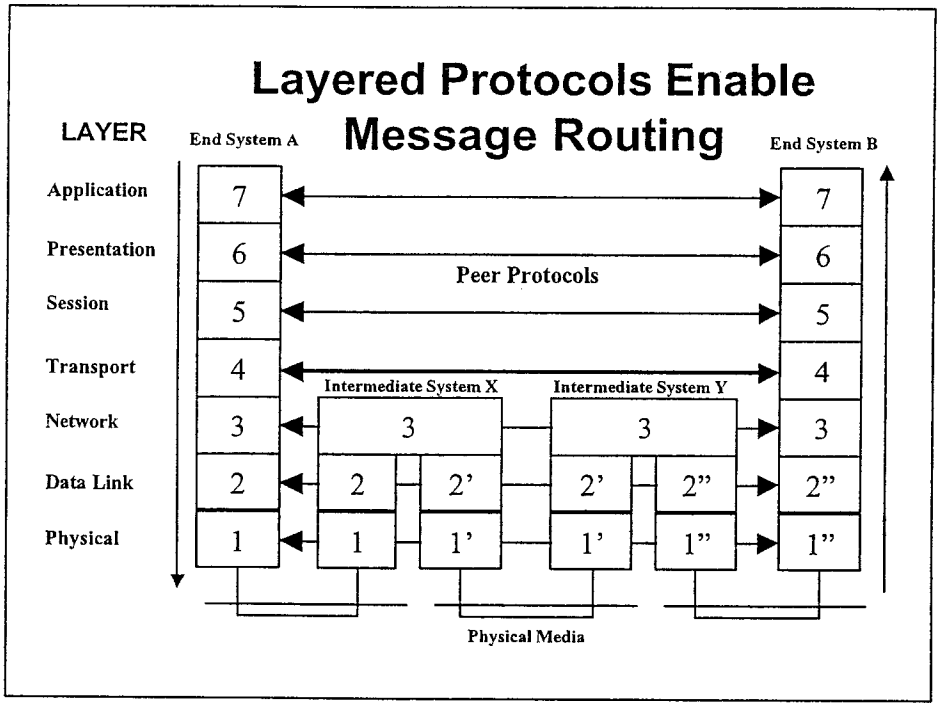


Figure 8: End-to-End Messaging in OSI Model

protocols can be routed over a wide-area network. IEC 61850 is built using a "profile" of other standards at each of the reference model layers so that it is applicable to a variety or physical media (lower layers), is routable (middle layers) and provides mature application layer services based on ISO 9506 – the Manufacturing Message Specification – MMS.

8. Security for Substation Communications

Until recently the term "security" when applied to SCADA communication systems meant only the process of ensuring message integrity in the face of electrical noise and other disturbances to the communications. But, in fact, "security" also has a much broader meaning. Security, in the broader sense, is concerned with anything which threatens to interfere with the integrity of the business. Our focus here will be to examine issues related more narrowly to SCADA security.

In an earlier section we discussed the role of the OSI Reference Model (ISO 7498-1) in defining a communications architecture. In similar fashion, ISO

7498-2, "Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture", issued in 1989, provides a general description of security services and related mechanisms which fit into the Reference Model and defines the positions within the Reference Model where they may be provided. It also provides useful standard definitions for security terms.

ISO 7498-2 defines the following five categories of security service:

- **Authentication**: The corroboration that an entity is the one claimed.
- **Access control**: The prevention of unauthorized use of a resource.
- **Data confidentiality**: The property that information is not made available or disclosed to unauthorized individuals, entities or processes.
- **Data integrity**: The property that data has not been altered or destroyed in an unauthorized manner.
- **Non-repudiation**: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the unit and protect against forgery, e.g., by the recipient.

Note that ISO 7498-2 provides standard definitions and an *architecture* for security services but leaves it to other standards to define the details of such services. It also provides recommendations on where the requisite security services should fit in the 7-layer Reference Model in order to achieve successful secure interoperability between open systems.

Security functions can generally be provided alternately at more than one layer of the OSI model. Communication channels which are strictly point-to-point and for which no externally visible device addresses need to be observable can employ encryption and other security techniques at the physical and data link layers. If the packets need to be routable, either messages need to be encrypted at or above the Network Layer (the OSI recommendation) or the security wrapper needs to be applied and removed at each node of the interconnected network. This is a bad idea because of the resultant complexities of security key management and the resultant probability of security leaks.

8.1 SCADA Security Attacks

A number of types of security challenges to which SCADA systems may be vulnerable are recognized in the industry. The list includes:

- **Authorization Violation**: An authorized user performing functions beyond his level of authority.
- **Eavesdropping**: Gleaning unauthorized information by listening to unprotected communications.
- **Information Leakage**: Authorized users sharing information with unauthorized parties.

- **Intercept/Alter**: An attacker inserting himself (either logically or physically) into a data connection and then intercepting and modifying messages for his own purposes.
- **Masquerade ("Spoofing")**: An intruder pretending to be an authorized entity and thereby gaining access to a system.
- **Replay**: An intruder recording a legitimate message and replaying it back at an inopportune time. An often-quoted example is recording the radio transmission used to activate public safety warning sirens during a test transmission and then replaying the message sometime later. An attack of this type does not require more than very rudimentary understanding of the communication protocol.
- **Denial of Service attack**: An intruder attacking a system by consuming a critical system resource such that legitimate users are never or infrequently serviced.

8.2 Security by Obscurity

The electric utility industry frequently believes that the multiplicity and obscurity of its SCADA communication protocols make them immune to malicious interference. While this argument may have some (small) merit, it is not considered a valid assumption when security is required. An often-quoted axiom states that "Security by Obscurity is No Security At All". In the same way that the operation of door locks is well understood but the particular key is kept private on a key ring, it is better to have well-documented and tested approaches to security in which there is broad understanding of the mechanisms but in which the keys themselves are kept private.

8.3 SCADA Message Data Integrity Checking

Early SCADA protocols based on telephone switching technology did not have message integrity checking built into the protocols. Incoming (status) information integrity was not considered mission-critical on a per-message basis, and errors would be corrected in the course of repeat transmissions. Control message integrity was provided by redundant messages and by select-check-operate sequences built into the operation.

Traditional packet-based SCADA protocols provide message integrity checking at the data link layer through the use of various check-sum or cyclic redundancy check (CRC) codes applied to each data packet. These codes can detect single- and many multiple-bit errors in the transmission of the data packet and are extremely useful for detecting errors caused by electrical noise and other transmission errors. The selection of the particular frame checking algorithm has been the subject of a great deal of study in the development of the several existing SCADA protocols. Usually the frame check sequence is applied once to the entire packet. In the case of IEC 870-5 and DNP, however, a CRC is applied to

both the header of a message and every sixteen octets within the message in order to ensure message integrity in the face of potentially noisy communication channels.

The OSI reference model prescribes data link integrity checking as a function to be provided by the link layer (Layer 2), so all protocols built on this model (eg, IEC 61850) will have CRC-based frame check sequences built into their lower layers, although they may not be optimized for performance in very noisy communication channels as is the case with the IEC 870-5 family of protocols.

Since the link layer integrity checks discussed above do not include encryption technology and they use well-documented algorithms, they provide protection only against inadvertent packet corruption caused by hardware or data channel failures. They do not provide, nor do they attempt to provide, encryption which can protect against malicious interference with data flow.

8.4 Encryption

Security techniques discussed in this section are effective against several of the attacks discussed above, including Eavesdropping, Intercept/Alter, and Masquerade ("Spoofing"). They can also be effective against Replay if they are designed with a key that changes based upon some independent entity such as packet sequence number or time.

The OSI Reference Model separates the function of *data link integrity* checking (checking for transmission errors) from the function of protecting against malicious attacks to the message contents. Protection from transmission errors is best done as close to the physical medium as possible (data link layer), while protection from message content alteration is best done as close to the application layer as possible (network layer or above). An example of this approach is the IP Security Protocol (ipsec), which is inserted at the IP level in the protocol stack of an Internet-type network.

For those instances where packet routing is not required, it is possible to combine error checking and encryption in the physical or data link layer. Commercial products are being built which intercept the data stream at the physical (or sometimes data link) layer, add encryption and/or error detection to the message, and send it to a matching unit at the other end of the physical connection, where it is unwrapped and passed to the end terminal equipment. This approach is particularly useful in those situations where it is required to add information security to existing legacy systems. If such devices are employed in a network where message addressing must be visible, they must be intelligent enough to encrypt only the message payload while keeping the address information in the clear.

For systems in which the packets must be routed through a wide-area network, the addition of a physical-layer device which does not recognize the packet structure is unusable and it is more appropriate to employ network-layer or above security protection to the message. This can be accomplished using either proprietary (eg, many Virtual Private Network schemes) or standards-based (eg, the IP Security Protocol - ipsec) which operate at the Network Layer or above in the OSI model.

8.5 Denial of Service

Denial of Service attacks are attacks in which an intruder consumes a critical system resource with the result that legitimate users are denied service. This can happen on a wide area network by flooding the network with packets or requests for service, on a telephone network by simultaneously going "off-hook" with a large number of telephone sets, or on a radio network by jamming the frequency used by radio modems. Defense against such attacks varies depending on the type of communication facility being protected.

Denial of Service is usually not an issue on networks that are physically isolated. The exception is defending against system failures which might arise under peak load conditions or when system components fail.

Defense against Denial of Service attacks in an interconnected wide area network is difficult and can only be accomplished using techniques such as packet traffic management and quality of service controls in routers. Denial of Service during normal system peak loading is a consideration that must be made when the system is designed.

Defense on a telephone system might include managing "quality of service" by giving preferential dial tone to "critical" users while denying peak-load service to "ordinary" users.

Defense on a radio system might include the use of Spread Spectrum techniques that are designed to be robust in the face of co-channel interference.

9. Electromagnetic Environment

The electromagnetic environment in which substation communication systems are asked to operate is very unfriendly to wired communication technologies. It is not unusual to expose communication circuits to several thousands of volts during system faults or switching as a result of electromagnetic induction between high voltage power apparatus and both internal and external (eg, telephone) communication facilities.

IEEE Standard 487-2000 states:

> Wire-line telecommunication facilities serving electric supply locations often require special high voltage protection against the effects of fault-produced ground potential rise or induced voltages, or both. Some of the telecommunication services are used for control and protective relaying purposes and may be called upon to perform critical operations at times of power system faults. This presents a major challenge in the design and protection of the telecommunication system because power system faults can result in the introduction of interfering voltages and currents into the telecommunication circuit at the very time when the circuit is most urgently required to perform its function. Even when critical services are not involved, special high-voltage protection may be required for both personnel safety and plant protection at times of power system faults. Effective protection of any wire-line telecommunication circuit requires coordinated protection on all circuits provided over the same telecommunication cable.

Tools that can be used to respond to this challenge include the use of isolation and neutralizing transformers for metallic telephone circuits, protection (and qualification testing) of connections to communication apparatus, and proper shielding and grounding of wired circuits.

The use of fiber optic communication systems for both local networking (eg, fiber Ethernet) and for telecommunication circuits is a valuable tool for use in hazardous electromagnetic environments.

IEEE and IEC standards which have been issued to deal with electromagnetic interference issues include the following (www.standards.ieee.org) :

- IEC Technical Committee No. 65: Industrial-Process Measurement and Control, Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment, Part 3: Radiated.
- IEEE Std C37.90-1994 Standard for Relays and Relay Systems Associated with Electric Power Apparatus.
- IEEE Std C37.90.1-2002 Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems.
- IEEE Std C37.90.2-2001 Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers.
- IEEE Std C37.90.3-2001 Electrostatic Discharge Tests for Protective Relays.
- IEEE Std 487-2000 IEEE Recommended Practice for the Protection of Wire-Line Communication Facilities Serving Electric Supply Locations
- IEEE Std 1613 Environmental Requirements for Communications Networking Devices Installed in Electric Power Substations

10. For more information

As discussed above, a number of standards organizations have produced standards which can be used as guidelines when designing substation communication systems, and there are Internet resources which can be studied for further information. References to some of these standards and web sites are provided below to help with finding more detailed information.

10.1 Useful Web Sites:

American National Standards Institute (ANSI): www.ansi.org
Institute of Electrical and Electronics Engineers (IEEE): www.ieee.org
International Electrotechnical Commission (IEC): www.iec.ch
Internet Engineering Task Force (IETF): www.ietf.org
International Standards Organization (ISO): www.iso.ch
National Institute of Standards and Technology (NIST): www.nist.gov
International Telecommunications Union (ITU): www.itu.int
DNP User's Group: www.dnp.org
UCA User's Group: www.ucausersgroup.org
Information on Systems Engineering: http://www.bredemeyer.com
Publicly available ISO Standards: http://www.acm.org/sigcomm/standards/

10.2 Relevant Standards:

10.2.1. IEEE 802.x Networking Standards

IEEE 802.x standards are available from www.standards.ieee.org.
802 standards are currently available in electronic form at no cost six months after publication.

10.2.2. IEEE Electromagnetic Interference standards (www.standards.ieee.org):

IEEE Std C37.90-1994 Standard for Relays and Relay Systems Associated with Electric Power Apparatus.

IEEE Std C37.90.1-2002 Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems.

IEEE Std C37.90.2-2001 Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers.

IEEE Std C37.90.3-2001 Electrostatic Discharge Tests for Protective Relays.

IEEE Std 487-2000 IEEE Recommended Practice for the Protection of Wire-Line Communication Facilities Serving Electric Supply Locations

IEEE Std 1613 Environmental Requirements for Communications Networking Devices Installed in Electric Power Substations

10.2.3. IEC 870-5 Standards (available from www.iec.ch):

IEC 60870-1-1 TR0 Ed. 1.0
Telecontrol equipment and systems. Part 1: General considerations. Section One: General principles

IEC 60870-1-2 Ed. 1.0
Telecontrol equipment and systems. Part 1: General considerations. Section Two: Guide for specifications

IEC 60870-1-3 TR3 Ed. 2.0
Telecontrol equipment and systems - Part 1: General considerations - Section 3: Glossary

IEC 60870-1-4 TR3 Ed. 1.0
Telecontrol equipment and systems - Part 1: General considerations - Section 4: Basic aspects of telecontrol data transmission and organization of standards IEC 870-5 and IEC 870-6

IEC 60870-1-5 TR Ed. 1.0
Telecontrol equipment and systems - Part 1-5: General considerations - Influence of modem transmission procedures with scramblers on the data integrity of transmission systems using the protocol IEC 60870-5

IEC 60870-2-1 Ed. 2.0
Telecontrol equipment and systems - Part 2: Operating conditions - Section 1: Power supply and electromagnetic compatibility

IEC 60870-2-2 Ed. 1.0
Telecontrol equipment and systems - Part 2: Operating conditions - Section 2: Environmental conditions (climatic, mechanical and other non-electrical influences)

IEC 60870-3 Ed. 1.0
Telecontrol equipment and systems. Part 3: Interfaces (electrical characteristics)

IEC 60870-4 Ed. 1.0
Telecontrol equipment and systems. Part 4: Performance requirements

IEC 60870-5-1 Ed. 1.0
Telecontrol equipment and systems. Part 5: Transmission protocols - Section One: Transmission frame formats

IEC 60870-5-2 Ed. 1.0
Telecontrol equipment and systems - Part 5: Transmission protocols - Section 2: Link transmission procedures

IEC 60870-5-3 Ed. 1.0
Telecontrol equipment and systems - Part 5: Transmission protocols - Section 3: General structure of application data

IEC 60870-5-4 Ed. 1.0
Telecontrol equipment and systems - Part 5: Transmission protocols - Section 4: Definition and coding of application information elements

IEC 60870-5-5 Ed. 1.0
Telecontrol equipment and systems - Part 5: Transmission protocols - Section 5: Basic application functions

IEC 60870-5-101 Ed. 1.0
Telecontrol equipment and systems - Part 5: Transmission protocols - Section 101: Companion standard for basic telecontrol tasks

IEC 60870-5-101 Amd.1 Ed. 1.0
Amendment 1

IEC 60870-5-101 Amd.2 Ed. 1.0
Amendment 2

IEC 60870-5-102 Ed. 1.0
Telecontrol equipment and systems - Part 5: Transmission protocols - Section 102: Companion standard for the transmission of integrated totals in electric power systems

IEC 60870-5-103 Ed. 1.0
Telecontrol equipment and systems - Part 5-103: Transmission protocols - Companion standard for the informative interface of protection equipment

IEC 60870-5-104 Ed. 1.0
Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles

10.2.4. DNP3 Specifications

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

DNP 3.0 specifications, available from www.dnp.org. Available on-line: "A DNP3 Protocol Primer" Specifications in four documents available to Users Group members: DNP V3.00 Data Link Layer Protocol Description; DNP V3:00 Transport Functions; DNP V3.00 Application Layer Protocol Description; DNP V3:00 Data Object Library

10.2.5. IEC 870-6 TASE.2 (UCA / ICCP)Standards (available from www.iec.ch)

IEC 60870-6-1 TR3 Ed. 1.0
Telecontrol equipment and systems - Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - Section 1: Application context and organization of standards

IEC 60870-6-2 Ed. 1.0
Telecontrol equipment and systems - Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - Section 2: Use of basic standards (OSI layers 1-4)

IEC 60870-6-503 Ed. 2.0
Telecontrol equipment and systems - Part 6-503: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE.2 Services and protocol

IEC 60870-6-505 TR Ed. 1.0
Telecontrol equipment and systems - Part 6-505: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE.2 User guide

IEC 60870-6-601 Ed. 1.0
Telecontrol equipment and systems - Part 6: Telecontrol protocol s compatible with ISO standards and ITU-T recommendations - Section 601: Functional profile for providing the connection-oriented transport service in an end system connected via permanent access to a packet switched data network

IEC 60870-6-602 TS Ed. 1.0
Telecontrol equipment and systems - Part 6-602: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE transport profiles

IEC 60870-6-702 Ed. 1.0
Telecontrol equipment and systems - Part 6-702: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - Functional profile for providing the TASE.2 application service in end systems

IEC 60870-6-802 Ed. 2.0
Telecontrol equipment and systems - Part 6-802: Telecontrol protocols compatible with ISO standards and ITU-T recommendations
- TASE.2 Object models

10.2.6. IEC 61850 / UCA Standards (available from www.iec.ch)

IEEE TR 1550-1999 EPRI/UCA Utility Communications Architecture (UCA) Version 2.0 1999 , IEEE Product No: SS1117-TBR IEEE Standard No: TR 1550-1999

IEC 61850-1 (to be published)
Communication networks and systems in substations - Part 1: Introduction and overview

IEC 61850-2 (to be published)
Communication networks and systems in substations - Part 2: Glossary

IEC 61850-3 Ed. 1.0
Communication networks and systems in substations - Part 3: General requirements

IEC 61850-4 Ed. 1.0
Communication networks and systems in substations - Part 4: System and project management

IEC 61850-5 (to be published)
Communication networks and systems in substations - Part 5: Communication requirements

IEC 61850-6 (to be published)
Communication networks and systems in substations - Part 6: Configuration description language for substation IEDs

IEC 61850-7-1 (to be published)
Communication networks and systems in substations - Part 7-1: Basic communication structure for substation and feeder equipment - Principles and models

IEC 61850-7-3 (to be published)
Communication networks and systems in substations - Part 7-2: Basic communication structure for suubstation and feeder equipment - Abstract communication service interface

IEC 61850-7-4 (to be published)
Communication networks and systems in substations - Part 7-2: Basic communication structure for suubstation and feeder equipment - Abstract communication service interface

IEC 61850-8-1 (to be published)
Communication networks and systems in substations - Part 8: SCSM - Mapping to MMS (ISO/IEC 9506 Part 1 and Part 2) and ISO/IEC 8802-3

IEC 61850-9-1 (to be published)
Communication networks and systems in substations - Part 9-1: SCSM - Specific Communication Service Mapping (SCSM) - Sampled values over serial unidirectional multidrop point to point link

IEC 61850-9-2 (to be published)
Communication networks and systems in substations - Part 9-2: SCSM - Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3

IEC 61850-10 (to be published)
Communication networks and systems in substations - Part 10: Conformance testing

10.2.7. ISO Reference Models (available from www.iso.ch)

ISO/IEC 7498-1:1994 2nd Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model

ISO/IEC 7498 Security Architecture, part 2 (superceded by ISO/IEC 10745 and ITU-T X.803 "Upper Layers Security Model", ISO/IEC 13594 and ITU-T X.802 "Lower Layers Security Model", and ISO/IEC 10181-1 and ITU-T X.810 "Security Frameworks, Part 1: Overview")

ISO/IEC 7498-3:1997 2nd Information technology -- Open Systems Interconnection -- Basic Reference Model: Naming and addressing

ISO/IEC 7498-4:1989 1st Information processing systems – Open Systems Interconnection -- Basic Reference Model -- Part 4: Management framework

Design and Implementation Of a UCA based Substation Control System

Mark Adamiak, Senior Member, IEEE
GE Power Management
King of Prussia, PA, USA
Email: mark.adamiak@indsys.ge.com

Ashish Kulshrestha, Member, IEEE
Powertec (A Member of KVB-Enertec Group)
Hatfield, PA, USA
Email: ashish@kvb-enertec.com

ABSTRACT: With the maturing of the Utility Communication Architecture (UCA) and standardization through IEC 61850, utilities and industrials are beginning to implement protection and control systems that are based on this technology. This paper describes such an implementation for the control of the Bateias 525kV substation on the COPEL power system in Brazil. In particular, the paper will describe the customer's requirements and expectations with regard to the information flow, control sequences, automation functions, and reliability. The design of the substation automation architecture to meet these customer requirements will be presented including the communication network structure, and redundancy software. Also to be discussed will be the installation issues encountered and system performance levels achieved.

In addition to the above, the paper will include a brief tutorial on UCA/IEC 61850

KEYWORDS: UCA2.0, CASM, Substation Architecture, High Availability, Redundancy, SCADA, GOOSE, GOMSFE, IEC-61850, ECS, GSSE

I. NEEDS OF COPEL

Bateias substation is an important high Voltage transmission substation for COPEL. There are four voltage levels in the substation: 525 kV, 239 kV, 138 kV and 13.8 kV. The major needs for the automation system as outlined by the customer were as follows:

Collection of Information: COPEL needed to collect analog and digital information from the equipment in the substation. This was to facilitate local operations by providing the consolidated metering values, alarm and status information. A substation level sequence of event recorder was required to monitor various events up to millisecond accuracy.

Control and Monitoring: A need for substation level control and monitoring was specified. COPEL wanted a defined control hierarchy to be implemented between the three Energy Control Stations (ECS), local substation and IEDs. Monitoring for various alarm conditions, demand reports, energy reports were also specified. The ECS specified required three different SCADA communication protocols, hence, a protocol translator was required to communicate to the various ECS systems

High Availability / Redundancy: A requirement for "no single point of failure" was specified to provide high availability of the system. This required a redundant architecture for the system. Two independent communication systems and substation control computers were subsequently supplied. In the event of failure of one

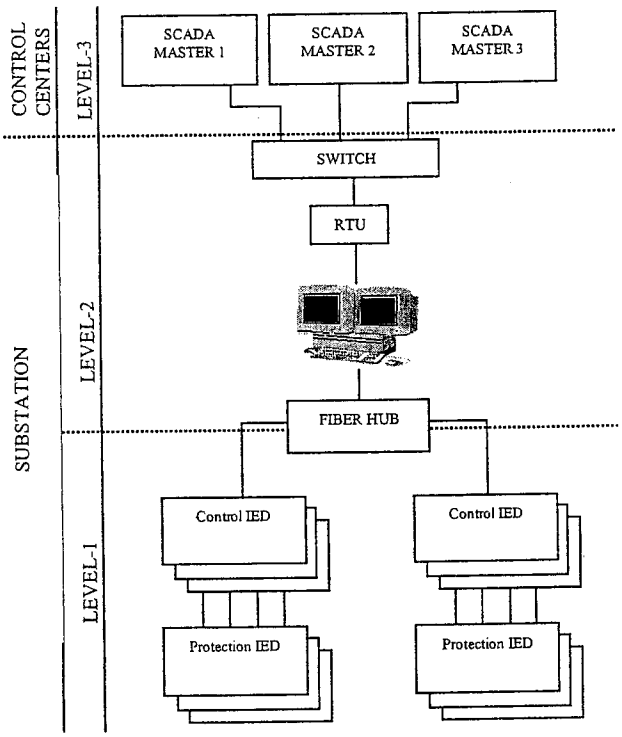


FIG. 1. AUTOMATION SYSTEM OVERVIEW

communication network or computer, the other component was required to perform the tasks needed for the automation system.

Automation Functions: COPEL specified a detailed interlocking schema for control of the substation. The control scheme required a bay controller type of application to be implemented. I/Os from the various field equipment were involved in the logic decision for the control operations. An automated control model was specified by COPEL for all the breakers and switches in the substation. Transformer thermal curve calculation was required as part of the automation functions. Features like check for mutual exclusivity between various binary contacts and Select Before Operate (SBO) for controls were also among the needs defined by the customer.

Capability for Future Expansion: Two bays were identified as future bays in the system. A requirement for a modular and extensible architecture was specified.

Fig. 1 describes the system overview for the Bateias substation.

II. INTRODUCTION OF UCA 2.0 / IEC-61850

Electric Power Research Institute (EPRI) launched a concept in 1990 known as the Utility Communication Architecture or UCA. The goal behind UCA was to identify a suite of existing communication protocols that could be easily mixed and matched, provide the foundation for the functionality required to solve the utility enterprise communication issues, and be extensible for the future. UCA provides a "network" solution to the interconnection of data sources – similar to the Internet used throughout the world to interconnect computers.

At this time, the next generation of Intelligent Electronic Devices (IEDs) based on UCA are available with IEC version availability early 2004. These devices are focused on networking in the substation and are based on the Manufacturing Messaging Specification (MMS) / Ethernet profile with one of two "networking" layers in-between (see figure 2).

<table>
<tr><td colspan="2">Equipment Data Models – IEC Part 7.3 & 7.4
In UCA: Generic Object Models for Substation and Field Equipment (GOMSFE)</td></tr>
<tr><td colspan="2">Abstract Communication Service Interface (ACSI) / IEC 7.2</td></tr>
<tr><td colspan="2">Manufacturing Messaging Specification (MMS)</td></tr>
<tr><td>International Standards Organization (ISO) Networking Layers</td><td>TCP/IP Network Layers</td></tr>
<tr><td colspan="2">10/100/1000 MB Ethernet
Twisted Pair / Redundant Fiber</td></tr>
</table>

FIG. 2. UCA2 – SUBSTATION COMMUNICATION PROFILE

Ethernet: Ethernet was chosen as the Physical / Data Link layer 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, the scalability of Ethernet is well defined with 100Mb implementations becoming the standard, 1Gb gaining acceptance, and 10Gb Ethernet well on its way into hardware. Processors are available today with multiple 10/100 Mb Ethernet ports integrated into the chip.

A concern was raised early on as to the reliability of the "on time" message delivery capability of Ethernet due to the Carrier Sense Multiple Access (CSMA) nature of Ethernet. When two or more IEDs desire access to the Local Area Network (LAN) through a shared hub, a data collision may occur is the messages are sent simultaneously. When this happens, all colliding devices set a random delay time and try again, after the delay, to get access to the bus. There is a probability that subsequent collisions may occur which could delay critical messages from being delivered in a timely manner. For the substation environment, "timely" was defined to be 4ms in order to perform functions such as, tripping over the LAN.

To quantitatively address this concern, a study was undertaken by EPRI where the performance of Ethernet was evaluated under a "worst case" scenario in comparison to a 12 MB Token Passing Profibus network. Results of this study [1] showed that either 100Mb Ethernet on a shared hub or 10Mb Ethernet connected via a switched hub could meet the 4ms network communication time - both of which were faster than the token bus solution operating at 12Mb.

TCP/IP, OSI Network Layers: As it was deemed desirable to be able 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 OSI transport & networking layers.

TCP/IP stands for Transmission Control Protocol / Internet Protocol which are the ubiquitous transport/network layer used over the Internet. Its inclusion in the profile is due to its omnipresence and overall acceptance in the marketplace. TCP/IP is a streaming protocol which means that transmission of a packet of data waits for either a "stream" of data (such as that from a teletype terminal) to fill a buffer or a time-out before the buffer is transmitted. 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 transport/network layer included is the ISO-OSI network layers. ISO is the International Standards Organization that 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" of multicasting" 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 control messages to multiple devices.

ASCI: Abstract Communication Service Interface – defines the "base" service definitions required to operate a substation/enterprise communication system. These include device connection, data definition, data & file handling, real-time control messaging, event reporting, file handling, etc. The abstract nature of the services allow the mapping of the service to multiple different application protocols. In UCA/IEC, the actual protocol layer of MMS was used.

MMS: MMS is an ISO defined (ISO 9506) protocol that provides implementable application services. MMS provides services such as read, write, get file, get list of files, etc. and clearly defines how the bits go onto the wire. It supports object oriented data definitions, which makes self-description a reality. Support for unsolicited data reports and file transfers are also offered by MMS.

The ability to perform exception reporting is also defined in the ACSI. Exception reporting is the concept of only sending data items when one of them has changed. This is a major paradigm shift from traditional SCADA that has to constantly poll the source to detect changes in data.

Data Models: UCA/IEC define standard data models for equipment and functions found in the substation. By defining and using common objects, UCA/IEC provides intra-operability between different devices and user interfaces. IEC 61850 provides guidelines on how to model an IED and it also defines, in detail, the protection setting objects and a special device to multiple device communication object model known as the Generic Object Oriented Substation Event or "GOOSE".

The data models use the basic data types like Integer, Float, String etc. to define more complex data models specific for the application. For example, a data measurement on a three phase system (WYE class) may have up to ten data members {PhsAi, PhsAf, PhsBi, PhsBf, PhsCi, PhsCf, Neuti, Neutf, q, t} where PhsAi represent the phase "A" value in 32 bit signed integer format, PhsAf, represent phase "A" value in 32 bit float and so on. The data items are aggregated in what are termed Logical Nodes (LN). See Fig. 3 for an example of a the ploy phase measurement LN - MMXU.

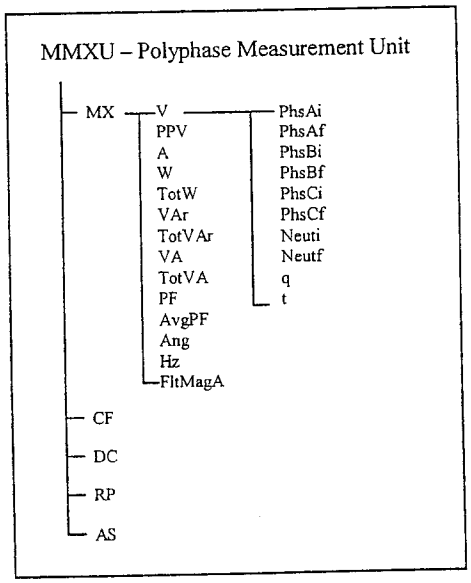


FIG. 3. Measurement Logical Node

The IEC 61850 standard presently defines 91 different Logical Nodes and several new proposals are under consideration. Any one product will be composed of any combination of LN as required to meet the product's functionality. A special reporting model in UCA is GOOSE which allows the IEDs to communicate binary information amongst themselves using an MMS based publisher and subscriber mechanism. The IEC GOOSE is more generic whereby the user can define a dataset that is to be transmitted where the dataset can include any defined object in the device. Only the UCA GOOSE was used in Bateias.

The IEDs subscribing to the GOOSE reports from remote peers can use the information to perform any logic or control associated with the GOOSE bit pairs. Fig. 4 illustrates the GOOSE operation model.

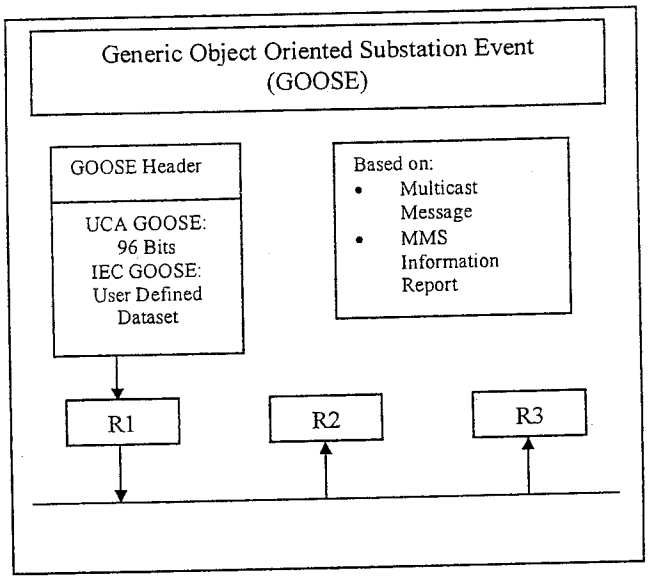


FIG. 4. UCA2 – GOMSFE – GOOSE APPLICATION

The following features of UCA made it a simple choice for COPEL's Bateias substation system:

1. High performance based on 10Base-F network with ease for future upgrade to 100Base-F
2. Simultaneous dual accesses to IEDs for real time data transfers and controls. UCA IEDs support multiple concurrent connections eliminating duplicate wiring for communication. Each computer makes a separate connection to the IEDs, thus providing built-in redundancy for communications.
3. Standard application definitions for network and protocol independence
4. GOMSFE / GOOSE definitions for interoperability between the current selection of IEDs. In the future, the current IEDs can be replaced with only a few changes to client applications in the substation computers
5. Elimination of wiring between IEDs by maximizing the use of GOOSE for the transfer of status and control information
6. Low cost for Application development, as there is high re-usability in terms of configuration and scripting for the HMI tools.

III. SUBSTATION ARCHITECTURE

The system architecture for Bateias (shown in Fig. 1) is divided into three levels. Level-1 involves IEDs connected to process equipment in the substation. The IEDs are classified as either protection or control IEDs. Protection IEDs provide all the status information to the control IEDs that in turn implement the control logic for the substation operation. The protection IEDs do not directly communicate to the higher levels in the architecture. The control IEDs act as UCA servers and allow multiple UCA clients to make

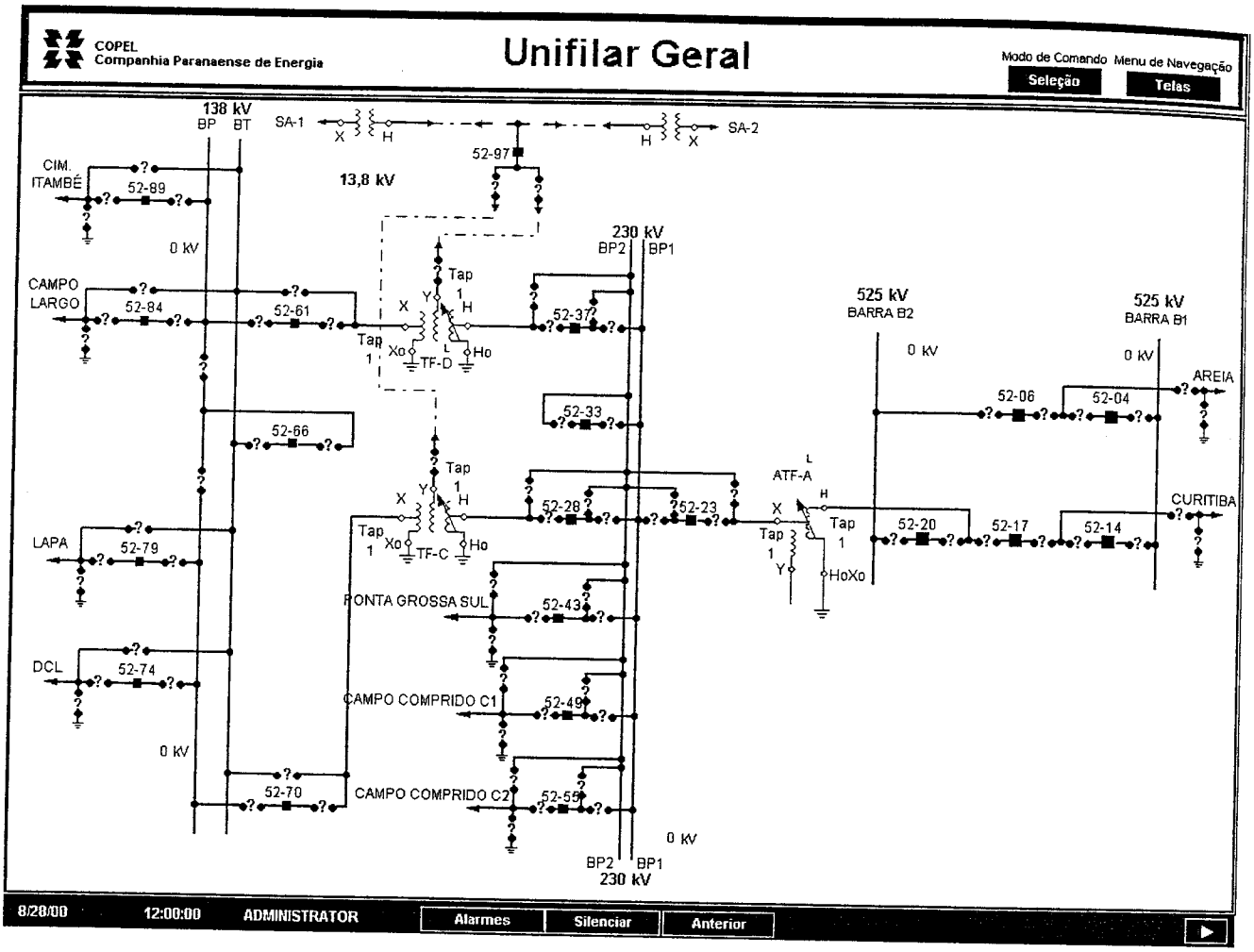


FIG. 5. BATEIAS SUBSTATION ONELINE DIAGRAM

simultaneous connections to it. Control IEDs also send and receive GOOSE messages to each other using the substation fiber LAN. There are 42 control IEDs in this substation. Each control IED provides redundant 10BaseFl - ST type connections to itself. The fiber cables from the IEDs are connected to two layers of switched HUBs.

The HUBs are smart enough to recognize and break loops of messages. They run spanning tree algorithm using SNMP (Simple Network Management Protocol) to ensure a path to the device and to realize and break duplicate paths to the device.

Level-2 consists of the two substation computers with dual monitor displays. Each computer system runs its own UCA client to connect in real time to all 42 UCA IEDs. TCP/IP is used as the choice for the network protocol to run MMS requests between the UCA clients and servers. Fig 6 shows the software architecture used inside the computers. For simplicity sake, only important software components are displayed. Both computer systems run asynchronous to each other. A user can perform all monitoring and control operations from either computer at any given instance of time. Special redundancy software in each computer monitors the tasks in each computer to determine failures.

It also maintains the latest configuration using database replication between the two computers.

Level-2 also emulates RTU (Remote Terminal Unit) functionality for three remote ECS locations using three different SCADA master protocols, namely: DNP3.0, Microplex 5000 and Conitel. Since both host computers share the same data and can run the SCADA emulation software, a cross-over network was designed that allows the SCADA emulation to be provided by either host computer. Mapping tools were developed to map UCA data onto the various ECS protocols.

Level-3 refers to the Energy Control Systems of the utility. As mentioned, Bateias interfaces with three ECS systems named COE, SE and Electrosul.

IV. PERFORMANCE

The substation system offers high performance for data updates and controls when compared to traditional non-UCA system. A typical data update rate for a brick of data like MMXU (Measurement Unit) takes 20 to 30 milliseconds. The following performance figures are achieved for the various IEDs:

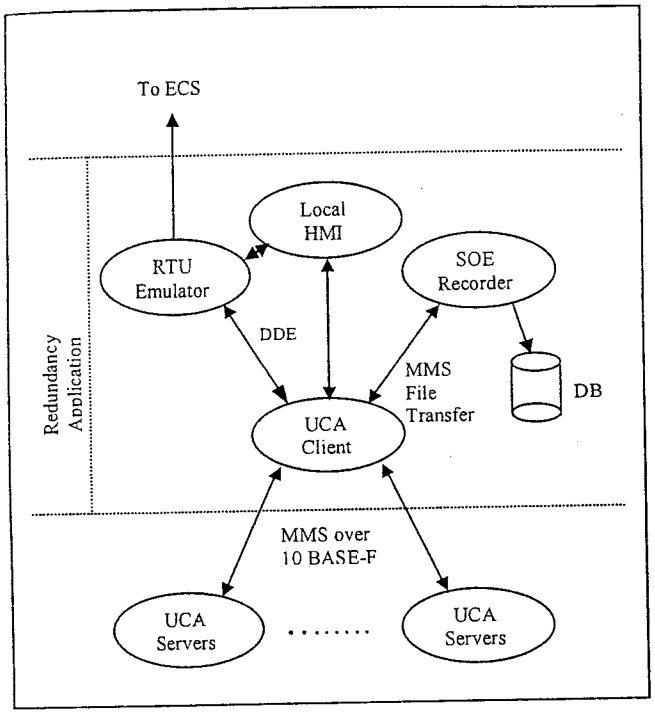


FIG. 6. BATEIAS LEVEL-2 SOFTWARE ARCHITECTURE

- Data Update rate at the HMI - under 1 second
- Site Event recorder update - under 2 seconds (when 10 events are generated every second at the IEDs)
- Site Event recorder update - under 3 seconds (when 100 events are generated every second at the IEDs)
- Control execution - less than 1 second.
- During commissioning, 14 million GOOSE messages were recorded during one 18 hour period. The system ran flawlessly during the GOOSE flood.

V. INSTALLATION ISSUES

While performing the system integration for the Bateias substation, some installation issues were encountered and addressed. Since a relatively newer technology was used, a number of firmware and software revisions were required before an acceptable performance level was achieved. From our installation experience, there are a number of areas that we feel that could be addressed to facilitate the integration of UCA based systems:

- A smart IED settings program is required to cross check the GOOSE settings between various IEDs in the system. IEDs now subscribe many remote IED GOOSE messages. Since a unique user bit pair is mapped from a remote IED, changing that bit pair combination requires all subscribers to be notified. This may be an easy task with few IEDs but with 42 IEDs it wasn't so simple.
- A GOOSE Monitor / Historian program is required to facilitate the debugging of the distributed logic that one can now create. Specifically, the ability to trigger a GOOSE capture based on logical expressions of GOOSE bits would be very useful. In general, a GOOSE historian to monitor traffic and other performance features is desirable.
- UCA has become the IEC-61850 standard. All object definition are now codified in sections 7.3 and 7.4 of the IEC 61850 standard. The IEC standard provides for backward compatibility at the client level in as much as an IEC client is required to be able to read UCA device definitions. The IEC object models are basically backward compatible with the UCA objects with the primary difference being an change in the time field to accommodate greater time accuracy.

VI. BENEFITS

In implementing the Bateias integration system, a number of benefits were identified as a result of using the UCA substation network approach:

- Lower cost of Engineering as drawings were simplified
- Lower cost of installation as less wiring was needed
- Standard object models for data names and Self describing feature of the UCA reduced the time to map data to the HMI
- Lower cost of commissioning, as most of the operation errors could be correct via logic re-configuration. Minimal re-wiring was required.
- Modular HMI screens design gave high re-usability of screens and set the stage for future expansion and upgrades
- Data values were reported directly in engineering values so no scaling was required
- The choice of standard Ethernet for the substation LAN allowed the use of off the shelf hubs, Network Interface Cards (NICs), and other communication equipment and tools
- All fibers based Ethernet network basically eliminated the effects of electrical noise on communications.
- Twist in and out connectors meant no communication wiring screws to undo

Although not required on this job, the use of standard UCA communications would have facilitated the integration of other manufacturer's equipment into the system.

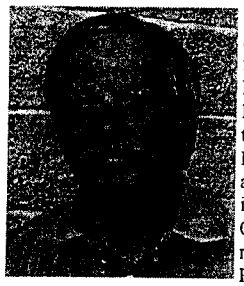
VII. SUMMARY

This paper documents the design of a substation integration system from functional specification to system design to implementation and commissioning. A system solution based on UCA was presented and the benefits (including performance) were identified.

VIII. REFERENCES

1. UCA2.0 Standard Document. Part 1; Electric Power Research Institute (EPRI); Palo Alto, CA.
2. Common Application Service Models (CASM); ftp.sisconet.com/EPRI/UCA2.0/CASM97.zip
3. General Object Models For Substation and Feeder Equipment (GOMSFE .91); ftp.sisconet.com/EPRI/UCA2.0/GOMSFE91.zip

IX. BIOGRAPHIES



Mark Adamiak received his Bachelor of Science and Master of Engineering degrees from Cornell University in Electrical Engineering and an MS-EE degree from the Polytechnic Institute of New York. From 1976 through 1990, Mark worked for American Electric Power (AEP) in the System Protection and Control section where his assignments included R&D in Digital Protection and Control, relay and fault analysis, and system responsibility for Power Line Carrier and Fault Recorders.

In 1990, Mark joined General Electric where his activities have spanned development, product planning, and system integration. Mr. Adamiak has been actively involved in developing the framework for the implementation of the MMS/Ethernet communication solutions and is presently the Principle Investigator on the Integrated Energy and Communication System Architecture (IECSA) project which is tasked with extending the communication architecture from the energy traders desk to home automation and control systems. Mark is a Senior Member of IEEE, past Chairman of the IEEE Relay Communication Sub Committee, a US member of IEC TC57, and a registered Professional Engineer in the State of Ohio.

Ashish Kulshrestha received his Bachelor of Engineering degree from S.G.S. Institute of Technology and Science (Indore, India) in Electronics & Instrumentation Engineering. From 1993 to 1998, Ashish worked at CMC Limited (a leading company in India to provide systems services and consulting). His assignments included working on various Information Technology projects involving high availability and redundancy for financial systems.

Since 1995, Ashish was involved in the system integration of Power Substation Systems (while consulting at General Electric). In 1998, Ashish joined KVB-Enertec where his activities have ranged from development, product planning, and system integration. He is presently Manager of Products and Software for Power Systems. Ashish was the primary project engineer for the COPEL Bateias system.

X. Addendum

GOOSE vs. GSSE

The IEC 61850 document redefines the meanings of GOOSE as compared with the original UCA documents. In UCA, the Generic Object Oriented Substation Event only defined binary event information. There was no mechanism to multicast other values such as analog measurements to other devices.

In IEC 61850, the scope of GOOSE changed to the multicast of a "user defined" dataset. The dataset could include any object that was defined inside the device as long as the total length of the dataset and associated protocol information fit into one Ethernet frame. For this "user defined" concept to work, the "subscriber" must configure a reception dataset that is identical to the "published" dataset.

Backward compatibility with the binary state UCA GOOSE was maintained but the name was been changed to: Generic Substation Status Event – GSSE. Inclusion of the GSSE function is a vendor option.

Virtual Wire Check

As identified in the "Issues" section of this paper, verification of the GOOSE connections was troublesome. As a result of this experience, IEC 61850 has included new GOOSE services that aid in the automatic determination of proper connection between a publisher and a subscriber. On startup, the subscriber issues a "get reference name" request to the publisher based on an offset into the dataset. The publisher returns the Data Label for the requested dataset item. If the returned Data Label matches the programmed label, a "Valid" virtual wire check is issues. If not, a configuration alarm is issued.

Practical Considerations in Application of UCA GOOSE

Mark Adamiak Drew Baigent
GE Power Management
King of Prussia, PA Markham, Ontario

Scott Evans
GE Corporate Research and Development
Schenectady, NY

Introduction

The power and functionality of next generation microprocessors has led the way to next generation digital relays. One particular characteristic of these new processors is the tight integration of the processor with a high-performance communication controller. Given this new communication capability, an international effort has ensued to create a single communication protocol that advantages the capabilities of these new processors. That effort has centered around the Electric Power Research Institute's Utility Communication Architecture or UCA including a definition for the relay to relay communication of binary state data known as the GOOSE.

Development of UCA

The Utility Communication Architecture or UCA had its origins in 1990 as the framework for the ensemble of communication requirements that exist in the utility enterprise. It was at this time that utility managers were looking to consolidate communications among their planning, SCADA, metering, protection, and control departments. In attempting this consolidation, the cost of integration of diverse communication protocols was realized and a drive towards communication commonality was begun.

Since 1993, there has been a focus on the application of UCA in the substation. The process started with the creation of a requirements document that defined the communication requirements for the various functions inside a substation. The functional requirements document was followed by an implementation and evaluation phase that defined the "profile" of a communication structure for the substation. The profile that has been defined is shown generically in figure 1.

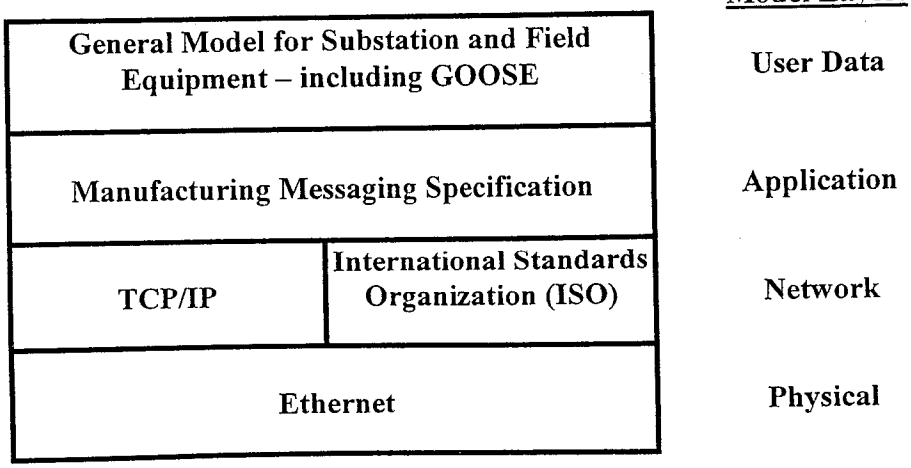


Figure 1
UCA Substation Profile

The goal in defining the "next generation" substation profile was to implement a high speed, networkable, peer to peer architecture using as many "existing" communications protocols as possible. In addition, the goal of user data interoperability required the definition of standard names for commonly used data objects.

The profile developed uses Ethernet for the Physical and Data Link layers. Although Ethernet is "non-deterministic" when operated in a "shared access" mode of operation (due to collisions), Ethernet technology has advanced to provide "switched" access which minimizes collisions. In addition, Ethernet provides a growth path to higher-speed Ethernet networks such as 100 MB and 1GB with 10 GB already defined.

For the "networking" layers, although the original goal was to stay within the realms of the International Standards Organization (ISO) standards, the popularity of the Internet dictated the inclusion of the TCP/IP networking layers. In November of 1999, the International Electrotechnical Committee (IEC) selected TCP/IP as the "mandatory" networking protocol for intra and inter substation communications and the ISO networking layers as optional. The inclusion of these networking layers makes data from the substation available over a utility intranet, WAN, or even the Internet.

For the Application or service layer, the Manufacturing Messaging Specification (MMS) was chosen. MMS provides a rich set of services to read, write, define, and create data objects. It is MMS and its ability to manipulate logical objects that differentiates this profile from all other existing profiles.

Lastly, the UCA substation profile defines standard "object models" for commonly used data elements. These standard models are defined in the document entitled: General Object Models for Substation and Field Equipment (GOMSFE). This standardization facilitates interoperability as any manufacturer who, for example, allows "Phase A - Gnd Voltage" to be externally visible, does so in a common manner.

Evolution of the GOOSE

One of the unique functional requirements identified for UCA was high-speed (goal of 4ms) device to *multi*-device communications of simple binary state information. Inasmuch as sending multiple messages to multiple devices would incur an unacceptable time delay, an implementation was chosen that could send the same message to multiple devices simultaneously in a communication mode known as "multicast" (see Figure 2). The implementation of this function was done through the MMS information report service. The information report was used to deliver a binary object model (a collection of binary states of the device), known as the **G**eneric **O**bject **O**riented **S**ubstation **E**vent or **GOOSE**.

GOOSE works in a model type known as "Publisher / Subscriber". In this model, the sending device "publishes" the user-selected state bits in the device. Any device interested in any of the states of the publishing relay is programmed to "subscribe" to the publishing device's GOOSE message.

The GOOSE message is launched under one of two scenarios. The first scenario launches a GOOSE on a change of state of any of the binary variables in the message. The second scenario launches a GOOSE message on a user-selectable periodic basis. The reason for the latter scenario is that in absence of a state change, there is no way for the subscribing device to determine that the publisher is alive. When the subscribing device fails to receive an expected GOOSE message, it can declare the publisher as "dead" and set default states on the binary variables expected from the publisher.

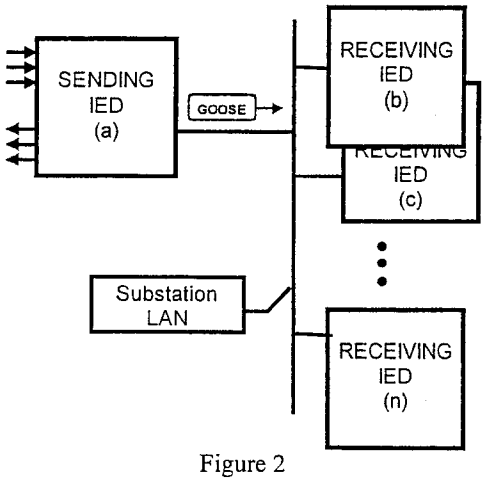


Figure 2
GOOSE Multicast Concept

One risk in the multi-cast GOOSE is the potential lack of assured and timely message arrival and processing due to "Best Effort" protocol quality of service (QOS) and the variable communications latency associated with a shared medium network. Coexistence of mission critical control signals with non-mission critical data causes variation in the QOS for the mission critical data that must be managed carefully. UCA GOOSE achieves reliability through the use of repeated unacknowledged messages. This paradigm produces specific challenges in that repeated messages add to the network load and device processing. Network collision problems can be met to some degree with switched routers. Message filters as low as possible in a device network stack can address device overload concerns by giving priority to mission critical messages related to a specific device and discarding others. Still, care must be taken to ensure that oscillography and other non-time critical data sent on the network are correctly managed at the application layer to prevent overloading the network or device buffers and delaying the control messages. In order for UCA GOOSE to be effective as a method to send mission critical data throughout the network, all of the above concerns must be addressed and enforced by all devices on the network.

The content of the GOOSE message can be broken down into three areas: a header, Dynamic Network Announcement (DNA) state information, and User State information.

The header contains operational information about the GOOSE message such as the name of the sending device, the time that the GOOSE message was constructed, and the maximum time until the next GOOSE message. The Max Time until next GOOSE is used to detect failure either in the sending device or in the network itself.

The Dynamic Network Announcement or standard bit pairs were designed to facilitate connection between devices. For example, if a line relay issues a "Trip" signal, any device subscribing to the line relay and that is interested in that particular signal can take action accordingly. There are 32 pre-defined bit pairs which can be seen in Appendix I. The concept is similar for the "User State" information except that the definition of the data is totally user defined. Data states are sent in pairs with (0,1) and (1,0) being the primary logical states, (0,0) being defined as a "transition" state, and (1,1) being undefined.

The delivery of the GOOSE object is through the connectionless ISO stack, which means that there is no specific destination address. As such, some address must be entered for the Ethernet receiver to resolve. One option is to require the user to create and enter a 48 bit address to define who the publisher is. This same 48 bit address would have to be programmed into each subscriber that wanted to receive a GOOSE message from that publisher.

A second option is to work with a **S**elf **M**entoring **A**nd **R**e-**T**raining or **SMART** GOOSE. Self Mentoring is the process of automatically defining and determining an address of the publisher and subscriber(s) based on a logical name. During set-up, the engineer programs every device in the station with a unique name and programs the receiving devices with a list of device names from which it should expect to receive data. On start-up of the network, the SMART GOOSE reads the Media Access Control (MAC) address of the Ethernet controller and uses this unique address as its source and destination address for GOOSE messages. Next, the Ethernet receiver in the receiving devices goes into "promiscuous" mode whereby all multi-cast messages are read and decoded. The name of the device sending the message is compared with the programmed list of "devices to listen to". If the names match, the receiving device stores the MAC address of the sending device in a high-speed hardware address comparator. Once all address / name matches have been made, promiscuous mode is turned off and all multi-cast messages are now captured based on a hardware address comparison.

The "Re-Training" part of the SMART GOOSE comes into play when a relay is taken out of service or a CPU module is exchanged or upgraded. When the CPU card is changed, the corresponding MAC address for the Ethernet card changes as each Ethernet controller in the world has a unique 48 bit address. SMART GOOSE (on the receiving side) recognizes that the GOOSE message it was expecting is missing. In this scenario, the receiving relay goes back into promiscuous mode – again searching for a message with the name of a desired device inside. Once found again, the new MAC address for the new CPU / Ethernet controller is stored in

the high-speed look-up table and the receiving relay once again turns off promiscuous mode and returns to normal operation.

As mentioned earlier, the goal for "max time on the wire" was less than 4ms. Achieving this time involves defining a number of system factors including internal GOOSE processing, communication speed, number of devices on the LAN, and LAN loading. Figure 3 shows an oscilloscope timing of a digital input on one relay and the closure of the output contact on a second relay. This time (7.8ms) includes processing of the digital input (including debounce), processing of relay logic, transmission through the communication stack, time on the wire, communication processing on the receiving relay and output contact execution time. Time on the wire for this application was in the microsecond time frame.

Generalized Relay Architecture

Given this new construct of device to device communications, there is now a need to be able to logically integrate data not only from one device but also from other logical devices in the network. As such, one can now look at a generalized device logical architecture to perform this integration function. This generalized architecture is shown in figure 4.

The architecture can be divided into three areas: inputs, combinatorial logic, and outputs. In the GOOSE enabled device, there are four sources of inputs. The first are the outputs from the various protection functions. The second is from the traditional "hard wired" digital inputs. Third, we can speak of "remote inputs" that come from other devices in the network. Lastly, there are "virtual inputs". These inputs are memory locations that can be set from external sources such as a Human Machine Interface. A good example of a virtual input is user flag that is set to block operation of a device or function.

Given the various input signals present in this next generation device, some sort of programmable logic is now needed to combine these signals into the functionality required by the user. In general, any given device may have multiple logic functions internally programmed – each with its own resultant output.

This leads to the third area of the generalized functional architecture which is the output structure. Each logic equation implemented will have an internal result or "virtual" output. It is desirable from a user's perspective to be able to time tag the virtual outputs in order to evaluate the proper operation and performance of the programmed logic. Virtual outputs can then be mapped to one of three places: First of all, virtual outputs can be mapped to a physical output contacts. Secondly, virtual outputs can be mapped to "remote" GOOSE outputs and sent to multiple other devices. Lastly, if the programmable logic permits, a virtual output can be fed back as an input to the programmable logic. This capability allows one to create a state machine in the device.

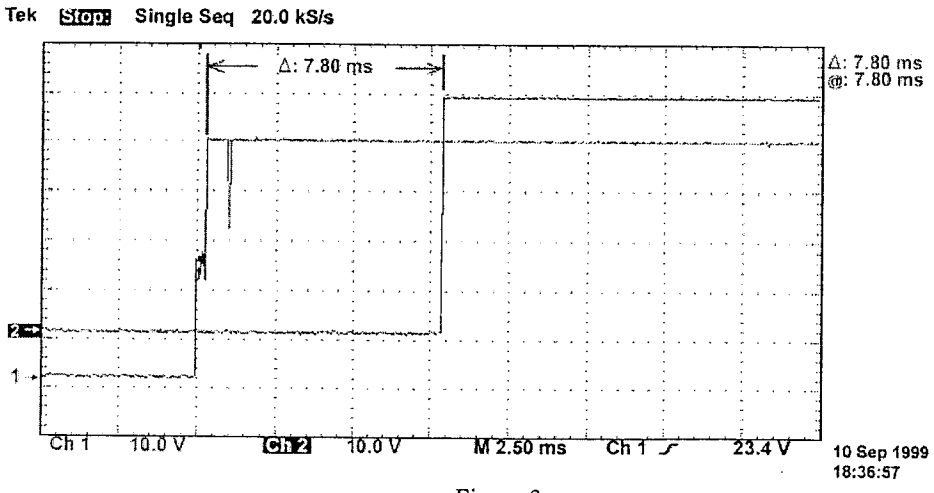


Figure 3
Oscilloscope Timing of Relay to Relay GOOSE Message

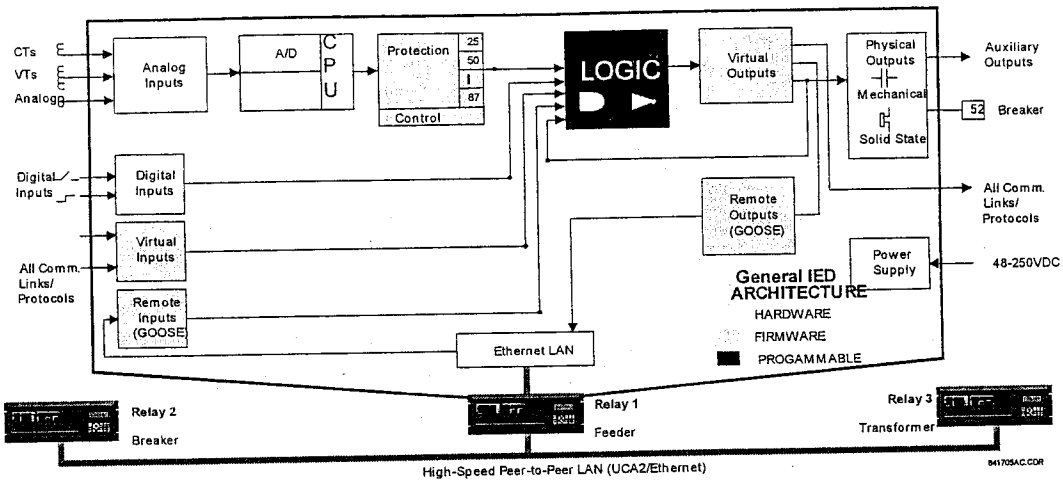


Figure 4
Generalized Device Logical Architecture

GOOSE Applications

Given GOOSE messaging in conjunction with a programmable logic architecture, there are now a limitless number of applications that can be implemented. This section looks at four of these possible applications:

Voting:

In the art and science of protection, part of the "art" is creating a balance between the security and dependability of a protection scheme. One technique that is used in mission critical application is the concept of voting (see figure 5). Voting says to issue a trip only if 2 out of 3 relays say trip. To implement this function, relay 1 needs to get trip information from relays 2 and 3, relay 2 needs to get trip information from relays 1 and 3, etc. Each relay is required to implement the voting logic internally and each relay has to subscribe to the others trip message.

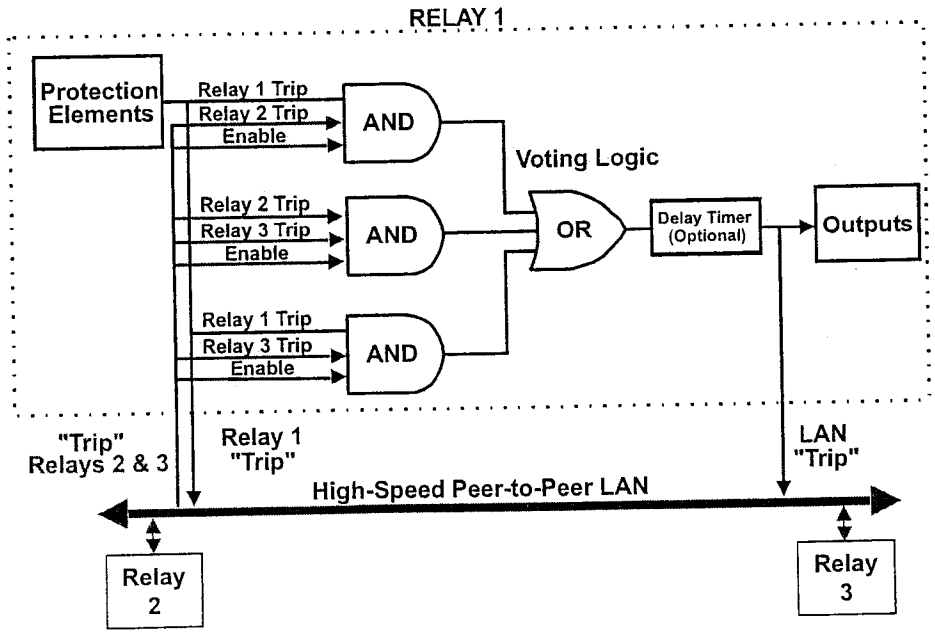


Figure 5
Relay Voting Scheme using GOOSE Messaging

Since each relay has the voting logic internal to itself, failure of a single relay does not fail the voting scheme.

What is interesting to note is the performance of the scheme under a "dead GOOSE" scenario – that is – when a particular relay fails to send a GOOSE message in the allotted time frame. When this happens, a default state is assigned to the expected data. Depending on how the default is set by the engineer, the voting scheme will default to be more secure or more dependable. For example, if relay 2 fails and the trip input to relay 1 is defaulted to "no trip", for a trip to occur, both relays 1 and 3 must issue a trip thus defaulting to a secure state. On the other hand, if the failed input from relay 2 is set to "trip", the system defaults to a dependable state in that if either relay 1 or relay 3 say trip, the system will trip.

Bus Blocking

In many distribution station applications, an incoming feeder has a breaker feeding a bus with multiple feeders exiting from the bus (see figure 6). Typical protection calls for an instantaneous overcurrent function that is coordinated with the overcurrents on the underlying feeders. Coordination typically can be translated as "time delay". Application of GOOSE messaging between the underlying feeders and the incoming feeder breaker can optimize this situation.

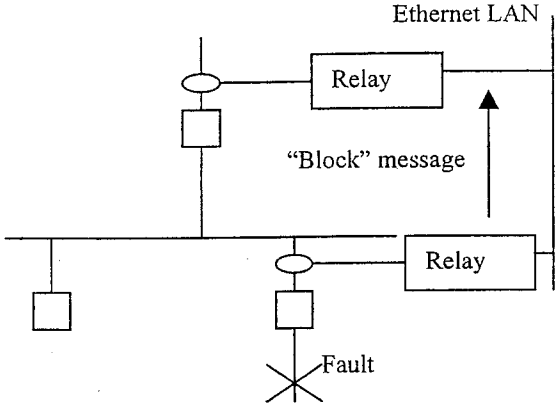


Figure 6
Bus Breaker Blocking

When any of the feeders detects an overcurrent, it is to send a "block" message to the incoming feeder telling it not to trip. Such communication can speed up protection for bus faults and add security for feeder faults.

Load Shedding

Typical load shedding applications in a substation require the addition of a separate under frequency relay followed by wiring from the load shed relay to any breakers to be tripped under an under-frequency condition. Reality is that most breakers in a substation are connected to the tripping output of at least one relay in a substation. Connecting these relays via an

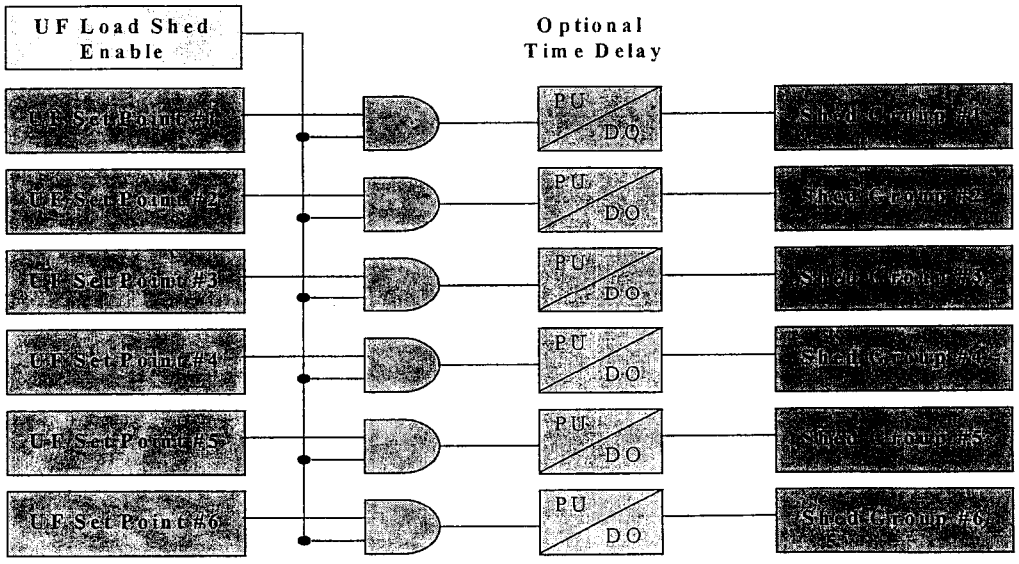


Figure 7
Distributed Load Shed

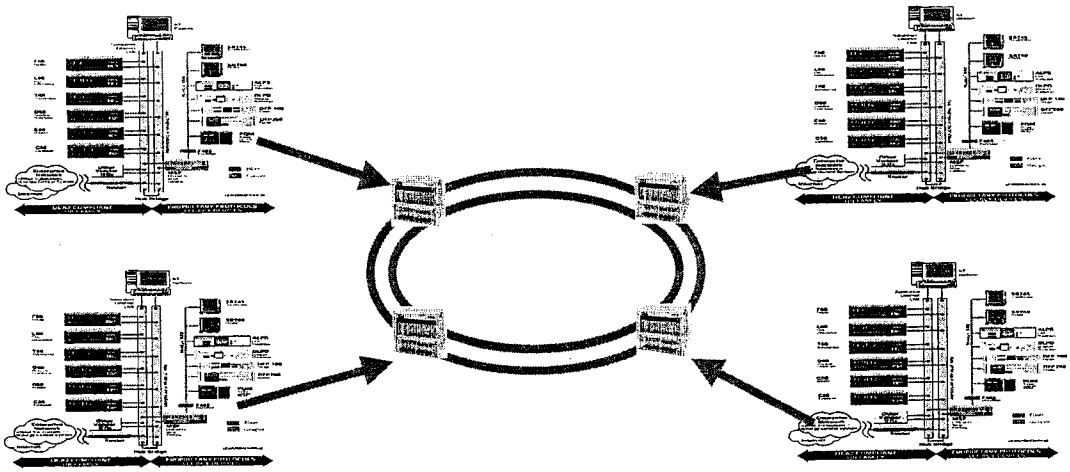


Figure 8
Wide Area GOOSE (WAG)

Ethernet network, load shed becomes a GOOSE message to trip the appropriate breaker (figure 7). With some additional logic, the engineer could actually create a rotating schedule of loads to shed. Clearly, a restoration scheme could be created in similar manner. Since this scheme could be loaded into any relay, redundancy is also easy to implement.

Wide Area GOOSE (WAG)

Although the GOOSE message is not routable, a number of SONET multiplexors are capable of "bridging" GOOSE messages between substations over Ethernet. With this configuration, one is able to perform functions such as transfer tripping, pilot based protection, high speed data transfer, and in general, have a foundation for next generation power system control. Caution need be taken when implementing such a scheme as too many GOOSE messages can clog the network.

Conclusions

Next generation microprocessors in next generation digital relays have provided the foundation for next generation communication protocols and applications. The Utility Communication Architecture has provided the relay engineer with a new high-speed binary tool in the form of the Generic Object Oriented Substation Event or GOOSE. With this tool, relay engineers will be able to create advanced protection schemes more easily with no additional wiring.

Bibliography

1. General Object Model for Substation and Feeder Equipment (GOMSFE). Version .9, January 14, 1999 ftp.sisconet.com/EPRI/UCA2.0/ gomsfe9.zip