Back to Table of Contents

High Speed Communications for Protective Relays

By
Steven A. Kunsman and Michael C. Kleman
ABB Power T&D Company, Inc.
Power Automation and Protection Division
Allentown, PA

Charles B. Adamson
Southern California Edison Company
Rosemead, CA

Presented to
24th Annual
Western Protective Relaying Conference
Spokane, WA
October 21-23, 1997

INTRODUCTION

This paper covers new technological developments in communication systems as they apply to protective relays, power system information and automation systems. Over the past decade, advances in the microprocessor have allowed for new and innovative ways to transfer information between applications. This is evident with the growth and acceptance of communication networks, like the Internet, as a means of transferring and/or accessing information from around the world. As corporate and department managers learn of this available information from various sections of the power system, the need to easily access this data will be a requirement of the communication's network and its components.

With the increasing demand for power automation, a need arises to develop a system communication strategy that can handle high rates of data transfer. The ideal solution is to have the ability for data collection from various types of intelligent electronic devices (IEDs) on a distributed network as well as a means to reliably control the substation equipment. Some high speed communication interfaces embedded within the protective relay, which can also be called an IED, provide a means to communicate at rates of one million bits per second (1 Mbps) and higher. This type of system connects devices such as a Programmable Logic Controller (PLC) and various types of IEDs allowing for plug and play automation solutions. In this paper, a plug and play solution refers to a system where components can easily be setup with minimal efforts and in some cases, the only setup required is to configure a device's network address and make the physical connection to the network.

BACKGROUND OF THE TRADITIONAL PROTECTIVE RELAY

A protective relay is a device that monitors the power system for abnormal conditions and takes preventative actions to limit power system stress and reduce equipment damage. With the early 8-bit microprocessor based relay systems, protection of the power system was the primary function, but, advances in the computing power of a microprocessor allowed for additional functionality like metering, breaker reclosing and communications. The communication's interface in the typical microprocessor based protective relay used EIA-RS232 serial communication port(s) connected to a VT100 terminal or a computer with a terminal emulation program. EIA-RS232 is a point-to-point system allowing communication to a single device or multiple devices through a switch box or data concentrator.

Although these 8-bit devices had the capability to communicate at rates of 19,200 bits per second (bps), the actual data through-put was much slower. This was because the device's protection functions had a higher priority over the communication process. This required either hardware or software data flow control between the master and slave devices to ensure that the information was received and processed correctly. An example of hardware data flow control, or also known as hardware handshaking, is when a master Requests To Send (RTS) data to the slave and the slave grants the master access through a Clear To Send (CTS) signal. When the slave device is not able to process any more data, it deasserts the CTS signal stopping the master from additional data flow. Once the slave is able to process more data, it asserts the CTS signal allowing the master to continue the data transfer. This stop and go process continues until the transaction completes.

Another type of common communication's interface for microprocessor based relays is an EIA-RS485 supporting communication's rates of up to 19,200 bps. This serial communication technology allows a single master to communicate to multiple slave devices using a two wire (half-duplex) differential multi-drop physical layer. Each device, whether it is a master or slave, must have a unique address and this address must be embedded in the master's command sequence. This command sequence is received and address decoded by every slave device connected to the network. When the decoded address matches the slave's address, this device processes the master's request and replies with a response. Applications using the two wire differential pair to both transmit and receive data, do not permit the use of hardware data flow control. Thus, this technique requires greater processing capabilities from both the slave and master devices to ensure complete data transfer.

MULTIPLE MASTER COMMUNICATIONS

Typical relay communication networks, until present time, were only capable of being configured as a single master device communicating to slave devices. A recent advancement in IED communications has been the application of high speed communications networks allowing multiple masters and peer-to-peer networking schemes. Unlike the EIA-RS485 multi-drop network, multiple masters can issue commands to several slaves and their responses could occur simultaneously. This requires a network architecture that prevents and avoids data collisions from multiple devices transmitting at the same instance as discussed in the Collision Detection Network section.

A major advantage of the multiple master environment is the distribution of the communication tasks to the various masters. These multiple masters allow for the segregation of tasks during critical periods when events occur like faults or frequency disturbances. An application of the multiple master is when precise control logic requires the timely supervision of networked IEDs while at the same time the system operators need information on the events. In a single master environment, less important data collection has the potential to cause congestion on the network not permitting the time critical information exchange between the master and slave devices.

TOKEN RING NETWORK

One technique commonly used in network communications is a token passing architecture. The token is a virtual privilege to network access and is passed between every device or node connected to the local area network (LAN). For a device to communicate on the network, it must possess the token subsequent to any network services (read, write, etc.) being permitted. Another important feature in the token passing architecture is the internal policing of the token allocation time. Each device is allowed token possession for maximum amount of time before forfeiture of the token to ensure that every node has equal access to the network. In some token ring networks when a token owner does not require the maximum time, the node relinquishes the token and its remaining time to the next device in the token ring. After all devices in the network have possessed the token, the first device regains the token and the process starts all over again. This is how the term "token ring" is derived. In addition, the amount of time required to make one complete loop in the token ring is called the token rotation time. There are other token passing architectures that will hold the token for an allocated time regardless of whether the node requires network access.

Token ring networks provide various techniques to exchange data from device to device on the network. As with the traditional EIA-RS485 networks, a token passing network also supports master to slave communications. One difference in this type of command is that the master must posses the token to issue the slave's command sequence. Once the master owns the token, it can issue a command to a single, or to multiple slave devices. The command sequence is received by all devices on the network and the addressed slave device(s) processes the request after it obtains token ownership. The major advantage of this type of architecture is that while the slave is processing the master's request, the network remains active allowing for other masters (or the same master) to process additional slave commands. When using the EIA-RS485, the master must wait for the completion of the master-slave transaction before another slave device can be solicited.

TABLE 1. RESPONSE TIME COMPARISONS

Network	Data Transmit Time	Device Response Time	Total Response
EIA-RS485	20*512/9600 = 1067 mS	20 * 100 = 2000 mS	3067 mS
Token Ring Poll	20*512/1M = 10 mS	20*25 + 100mS = 600 mS	610 mS
Token Ring using Global Data	20*512/1M = 10 mS	100 +25 =125 mS (IED Global Update Time + One Token Rotation)	135 mS

This is important when large data through put is required. For comparison, a master requests 64 bytes (512 bits) of binary metering data from each of 20 slave devices. For this example, the average response processing time of the IED is 100 mS (Note: that the response time will vary depending on the processing capability of the IED). The comparison will be between an EIA-RS485 (9600 bps) and a token passing (1 Mbps) network. The results are shown in Table 1. The example is for comparative purposes only and assumes that protocol overhead is nominal and raw data (only necessary bits. i.e., no start and stop bits) is being transmitted.

UNSOLICITED/GLOBAL DATA EXCHANGE

Another advantage of some token ring networks is the transmission and collection of unsolicited user definable data (global data). Global data is broadcast from one device to all other peers in the local network. Every peer device receives and maintains a local copy of this global data for every other node in the network. The ability to transmit and receive global data is dependent on the peer's application and how the IED was implemented. Global data exchange, like any other network access, requires token ownership of the peer. Updates can occur once per token rotation or at slower rates if the peer does not need to update its global data. These global database update rates are dependent on the implementation and capability of the IED.

Global data can be used in cases where commonly required information, like analog power quantities and binary input/output status words, would require fast update rates in the master. In a master-slave type network, this data would be polled by the master using valuable network resources. Another advantage of using global data exchange is the ability to customize the number of data points broadcast, thus, minimizing the amount of time required for transmission. In the event that the global data is not required from an IED, the transmission of global data points can be turned off.

COLLISION DETECTION NETWORK

Another type of network that supports peer-to-peer communications is Ethernet (IEEE 802.3). These types of networks are commonly used in office environments for the purpose of interconnecting desktop computers, file servers, printers, etc. in a common resource pool. Permission for a master to access the network is not supervised by a token passing scheme as described earlier, instead it utilizes a Carrier Sense Multiple Access with a Collision Detection (CSMA/CD) technique to determine accessibility to the network.

This method allows all devices on the network to gain access at anytime. When a device requires network access, it will listen for other network traffic. If the network is idle (i.e., no communications occurring), the device transmits a data packet on the network. The transmitting device also receives the same packet and compares this data to the data originally sent for the determination of network contention. When no collisions are observed, the device continues the data transfer. In the event that a network collision is detected, all devices in contention wait for an allocated time determined by a random number generator before attempting retransmission. This process will continue until all devices in contention successfully complete transmission.

The physical layer interconnections between nodes utilize a shielded twisted pair, unshielded twisted pair, coaxial cable or fiber cable. These systems are typically non-isolated, except for fiber, and in a substation environment can be subjected to voltage transients and ground potential rises.

IMPLEMENTATION OF THE IED NETWORK INTERFACE

To achieve the many advantages of high speed networks, several considerations are required for the successful implementation of the IED's network interface. The high data transfer rate is only as good as the weakest link in the entire system. Furthermore, flexibility of the IED and the ability to provide a means of user customization allows for the ease of integration.

Since multiple master networks allow simultaneous command processing, the peer device must have the ability to process more than one command sequence concurrently. If the peer device only allows single command processing, a lower priority command may prevent a time critical command from being processed. This can be easily demonstrated in a substation automation application where two masters request data or issue commands to a common peer device. In this application, the masters consist of a PLC that accesses the network for automatic control and a host computer that is responsible for data collection and reporting status information to the system operators. If the IED's network interface only allowed single command processing and the peer was busy processing a response to the host computer, a PLC requested to trip a breaker would be blocked until the command path cleared. The ability to concurrently process commands allows the PLC trip command to be executed and not blocked.

Another important consideration is the IED's performance and its ability to execute requests efficiently. Certain requests issued to the IED may not require immediate processing and can be deferred to a lower priority processing task. Responding to metering requests and collection of event reports are examples of commands that can efficiently be processed in a lower priority task. In contrast, the time critical control logic of the PLC is required to be processed in the IED's high priority processing task where delays, due to lack of performance, could result in equipment damage in the power system. In this type of application, a worst case timing study should be performed on the entire system to ensure that the critical timing events are accomplished. Key factors in determining the worst case timing are the token rotation time and the IEDs processing time that is dependent on the ability to prioritize incoming requests.

Flexibility of the IED is another key factor in the adaptation to user's various applications. Global data definitions are typically restricted to a limited number of available data points. To maximize the use of global registers fixed or non-configurable global data points within the IED are undesirable. Rather, the ability to customize and allow the user to select which points are made available to other peer devices through the use of global data, provides the necessary flexibility required for ease of automation and integration of the IED.

APPLICATION - A FULLY AUTOMATED POWER RESTORATION SYSTEM

The key to fast, reliable, repeatable, substation restoration performance is a high speed communication link between all components. The link used in this application is a 1 million bit per second (Mbps) Modbus Plus™ token ring type network. A token passing communications network is predictable in its performance given multiple fault and restoration scenarios. It is not only the speed of the network that allows for restoration reliability but the intense use of global data variables. As described earlier, global data points are broadcast over a token ring network when a network device receives the token (permission to talk). Every other device on the network keeps a local copy of all other devices global data. This is typically stored in Random Access Memory (RAM) and is refreshed every token pass. This allows high speed data transfer without the need to poll by any of the network masters, such as, the Programmable Logic Controller (PLC) or Supervisory Control and Data Acquisition system (SCADA). Some communications networks do not support the use of global data. In this case a "master" (the PLC in this example) must constantly poll each device for tripping status, breaker state, and control bit positions. Anytime polling is required, network capacity suffers, especially in larger stations where many devices require polling. The reduced network capacity may be acceptable in smaller substations if fast power system restoration is not required and data acquisition and control are kept to a minimum.

SCADA systems typically are programmed to expect acknowledgments to commands or scans within a pre-programmed time interval. If a command or scan is not acknowledged within this preprogrammed time, a communication error or time-out will occur. Various bit oriented communication protocols are typically used as a method of efficient data transport from a SCADA master station to a remote location. This allows for the use of 1200 bits per second (bps) communication links (via modem) without sacrificing command and scan turn around timing. An argument can be made that current modem technology allows for communication speeds in excess of 28,800 bps thus not requiring the use of efficient bit oriented communications protocols. Although this is true, it is rare that a modem will reliably connect with a remote at 28,800 bps 100 percent of the time. Typically both modems will negotiate an optimum baud rate which may be substantially less than the maximum modem rating. If the SCADA system was designed to operate at the 28,800 bps level, time-out or communications failures will occur at a lower bit rate. The cost of line conditioning beyond the standard voice grade channel is also a consideration when requiring high speed links.

Many substation automation systems consist of SCADA systems only. The following application deals with a "true" substation automation system where along with SCADA functionality, fast automated restoration of service occurs after multiple types of line, bus, transformer, and feeder faults.

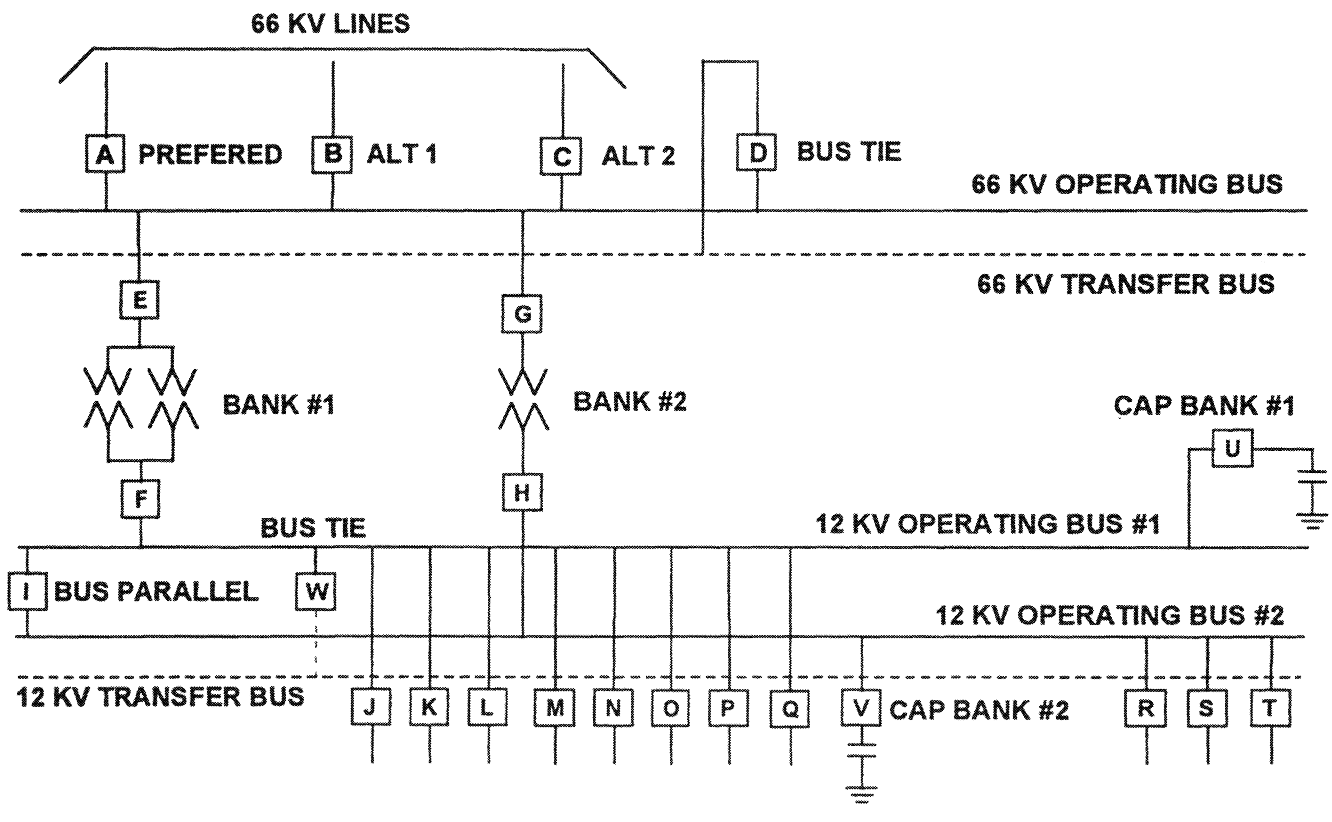

Figure 1.Sample Substation

IED's are placed at every breaker from A to V and connected along with the PLC and SCADA system to the high speed communications network. The IED's are placed at every station circuit breaker to provide protection, control, and analog and digital data associated with the breaker on which it is applied. A station Programmable Logic Controller (PLC) is used to coordinate and supervise circuit breaker reclosing after a major outage such as a bus fault. The application described in this text deals with this type of fault since it requires intense communication between PLC and IED's. Multiple restoration schemes are programmed into the PLC. The PLC that decides what the best method of restoration is based on input from all of the station IED's. Figure 1 outlines a station single line drawing. This section will deal only with the 66 kV line (A,B,C) and bus tie (D) circuit breakers. The 66 kV bus restoration scheme is only a very small part of the substation logic.

An IED is applied as a 66 kV bus differential relay. The line current transformers (CTs) and transformer bank high side CTs are connected in parallel so that anything other than through current will energize the instantaneous overcurrent element (50P). A programmable logical bit in the bus differential IED is assigned as "Bus Test Enable" and is used as the SCADA or local interface to the PLC for bus restoration permission. Each line and bus tie IED also utilize a "permission bit" allowing the PLC to close its associated circuit breaker. If this bit is a 1, bus testing is enabled. If the bit is a 0, bus testing is disabled. Refer to Figure 2 for an overall picture of the bus restoration logic. Since the PLC logic is extremely intense in its diagnostics of the overall fault and reclose scenarios, Figure 2 shows only the basic logical flow and does not account for all bus restoration logic conditions. The following text will define, in more detail, the restorationlogic.

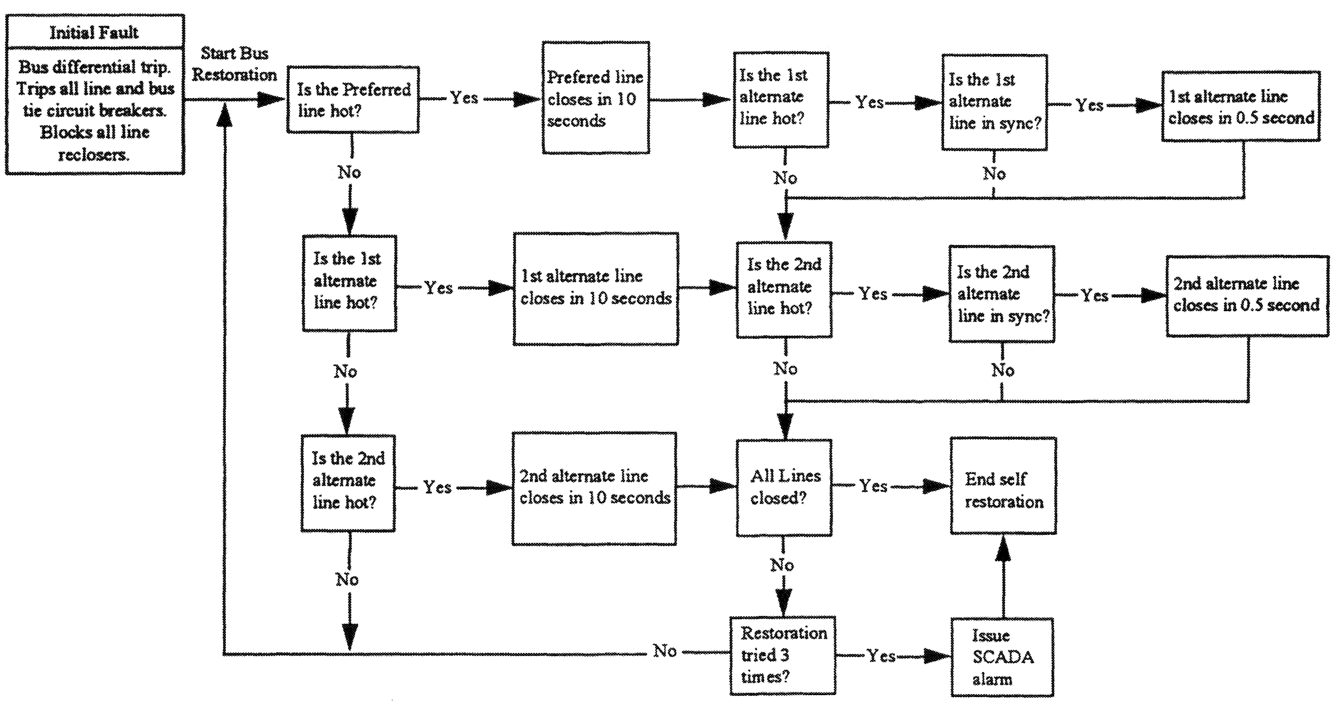

Figure 2 - PLC Logic Flow

When a bus fault occurs, the bus differential IED will send an instantaneous unconditional trip command via hard wire to all line (A, B, C,) and bus tie (D) IED's. Since the PLC continually scans its local copy of the global data base for any breaker operations or trip conditions, it will detect the differential trip along with the line and bus tie circuit breaker status. The IED will determine if any breaker fail conditions exist. Once it is determined that all of the circuit breakers opened successfully the PLC will initiate the restoration logic. The PLC determines all of these conditions in approximately 28 milliseconds (1 scan of 412 ladder logic networks). If any line circuit breaker fails to open, the fault will be cleared by the remote breaker. In this case the PLC will read a breaker fail bit from the failed circuit breaker IED global data broadcast and lockout restoration. Each line IED also contains a PLC supervised hot and dead line recloser.

After a bus fault occurs, a "Recloser Block" latch sets and disables the individual hot and dead line reclosers until bus restoration is complete. The bus testing starts 10 seconds after any line becomes hot and all hot lines will test concurrently in a programmed sequence. Once a line circuit breaker closes and successfully energizes the bus, the PLC will check the status of the remaining lines. If they are hot and in sync, a close command is issued in 0.5 seconds. If any line is not hot or not in sync, the PLC will wait 60 seconds for these conditions to become true. If they do not, the PLC will abandon the effort and send an "Unsuccessful Restoration" alarm to SCADA. If restoration is successful, the logic will reset in 60 seconds. If the initial bus test fails, the logic will lockout until the circuit breakers are closed manually.

It is interesting to note that the entire time that this logic is active and timing, SCADA scans are occurring due to the event. The high speed network bandwidth combined with the use of global data variables assures that neither the PLC logical commands nor SCADA system are required to "wait" for the network. It can be concluded then that this type of system assures a very high percentage of timing accuracy and repeatability.

This type of restoration logic is not new and has been implemented in similar form for many years by use of electromechanical and solid state relay systems. The major difference here is greatly enhanced flexibility and reduced wiring costs. A PLC based restoration system is almost infinitely programmable. Logic changes with an electromechanical or solid state relay control system requires a power system outage and many hours of re-wiring and testing. Furthermore, control wires, sometimes in large bundles, are run between cubicles to perform the same functions that can be accomplished using a single LAN connection.

APPLICATION - DATA COLLECTION PERFORMANCE FROM A HIGH SPEED NETWORK

Another important use of the high speed network is "real-time" data collection of the various IEDs in the network. The multidrop network shown in figure 3 is a configuration of sample substation in the above application. The single segment communication's network connects all feeder, line, transformer, bus and capacitor control protective relays along with the PLC and data collection master workstation. The master workstation maintains a system database of all IED metering, I/O status, alarm and event information. In the above example, the protective IEDs utilize 22 of 32 available global data points for acquisition of power system analog registers, bit masked I/O status registers and an IED event status register. Other less critical system information is polled by the master workstation on timed intervals or by detecting a change in the status register. Change in state of the status register indicates that a fault or an operation of some sort has occurred in that specific IED. This tells the master to initiate polls to the affected IEDs.

There are 25 devices (23 IEDs, 1PLC, 1 Master Workstation) communicating in the 1 Mbps token ring that has a nominal token rotation time of 25 milliseconds (mS) for an average 1 mS per device. Each IED's global database updates the networked peer IEDs at a rate of 60-100 mS. When the IED has fresh data, it can transmit this information during the next token possession. Every peer device on the network will maintain an updated copy of each device's global database at a refresh rate of every 6 token passes or 150 mS.

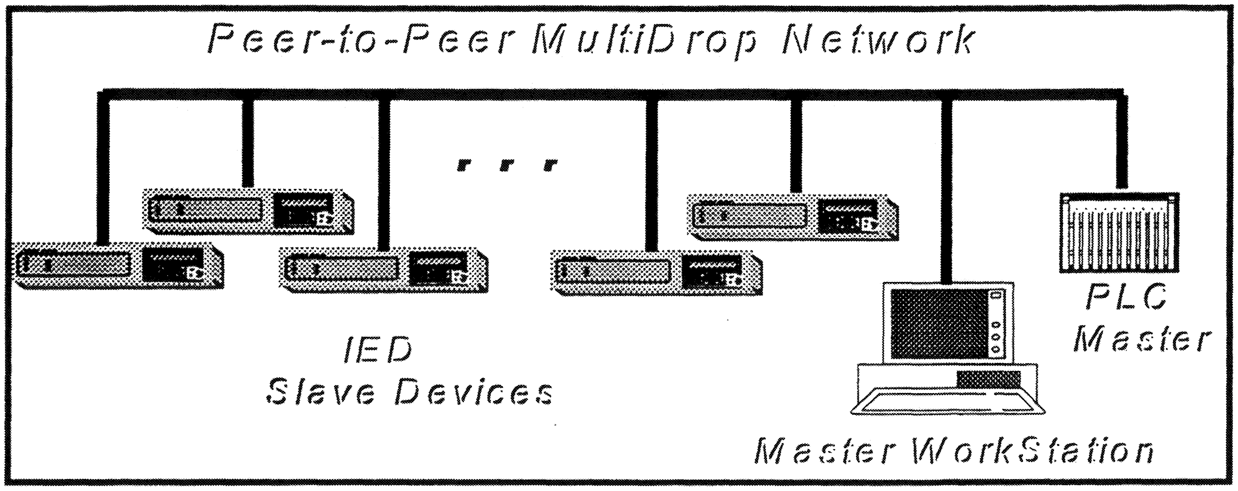

Figure 3 - MultiDrop Substation Network

In this application, the master workstation uses the global data, stored locally in the network interface, to create a substation database for all IEDs in the power system. Processing overhead in the master station for disk storage and MMI display allows for an update rate of the power system database to under one second. Typically, operators and technicians are accustom to instantaneous electromechanical metering responses and breaker state indicators. When using a virtual instrumentation panel, a screen update time of three or more seconds is usually unacceptable in the operator's perception questioning whether the breaker operated. Thus, the high speed communication's network is important when the master station's MMI provides a means to issue commands, to perform various IED functions, like tripping and closing breakers, and to acknowledge alarm conditions.

FUTURE HIGH SPEED NETWORKS

As the technology advances in microprocessor IED continue, the more functionality and information will be demanded. Some of today's complex IEDs contain several thousand data points and with these advances, higher performance requirements will be placed on the communications and information networks. These demands are currently being addressed through such forums as the Utility Substation LAN Initiative where the goal is to have a common protocol and interface compatibility across all manufacturer's IEDs. At the time of this publication, the technology being evaluated by this forum consists of a 100 Mbps Ethernet physical layer incorporating the UCA 2.0 application layer. To add further confusion to the next generation substation information networks, recently announced communication interface technology will allow device connectivity at rates of 1Gbps (1,000,000,000 bits per second).

CONCLUSION

In conclusion, the protective relay with an embedded high speed communications interface provides a reliable solution to data collection, transfer and control. This type of system is an integral part of substation automation that also provides additional features that are not currently available with traditional systems. Finally, the plug and play integration of these communication solutions allows for lower integration and application cost through the ease of integration and the elimination of third party hardware (i.e. protocol converters).

BIBLIOGRAPHY

1. "Advancements in Microprocessor Based Protection and Communications", IEEE Tutorial Course, IEEE Catalog Number 97TP120-0, 1997.

2."Substation LAN Options - An Overview", Unknown ,DA/DSM Proceedings VFA.4/2 970059,1997.

3. "The Southern California Edison Company Substation Automation System", Kleman, M., 1996

4. "Substation Integrated Protection, Control and Data Acquisition Phase 1, Task 2 Requirements Specification", EPRI, RP3599-01 Version 0.2, 1995.

5. "Modbus Plus™ Network Planning and Installation Guide", Modicon, Version 2, 1995.

Technical Biography of Steven A. Kunsman

Steve joined the ABB Power T&D Company Inc., formerly known as Brown Boveri Corporation, in 1984 in the design support group. He graduated from NCC with an ASDT and continued his education through part-time classes graduating from Lafayette College with a BSEE. In 1992, Steve transferred into the microprocessor product development group and was a core team member in the development of the DPU2000 and later the 2000/R series product line. Another critical project was the implementation of the Modbus Plus™ communication's interface for the 2000R series product. Steve presently holds the position of Lead Development Engineer for the ABB Power Automation and Protection Division's Allentown operation and is in pursuit of an MS in Management of Technology at Lehigh University. He is a Member of the IEEE Power Engineering Society.

Technical Biography of Michael C. Kleman

Mike Graduated from Lincoln Technical Institute in 1983 with ASET and began his career in the relay and controls industry when he joined GE Protection and Control in 1984 as a Relay Technician. Mike moved to the Design Engineering department at GE as a Relay Design Engineer in 1988. Here he was involved in the design of protective relays used primarily in high voltage transmission systems with emphasis on pilot wire current differential relaying. He completed his BSEE degree at LaSalle University in 1993. In June of 1995 Mike joined ABB Power T&D as an Application Engineer assigned to work on Substation Automation Projects. Mike has worked with many utility and industrial clients to provide cost effective high speed data acquisition and automated control systems. Mike is Member of the Institute of Electrical and Electronics Engineers and the Power Engineering Society.

Technical Biography of Chuck Adamson

Chuck started in the Utility Automation field as a protection and control technician commissioning and trouble shooting some of Southern California Edison's first Substation Automation projects in 1986. These early projects consisted of stand alone PLCs performing functions previously done by electro-mechanical devices. He remained involved with SCE's automation efforts through their evolution to relay interfaced PLC-RTU systems, Synchronous Condenser and Load Tap Changer automation, serial communication linked PLC-RTU systems, and most recently Networked IED-PLC-Emulated RTU systems. As the systems evolved, Chuck was involved in their design and programming. He helped to develop and program many of SCE's automation PLC logic programs. In 1994 Chuck helped develop one of SCE's early substation IED network systems. He co-authored a paper on the subject before the 1994 Western Protective Relay Conference, and 1995 Texas A&M Substation Automation Conference. Chuck is currently a Protection and Control specialist at SCE, with Project Management responsibilities for Substation Automation.

Back to Table of Contents