Using Information From Relays to Improve the Power System

David J. Dolezilek and Dean A. Klas, *Schweitzer Engineering Laboratories, Inc.*

I. Introduction

Innovative developments within microprocessor-based relays have created new ways of collecting and reacting to data and then using this data to create information. In this paper, the authors evaluate the types of data available in typical protection devices, as well as the value of communicating this data to other devices and applications. Currently, power providers are dealing with demands to increase productivity and reduce costs that translate into the need to collect and act on decision-making information. Communicating information between protection components enables superior yet simple protection systems. This same information can feed other system needs such as automation, monitoring, and control.

We begin with a description of the data available in microprocessor-based relays. The description includes why, how, and where the data are used. A simple analysis illustrates the value of retrieving data from microprocessor-based relays. Remote and local users of the data are discussed. System integration and automation are described, and the devices used in the substation are discussed and compared.

The different methods of transferring data to and from relays are discussed and compared. Direct and multidrop designs are discussed, as well as prioritization of data, transfer rate considerations, and protocols. This is followed by a discussion and comparison of contemporary substation network designs and a comparison of their relative reliability.

In general, the authors use the term "power system" to describe the collection of devices that make up the physical systems that generate, transmit, and distribute power. The term "instrumentation and control (I&C) system" refers to the collection of devices that comprise the system that monitors, controls, and protects the power system.

II. Types of Data Within Microprocessor-Based Relays

A. Instrumentation Data

Power system conditions are emulated by creating a digital representation of analog signals and discrete contacts. Various methods are used to instrument these values from physically interposed apparatus, such as current and potential transformers, dc-wetted discrete contacts, and other sensors. The method of instrumentation is not elemental to the purpose of collecting data. Many different ways exist to instrument different system values. Instrumentation data are the result of the various instrumentation techniques used in the relay.

The purpose of instrumentation data is to emulate the current status of the power system. Instrumentation data allow us to protect, control, and analyze the power system using a virtual representation of power system characteristics.

Instrumentation data are the source of all data and calculations in the relay and remote applications.

B. Protection Data

Protection decisions are based on the analysis of instrumentation data. The data used for protection can include currents, voltages, discrete digital inputs, physical location, and atmospheric conditions. The source of protection data may be local and/or remote. Local protection data are instrumented and/or calculated by the particular relay making a specific protection decision. Remote protection data are instrumented and/or calculated by another relay and communicated to the relay making the specific protection decision. In this instance, the remote relay acts in part as distributed instrumentation and processing for the local relay and vice versa.

Protection analysis detects abnormal operating conditions resulting from disturbances on the system. The protection equipment must quickly determine the type and severity of the disturbance and decide if it needs to perform immediate action. The faults must be cleared to protect people and equipment, and then power must be restored quickly to minimize customer outage.

Protection data are used for analysis within the local relay and remote relays coordinated within a protection scheme. Most protection decisions are mission critical and need to be made in a subcycle time frame. The method of communicating this information must be dedicated, fast, reliable, and secure. The most secure method is a channel dedicated to this purpose alone.

Protection is enhanced when these data are communicated quickly to several relays coordinated in a protection scheme. This coordinated protection is more robust and covers much greater distances when these data are communicated to remote relays via a single communications channel rather than the traditional method of a dedicated pair of copper conductors to sense every contact.

C. Metering Data

Traditionally, metering data are calculated analog values that emulate power system operating conditions. They are used for protection, monitoring, control, and revenue purposes. As mentioned above, the system operating conditions are calculated from the instrumentation data

associated with the protection equipment. Metering data are calculated periodically to give a snapshot of the instantaneous state of the power system. Calculation examples include integration over time, scaling, and filtering. Some of the values necessary for metering already exist as a result of protection calculations and can be reused. Other system values are calculated specifically for the purpose of metering. Instantaneous and integrated values are archived periodically to provide peak and load profile historical characteristics of the system.

Metering data can be displayed locally and/or remotely for the purpose of providing visibility of power system conditions to an operator. In this capacity, the metering data are a source of supervisory data. Local users traditionally view these data on a relay display, while remote users typically use a PC or other remote display with communications capabilities. Remote users view these data within a metering system, supervisory control and data acquisition (SCADA) system, energy management system (EMS), distribution automation (DA) system, or human-machine interfaces (HMIs).

Metering values such as demand and peak are archived within the relay for the purpose of creating historical information about the activity of the power system. These are discussed in more detail below as historical data.

Highly accurate metering data are useful for operations and revenue billing or validation purposes. These data can be the input to the revenue metering system within the enterprise and/or be used to validate calibration of other installed revenue metering devices. Revenue class metering at distributed locations within the power system allows operators and processes to make accurate operational decisions.

The remote uses of this metering data are operator visibility and operation of the power system.

In the past, protection actions were initiated as a result of an electromechanical process passing through a threshold, e.g., an induction disc rotating to operate a contact. These processes were often adversely affected by environmental conditions. Now, decisions are made within microprocessors that operate uniformly through a wide range of environmental conditions. Metering data enhance protection by virtue of being an accurate source for protection decisions unaffected by the passage of time or changes in the environment.

D. System Automation Data

System automation data are the result of logical decisions based on other types of data. These decisions often do not need to be made at the same frequency as protection decisions. Inputs to these algorithms can be derived locally or can be received from, or sent to, another device.

Results of these automated algorithms indicate that the relay needs to perform control, acquire and archive data, and generate event reports without intervention by an operator. These algorithms perform actions outside the scope of traditional protection algorithms at the device level and system level using protection data, metering data, extra contact inputs and outputs (I/O), and data communicated from other I&C components. The relay traditionally performs control of power system devices as a function of performing protection of the power system. System automation algorithms control the same, and additional, system components to perform ancillary actions like fault sectionalization, restoration, and load shedding or transfer. Relays are an integral part of automatically controlling substations (substation automation) and feeders (distribution automation).

System automation data serve as another source for device-specific and station-wide custom protection decisions. System automation can be a combination of predefined processes and custom application-specific algorithms. Predefined system automation processes, such as reclosing, and custom user-defined logic can work in a coordinated manner with other relays to create application-specific, system-wide protection.

System automation data are used locally by the relay and remotely by other I&C components performing system automation calculations. System automation data are an input to control and supervisory calculations. System automation decisions need to be made quickly and may result in mission-critical protection actions. Therefore, the method of communicating system automation data must be dedicated, fast, reliable, and secure.

Using these automation techniques, protection of individual power system components is obviously enhanced, but more importantly, the entire power system can be better protected as a whole. Adaptive protection methods are used as the power system configuration changes dynamically. Protection is further enhanced by communicating these data via a single robust communications channel rather than the traditional method of a dedicated pair of copper conductors to sense every contact.

E. Control Data

Control data are the results of process- or operator-initiated functions that perform control actions. Control actions are initiated by local or remote protection algorithms or system automation algorithms or through the intervention of an operator. When the need for a relay to perform a control action is determined remotely, this function is initiated by passing a control message to the relay. Control actions can, therefore, be the result of disparate algorithms in many different devices with different execution time requirements.

These data allow the relay to influence the state of the power system through physical contact with power system devices. Control actions result in manipulating the state of relay contact outputs, such as latching or pulsing discrete outputs or changing the value of analog outputs. These actions in turn initiate when and how power system devices actuate. Remotely generated control messages can cause control actions or the manipulation of local relay logic. Control actions are the result of decisions in protection devices, automation devices, and supervisory systems. These different sources of control actions vary in speed of execution from a subcycle to many seconds. Once the control function is initiated by the relay or accepted from another relay, the control action speed is limited only by the relay's ability to process and execute the result. The communications path for

control messages, which are initiated remotely, determines the additional time latency the control action will experience.

Control data enhance protection by initiating the operation of power system devices in accordance with protection and system automation decisions. Further, they allow remote operators and processes to change I&C system parameters and/or initiate the operation of power system devices as a result of system-wide protection considerations. Group settings selection commands can be sent to relays so that their processing is modified to match changes in the power system characteristics, such as load variation or power system device failure. Finally, as mentioned above, protection is further enhanced by communicating these data via a single robust communications channel rather than the traditional method of a dedicated pair of copper conductors to sense every contact.

F. Supervisory Data

When any of the data types within the relay, or other I&C system components, are used locally on an HMI or communicated to a remote device for the purpose of monitoring the power system, they become supervisory data. Much of the data used for supervisory purposes are the result of other processing. Extra I/O points on the relay are often used to create additional supervisory data about power system components. Examples of such data would be status of motor-operated disconnects, load tap changer positions, and transformer fan status.

Extra contact inputs and results of some logical calculations in the relay can be used solely to provide supervisory data. Contact inputs not used for protection are often used to otherwise instrument the status of system components. Extra contact outputs can be used to control additional power system devices. SCADA hosts, EMS hosts, DA hosts, HMIs, and other operator interfaces display system conditions and status. Operators can supervise the power system through these interfaces which, emulate its state, history, and reaction. The communications path for supervisory data influences the time discrepancy between when it is available in the relay and when it is visible to a remote operator or process.

The traditional data collection approach in the substation has been to build two separate I&C systems, one communications network and group of devices for protection and a separate communications network and group of devices for supervision and control. This adds complexity and cost while reducing reliability. It is likely that the relay is collecting the data necessary for supervision as it is performing protection and other functions. If the supervisory system cannot acquire these data from the relay, a separate I&C device, such as a remote terminal unit (RTU), must be added simply to communicate system data which, likely already exists in the relay.

Supervisory data enhance protection by allowing operators and processes to make rapid, better informed decisions about system-wide, device-specific protection.

G. Device Diagnostic Data

The relay stores information pertaining to power system devices for the purpose of analyzing their operation. Examples include the total number of operations, frequency of use, duration of control actions, and interrupted current. Additionally, self-test processes internal to the relay create information about the relay's operation.

These diagnostic data provide information about the quality of both the power system and the I&C system. The unavailability of either system is minimized through immediate component failure indication; by contrast, traditional periodic relay testing delays sensing of failures until the periodic test or a misoperation. In fact, during most tests, the device is unavailable and some testing actually introduces modes of failure. System-wide device diagnostics allow operators and processes to compensate for failed devices. In addition, system and device failure can be prevented through analysis of diagnostic data to determine appropriate intervals for maintenance and upgrade.

The I&C system immediately detects device deterioration and alerts automatic processes or operators to prevent or delay further deterioration. The system quickly alerts operators or processes when these devices are unavailable to perform, enabling quick repair or replacement. Device diagnostic data enhance protection by maximizing the availability of the protection system.

H. Historical Data

The relay stores data to provide information about the reaction of the power system over time or to an event. These collections include system profiles, event reports, sequential event recorder (SER) reports, power quality reports, and protection quality reports. Report generation is triggered automatically by system disturbances, other events, or by relay logic locally or remotely by other I&C components or an operator. A time-synchronization command from a centralized source allows all devices in the system to use the same clock value for time-stamp purposes. Some system values are captured and archived periodically to enable trending analysis.

Historical report information allows forensic analysis of the power system and the I&C system so that decisions can be made to validate or improve the system's designs. Additionally, periodically stored values provide a profile of system characteristics over time. Archived performance data are used to trend device deterioration or improper configuration.

Event reports are collections of pre-trigger and post-trigger analog and digital values measured and captured in sequence and time stamped. This report captures the reaction of the system and the relay to a disturbance or other event in the power system.

SER reports are collections of data records stored as a result of user-defined changes of state. Each record contains a time stamp and the present states of discrete digital inputs or digital logic values.

Power quality is a broad concept used in comparing the actual power system values to their ideal. Although there are

many dedicated power quality measurement devices, relays are an effective measurement and storage device for some power quality data. Harmonics, frequency, voltage sag, voltage swell, and voltage interrupt are examples of power quality data captured by relays.

Most significant power quality problems are identifiable as power system voltage variations: complete interruption of voltage (<0.1 per unit), undervoltage (sag) , and overvoltage (swell). A large percentage of these voltage variations are a result of power system faults. Recording and reporting voltage variation in the relay allows low-cost correlation and validation of power consumer complaints. Monitoring the power quality allows the relay to react and compensate for power system variation or to alert users.

Protection quality is the measure of the performance of the protection component of the I&C system. These data measure the fitness of items including instrument transformers, relays, batteries, and communications equipment. The quality of these components is the measure of their ability to perform against stated benchmarks. These data help to improve system performance with less testing. Relay element performance such as coordination margins, percent of settings reached, and other alarms are monitored so that the relay can alert an operator when the protection system deviates from nominal. In this manner, data are processed closest to the points measured, and protection quality answers are forwarded to operators.

Profile data are a collection of archived metering data used to provide a historical trend. At the pre-set profile acquisition interval, the relay adds a record to a profile report. This record contains a time stamp and present value of each analog quantity being profiled. Remote users acquire these data and use them to analyze the load requirements and reactions of the power system. The data time stamp allows system-wide evaluation of the sequence of events from several devices. This facilitates system-wide operational and enhancement decisions like connecting additional power sources and modifying protection settings.

Historical data are stored in report format and these reports are communicated to other devices automatically or on demand for additional remote processing. These reports can be quite large and take a lot of time to transmit. Fortunately, remote analysis is rarely appropriate immediately after it is recorded. Therefore, these reports can be communicated at a much slower rate than other data and need not reside on the same communications link as the other data types. Although it is convenient to transfer all data on a single channel, many integration protocols do not support file transfer.

Historical data enhance protection through dynamic system trend analysis as well as being the source for remote operator and process forensic analysis. By continually monitoring device conditions over time, operators and processes develop a clearer picture of device performance.

I. Settings Data

Settings are the variables used to configure relay software to function optimally in specific end user applications. Additionally, settings initiate trigger conditions for event report and sequential event records and act as the parameters used to archive information.

Multifunction and multiapplication relays improve I&C system design. Settings allow the end user to coordinate the I&C system with power system and end user protection practices. Power system parameters like conductor impedance and length influence each individual installation of a relay. Coordination between zones of protection, primary and backup schemes, and sectionalization and restoration processes is done through settings. Additionally, settings can be changed dynamically to conform to changes in the power system. Several groups of settings are stored within the relay, and it will change operation based on which group of settings is selected. Selecting pre-defined settings groups allows use of tested groups of settings for each selected condition.

This settings information is often calculated and stored remotely and then transmitted to the relay through a communications connection. Engineers, relying on their experience or expert software tools, can work remotely to create sophisticated, coordinated settings. Remote storage of the settings for each relay in the system allows a user to better maintain and review this data. This is particularly valuable in the event that an in-service relay needs to be replaced. Relay settings can be quickly retrieved from storage and transmitted to a replacement relay.

Many settings values interact so that to change the operation of a relay, several settings must be changed simultaneously. This results in a large amount of data being transferred during each transaction. However, if settings group selection commands are used for higher speed adaptation, these data are infrequently transferred to and from the relay. The path for communicating settings data must be secure but does not need to be high speed nor does it need to reside on the same communications link as other data. As mentioned above, it is convenient to transfer all data on a single channel; however, many integration protocols do not support file transfer.

Settings data enhance protection by allowing the user to configure the relay to perform optimally in many unique applications. Settings groups allow the protection system to change dynamically to compensate for changes in the power system or I&C system. Finally, the ability to quickly configure replacement relays further reduces the unavailability of system protection.

III. The Value of Retrieving Data From Microprocessor-Based Relays

A. Frequent Communication of Relay Data Enhances Protection

If data can be made into information and used locally within the relay, there may be no need to transfer it. Other data that have value to a remote user may not need to be transferred automatically. In some cases, the data are best left in the relay, or at least the substation, until a time that is convenient for the user to establish a connection and retrieve it. This may be due to the infrequent need for the data or the communication available to the substation. Some substations are isolated and

all data must be stored and periodically retrieved when an operator visits the site. The simple fact that there are uses, besides protection, for the data within relays makes them valuable to many departments within the utility. This helps make a successful business case for a protection designer attempting to procure new relays, which, in turn, enhances protection.

In order to determine what type of information to transfer and how often, the user needs to quantify the benefits that will be derived. We recognized the need to quantify the benefits of design choices in all aspects of protection, integration, automation, and control. In order to identify reliability, E. O. Schweitzer, III, and colleagues wrote the paper, "Reliability Analysis of Transmission Protection Using Fault Tree Methods." The paper introduced fault tree analysis as a tool for our industry to quantify the benefits of various system components and topologies. Gary W. Scheer wrote the paper, "Answering Substation Automation Questions Through Fault Tree Analysis," to help people quantify substation automation designs.

Reliability can be quantified by comparing unavailability for devices and systems. The unavailability for a system is created by combining the unavailability of system devices. The unavailability, q, is calculated using Mean Time to Repair (MTTR) and Mean Time Between Failures (MTBF). The MTTR is the sum of the mean time to detect plus the mean time to repair or replace. The MTBF is the reciprocal of the failure rate. A relay failure does not mean that the relay is inoperable. A failure exists any time the relay cannot create an accurate representation of sensor data, cannot detect a power system aberration, or cannot operate an output correctly, and so on. Causes of failure include settings out of calibration, reaction to environmental extremes, and hardware failure. Some failure modes can be corrected but do exist and may not be detected until recalibration occurs.

$$q = \frac{MTTR}{MTBF}$$

For electromechanical relays, a best-case, estimated MTBF is 50 years. Assume an industry average mean time to repair or replace an electromechanical relay of two days. An industry average schedule for maintenance on these relays is every 6 years. The time between this maintenance and the failure of an electromechanical relay varies between 1 second and 6 years, resulting in an average time to test for and detect failure to be 3 years. This results in a predicted unavailability of 22 days per year.

$$q = MTTR/MTBF = (3 \text{ years} + 2 \text{ days} / 50 \text{ years}) = (1{,}097 \text{ days} / 50 \text{ years}) = 22 \text{ days per year}$$

A probable industry average MTBF of microprocessor-based relays is 100 years. We consider that the time to detect a failure is negligible if the relay has self-test diagnostics and is communicating this information to an operator or process. Again, assume an industry average mean time to repair or replace of 2 days. This results in a predicted unavailability of 0.02 days per year.

$$q = MTTR/MTBF = (2 \text{ days} / 100 \text{ years}) = 0.02 \text{ days per year}$$

The change in unavailability is 22 days / 0.02 days = 1,100 times more available.

Therefore, the simple act of communicating a self-test diagnostic of a microprocessor-based relay to a user or process improves the reliability of protection over electromechanical relays by three orders of magnitude.

The value of communicating other types of data can be determined in a similar fashion.

IV. Remote and Local Users of Relay Data

Remote users of the data available in relays include people and processes within utilities, independent system operators, customer facilities, consultants, and vendors. Protection is enhanced by getting relay data directly to these users rather than leaving it uncollected or pushing it all to a centralized data warehouse. Once in the warehouse, the user must use extraction techniques to find and acquire the appropriate data. The variety of uses for the data is comprehensive and growing.

- Communications-assisted protection – Mirrored Bits® communications, POTT, DCUB
- Coordinated protection logic – adaptive relaying via settings groups
- Distribution automation – isolation, sectionalization, and restoration
- Substation automation – breaker failure, reclosing, and battery monitoring
- SCADA – operator control and supervision
- EMS – load flow, voltage control, and generation control
- Metering – revenue accuracy for billing or validation
- Power system disturbance analysis – forensic evaluation of an event and the system response
- Power quality – comparing actual power system values to their ideal
- Protection quality – measure fitness of system devices to perform protection
- Sequence of events analysis – system-wide evaluation of events in sequential order
- Power system planning – analysis of power system values to aid operations and expansion

A. System Automation and System Integration

System automation is the control of apparatuses and processes via I&C devices to take the place of the human functions of observation, decision, and action. Substation automation refers to using intelligent electronic device (IED) data within the substation and control commands from remote users to control the power system devices within the substation.

System integration is the act of communicating data to, from, or between IEDs in the I&C system and remote users. Substation integration refers to combining data from the IED's local to a substation so there is a single point of contact in the substation for all the I&C data. Remote and local substation

control is then mediated by this single point of contact. Since true substation automation relies on substation integration, the terms are often used interchangeably. There is often a need for multiple single points of contact to serve multiple user connections or provide redundancy. The single point of contact is an I&C device acting as a client/server, programmable logic platform, gateway, router, dial-out device, communications switch, time-synchronization broadcaster, or a combination of these.

The communications industry uses the term client/server for a device that acts as a master, or client, retrieving data from some devices and then acting as a slave, or server, sending this data to other devices. The client/server collects and forwards data dynamically. A data concentrator creates a substation database by collecting and concentrating dynamic data from several devices. In this fashion, essential subsets of data from each IED are forwarded to a master through one data transfer. The data concentrator database is used to pass data from one IED to another when they are not connected peer to peer. Most RTUs and programmable logic controllers (PLC) rely on messages from a master to collect data from one IED and pass it to another through the RTU or PLC. Designs that rely on this master connection cannot share data between IEDs when this connection is lost. The IEDs become stranded and do not work in a coordinated manner. The data concentrator creates an autonomous coordinated protection system within the substation that does not rely on a master connection.

A substation archive client/server collects and archives data from several devices. The archive data are retrieved when it is convenient for the user to do so. A programmable logic platform executes custom automation logic equations. A gateway converts conversations from one protocol to another. Router is another term from the communications industry that refers to a device that routes data in transit between source and destination. A dial-out device initiates conversations or triggers paging from the substation to a remote user. Uses for dial-out include assuring connection security, eliminating the need for a dedicated communications connection, and performing unsolicited indication of a disturbance with fault location. A communications switch is the single point of contact for remote users to make a direct connection to all substation IEDs individually. The user initiates a dynamic conversation with a specific IED and the port switch merely "passes through" the conversation. In order to synchronize the IED clocks, a device in the substation needs to generate, or acquire from an external source, a time value and then broadcast it to the IEDs.

Products from many industries are used to perform substation automation, including RTUs, port switches, meters, bay modules, and protocol gateways from the SCADA industry, PLCs from the process control industry, relays and communications processors from the protection industry, and PCs from the office environment.

Substation controller and bay controller are terms commonly used to refer to devices that perform data acquisition and control of IEDs and contain local I/O. The communications processor is the only substation controller that can perform all of the substation automation tasks. The communications processor is also the only device that is designed to meet the same harsh environmental conditions as the relays themselves. SCADA and process control industry products are not designed to meet these environmental standards.

When choosing the best new and in-service devices to create a successful I&C system, it is often necessary to select from multiple vendors and also multiple vintages or generations of products. Many of these devices employ proprietary communications and interfaces. Most substation controllers must have embedded software, written specifically to communicate via proprietary interfaces. The communications processor can communicate most relay protocols, or communication languages, without developing vendor-specific protocol software for each type of relay installed. Instead, through database settings, pertinent subsets of these protocols are communicated to the relay from the communications processor for data acquisition and control. The communications processor can also eavesdrop on conversations between two devices in the I&C system, capture, and store the data.

The communications processor simplifies implementation through autoconfiguration. This process automatically determines the proper baud rate to communicate with the connected relay as well as start-up parameters, device type, and capabilities.

Some substation controllers accommodate substations of varying size as well as redundant designs by supporting peer-to-peer and tier-to-tier functionality. Peer-to-peer refers to the direct data transfers between devices functioning in a similar capacity. Tier-to-tier refers to devices that can transfer data while connected such that one is the client and the other the server.

Table I presents the system integration and automation functions required in a substation. Comparison is made of devices commonly used in substation automation and the functions that each device commonly performs.

TABLE I
SUBSTATION AUTOMATION DEVICE COMPARISON

	Communications Processor	RTU	Bay Module	PLC	PC	Port Switch	Satellite Clock
Client/Server for Dynamic Data	✓	✓	✓	✓	✓		
Client/Server for Archived Data	✓				✓		
Data Concentrator	✓				✓		
Programmable Logic Platform	✓	✓	✓	✓	✓		
Protocol Gateway	✓	✓	✓	✓	✓		
Router	✓				✓		
Dial-Out	✓				✓		
Communications Switch	✓	✓			✓		
Time-Synchronization Broadcast	✓				✓	✓	
Local I/O	✓						✓
Emulate Protocol Messaging	✓	✓	✓	✓			
Eavesdrop Communications	✓				✓		
Autoconfiguration	✓						
Tier-to-Tier	✓						
Peer-to-Peer	✓			✓	✓		
Substation-Hardened Design	✓			✓	✓		

Substation integration enhances protection by migrating some of the communications functions to an intermediate substation device performing some or all of the functions listed above. The resources available within the relay can be focused on optimizing protection solutions. Also, as protocol requirements change in the substation, a single device acting as a client/server can be upgraded instead of each of the relays individually. This obviously enhances protection because the relays are left undisturbed and in service while a protocol change is made in the client/server. It is also more economical to make this change in a single device.

Many older IEDs in substations are still useful but lack the most recent protocols. Rarely is a substation integration upgrade project undertaken where all existing IEDs are discarded. A communications processor that can communicate with each IED via a unique baud rate and protocol extends the time that each IED is useful. Using a communications processor for substation integration also easily accommodates future IEDs.

V. DATA USAGE CONSIDERATIONS

A. Methods of Communicating With Relays

Direct connect and multidrop are two types of data link connections. In a direct connection, there are only two devices connected via a transmit and receive pair of conductors. Each conductor is used to transmit from one device and receive by the other device. Since there are only two devices, each of them can constantly control the conductor on which they are transmitting and both can know implicitly to which other device they are connected. Direct connections to many relays would allow each of them to communicate simultaneously. Many direct connections originating from one device are called a star network. Fig. 1 illustrates the star topology. Many star networks can be connected in a parallel or vertical hierarchy. Any protocol can be used in this configuration. Virtually all microprocessor-based relays have a simple EIA-232 serial port connection to support direct connections. Any of the other communications methods can be used in a direct connection as well.

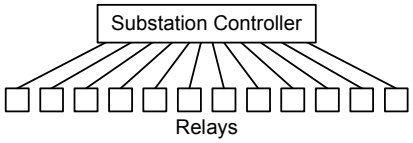

Fig. 1: Star Topology

Direct connection designs allow the network to support a wide range of relay capabilities. Simple, slow communicating devices can coexist with more complex fast communicating relays.

Open architecture is a term that refers to networks that are interoperable among vendors. The star network is the only design that is truly open and accommodates multiple protocols, multiple baud rates, and multiple network interfaces.

In a multidrop system, several devices are physically connected in a bus or ring network and must negotiate control of the transmit and receive conductors. Fig. 2 illustrates relays connected in a bus topology, and Fig. 3 illustrates relays connected in a ring topology. A multidrop connection requires that only one relay communicate at a time. Software and hardware are used to determine which device has permission to transmit so that data do not collide on the conductor. Since several devices are connected, addressing is necessary within the protocol to identify the source and destination of the data

being communicated. This addressing adds overhead in the form of processing time and amount of information that needs to be transmitted, thus reducing the amount of data that can be transferred at a given speed. Devices compensate for this by increasing the speed at which they communicate and increasing the amount of communications processing that they perform. Troubleshooting communication problems on a multidrop network is difficult. Messages from many sources must be captured and deciphered. Direct connections are quickly and easily verified using simple (light-emitting diode) LED indication.

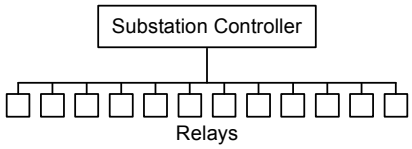

Fig. 2: Bus Topology

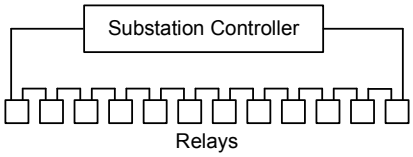

Fig. 3: Ring Topology

Relays have varying memory and computational capacities and, therefore, varying protocol support capabilities. Interactions on a multidrop network must be done at the lowest common denominator, and all devices must support the same baud rate and physical network connection.

It is important to keep in mind that, except for some redundant fiber networks with counter rotating tokens, if the mediation of control of data transmission fails, none of the multidropped devices can communicate. This can be caused by relay communications hardware failing to release control, relay communications software failing to process mediation schemes correctly, or corruption of the network.

A common multidrop option is EIA-485, which is a twisted pair network "daisy-chain" connection between multiple devices. EIA-232 connections can be converted to EIA-485 for use on some multidrop networks. Other copper and fiber connections are being developed to support standard interfaces like Ethernet as well as proprietary interfaces.

A broadcast multidrop is a common network that differs in function and purpose. One-sided conversations simply can be sent to multiple receiving devices that do not respond. Inter-range instrumentation group (IRIG) time-synchronization messages are often sent to relays in this fashion. Separate connections on the relay for this purpose are often necessary.

B. Prioritization of Data

The most direct way to transfer each data type would be over a single-purpose, uninterrupted conversation with the remote user who has a need for it. To do this, the relay would need to have up to eight simultaneous conversations. Obviously, there are more types of data than connections to a relay and some data cannot wait for the relay to perform eight consecutive conversations. Relays accommodate these restraints by prioritizing data, grouping multiple data types into a multipurpose conversation, and supporting multiple simultaneous conversations.

Protection data, for the purposes of security, reliability, and speed, are highest priority and should be transferred via a single-purpose conversation on a channel dedicated to this purpose alone. Metering, system automation, control, supervisory, and device diagnostic data are all of similar priority, second only to protection data, and are often grouped into one multipurpose conversation. This multipurpose conversation is often referred to as a SCADA connection. Historical and settings data share the lowest priority and continue to be transferred via individual single-purpose conversations.

Since the multipurpose conversation and the historical and settings conversations must be supported individually, the multipurpose conversation must, in most cases, be terminated to start a historical or settings conversation and restarted after the data transfer is complete. This is often unacceptable because visibility and control of the relay are suspended during this time. Some newer protocols are being developed to support the transfer of historical and settings data within the multipurpose data transfer. This will be useful but will require significant data transfer speeds and sophisticated processing to assure that control and visibility of the relay are maintained. Another possibility is to have multiple communications channels installed and connected to each relay for each conversation. This is often unacceptable due to complexity and cost.

Interleaved data streams are a simple innovative way that multiple conversations can occur simultaneously. Multipurpose, historical, and time-synchronization conversations can occur simultaneously on a single communications channel. Control of the relay and data acquisition are prioritized. The meter, system automation, control, supervisory, and device diagnostic conversation occurs deterministically or in a predictable fashion. An IRIG signal is broadcast in a deterministic fashion, and historical and settings conversations are interleaved as time permits. The amount of communications bandwidth available for the historic and settings conversations is determined dynamically and allocated accordingly. In other words, whatever communications channel idle time is available, after the multipurpose and IRIG messages have been sent, is used to transmit historical or settings conversations. The remote receiver of the data is expecting interleaved communications and collects the history or settings data nondeterministically or in a nonpredictable fashion based on channel availability. When the I&C system is extremely busy, a historical or settings conversation may have noticeable delays due to the reduced communications bandwidth available. This is acceptable as an alternative to losing visibility and control of the relay or installing expensive and sophisticated communication that would be necessary otherwise.

C. Data Transfer Rate Considerations

The rate at which the data need to be transferred from or to a relay depends on the relay communications hardware, the communications channel, remote uses and sources of data, and intermediate destinations for the data within the substation.

A protection data connection performs communications-assisted protection, including MIRRORED BITS communications, POTT, and DCUB. These functions perform optimally if data can be transferred every device processing interval (1 to 12 ms).

The multipurpose data connection is used by coordinated protection, SCADA, EMS, DA, and substation automation processes and operators. These processes require that the data transfer at various rates, but operators rarely digest and respond to data more frequently than every 2 seconds. Older SCADA, EMS, and DA systems actually request data every several minutes due to the technology available when they were installed. Therefore, the frequency at which the multipurpose data must be transferred varies between 0.2 seconds and 5 minutes.

Historical and settings data transfers are usually performed on an as-needed basis. Rarely is the transfer rate an issue. These data are often collected as a background task and made available at the user's convenience or they are transferred over a direct dynamic link and need only travel at the rate that an operator can digest and react to the information. This transfer rate may be further slowed to accommodate an interleaved multipurpose connection.

D. Data Transfer Considerations

Popular substation integration protocols support the multipurpose connections described above. Many can be supported on simple EIA-232 connections that exist on virtually every IED. They do not require network-specific hardware or processing. These include:

- Vendor-specific open protocols
  - SEL interleaved binary, ASCII, and IRIG
  - Modbus®
  - MV-90
- Vendor-specific closed protocols
  - Many vendor-specific protocols
- Standard open protocols governed by committee
  - ASCII
  - DNP 3.0
  - IEC 870-5 family
  - UCA

An industry-accepted standard protocol is one that is governed by committee to be described and maintained sufficiently so that multiple vendors can use it and be interoperable. Protocol standardization does not mean that a substation communications network design should use only one protocol. Some of these protocols may soon be available on Ethernet and other high-speed connections as vendors develop this functionality.

Some other popular protocols require a specific communications connection and processing hardware and vendor-specific integrated circuits or software licenses. These include:

- Vendor-specific open protocols
  - Modbus Plus™
- Vendor-specific closed protocols
  - There is a trend to move many vendor-specific protocols to Ethernet
- Standard open protocols governed by committee designed to exist on Ethernet
  - File Transfer Protocol (FTP)
  - Telnet
  - UCA and MMS
  - DNP 3.0
  - IEC 870-5

Protection is enhanced, and other applications supported, as long as data can get from the relay to the remote operator or process within the appropriate time. The protocols and communications channels that are used do not concern the user but are simply tools used by the communications network designer to perform substation integration. Standard, well-defined protocols and connections make this task easier.

E. Contemporary Network Design

The popular network configurations were listed above as direct peer-to-peer, direct star, multidrop bus, and multidrop ring. Popular network channels include power-line carrier, leased line, microwave, radio, cellular, copper, and fiber. Direct peer-to-peer, star, and some multidrop networks can be supported on any of these channels. Newer multidrop networks are designed to use high-speed channels to support multiple data transfer connections. Use of these newer technologies may result in higher device and installation costs. The star network can acquire and transfer substation integration data using much slower direct connections. These direct connections are also more reliable, more robust, and less expensive.

Using methods described in [1] and [2], fault tree reliability analyses were performed on several common substation controller-based network examples. These designs represent popular networks that provide a single point of contact for the multipurpose data for 12 relays. Table II shows the relative reliability of redundant and nonredundant system designs. The communications processor is the only substation controller that transfers both multipurpose and historical data.

TABLE II
UNAVAILABILITY[1] OF NETWORK TO PROVIDE LINE DATA OR PERFORM CONTROL ACTION

	Nonredundant Design	**Redundant Design**
RTU with multidrop relay network	1368	984.2
PLC with multidrop relay network	1176	920.1
PC with multidrop relay network	3354	1650
PC with point-to-point star relay network	2936	665.2
Communications processor with point-to-point star relay network	690	660

[1]Unavailabilities x 10^{-6}

The unavailabilities of the system components are derived from publicly available MTBF sources, including vendor publications and studies performed in the workplace. It is also important to keep in mind that these values are appropriate for the normal operating environment of the product. Some PCs, PLCs, and RTUs are not designed for the harsh operating environment of the substation, and their unavailabilities are expected to rise when used in the substation. This fault tree tool is most accurate when MTBF values from a proposed vendor or from historical records are used. The fault trees are attached in Appendix 1.

F. Future Network Design

Vendors are constantly working on faster, more secure, and more reliable communications designs. Many vendors are working to create high-speed networks as well. We recognize the value of this single network interface and are actively developing products to support it. This development will likely yield an efficient, high-speed network, but it may not solve every interconnection issue.

As discussed above, relay data have different users, destinations, functional groupings, transfer rate requirements, and reliability requirements. A network capable of transferring all of the data from a relay would need the following qualities.

Speed. Since the network will not be able to anticipate the type of data it is transferring, it will need to transfer all data at an incredibly high transfer rate so that regardless of other data traffic, the protection data will reach the destination in 1 to 12 ms. Protection processing also requires that these data be transferred at a specific frequency or deterministically. Careful calculation can provide a deterministic transfer time once the data are on the network, but a multidrop network cannot be explicitly deterministic from device to device because each device has to negotiate permission to transmit. Essentially, each device must wait until the network is idle to transmit. It is possible that multiple devices will recognize that the network is idle and attempt to transfer simultaneously, causing a data collision. Carrier-sense multi-access with collision detection (CSMA/CD) processing must be performed to negotiate data transfer at each IED and recover from data collisions. Determinism is approximated by restricting the data transfer load on the network so that a worst-case scenario of data transfer will not jeopardize the network throughput. Traditionally, the load is maintained well below 15 percent of the total network capacity.

It should also be noted that achieving the necessary transfer rates through a network connection is not sufficient. The device itself must be capable of processing data fast enough to be transferred. Few relays are capable of this today. A typical relay today makes data available for multipurpose communications every 300 to 700 ms. Therefore, although some relays can connect to a high-speed network, the data update rate at a remote destination will be much slower than the data transfer rate. A new generation of relays capable of high-speed communications processing will be necessary.

Reliability. Protection, system automation, and control data are mission critical. Therefore, a common multidrop network must transfer all data with the same reliability requirements as protection data. As mentioned above, a multidrop network must add overhead in the form of addressing and communications processing. This is an obvious contradiction to the traditional effective designs that achieve speed and reliability by transferring a minimum amount of protection data point to point. Reliable substation-grade hardware is not available to support such a network.

Cost. Many vendors are also recommending other protocols to be used on an Ethernet network. The popularity of Ethernet has made office-grade PC accessories readily available and inexpensive. However, these accessories rely on the PC CPU to perform the elaborate communications processing. This is not acceptable for a relay application; the Ethernet connectivity will have to be supported by a separate processor and not rely on the one performing protection. Ethernet components designed to meet the same harsh environmental conditions as the relays themselves will be expensive when they are available.

Network Parameters. Such a network will allow a single relay connection to perform transfer of every data type. Each relay will need to support this network, there will be no single point of contact for the substation. If the network fails, transfer of all data types is suspended. Development of substation-grade communications hardware is necessary.

VI. CONCLUSIONS

Protection is enhanced, and other applications supported, as long as the data can get from the relay to the remote operator or process within the appropriate time. The protocols and communications channels that are used do not concern the user but are simply tools used by the communications network designer to perform integration.

It is important to understand the use of information to best determine the paths it should follow in route to the appropriate destinations. Build a system by choosing relays and communications paths based on individual merit for each specific task.

Deregulation is forcing utilities to provide ever-increasing degrees of automated support. Substation automation systems are the path to meet this demand.

- The simple act of communicating a relay self-test diagnostic to a user or process drastically improves protection reliability.
- Substation integration enhances protection by migrating some of the communications functions to an intermediate substation device. Moving protocols into the relay adds to their cost and accelerates their obsolescence as technology advances. The resources available within the relay are instead better focused on optimizing protection solutions.
- MIRRORED BITS communications and other direct connections provide robust, reliable, and secure connections to transfer data that do not need to be on a centralized network.

- Metering data enhance protection by virtue of being an accurate source for protection decisions unaffected by the passage of time or changes in the environment.
- System automation, control, and supervisory data enhance protection of individual power system components as well as the entire power system by permitting rapid, well-informed decisions. Adaptive protection methods are used as the power system configuration changes dynamically.
- Device diagnostic data enhance protection by maximizing the availability of the protection system.
- Historical data enhance protection through dynamic system trend analysis as well as being the source for remote operator and process forensic analysis. By continually monitoring conditions of devices over time, operators and processes develop a clearer picture of device performance.
- Settings data enhance protection by allowing the user to configure the relay to perform optimally in many unique applications. Settings groups allow the protection system to change dynamically to compensate for changes in the power system or I&C system. Also, the ability to quickly configure replacement relays further reduces the unavailability of the system protection.
- A substation controller is often called upon to act as a client/server, data concentrator, substation archive, programmable logic platform, gateway, router, dial-out device, communications switch, and time-synchronization broadcaster. The communications processor is the only device that can perform all of these functions.
- The communications processor can communicate without developing vendor-specific protocol software and can eavesdrop on conversations between two devices in the I&C system.
- Star networks can acquire and transfer substation integration data using much slower direct connections. These direct connections are also more reliable, more robust, and less expensive.
- The communications processor simplifies implementation through autoconfiguration. This is similar, though not as comprehensive, to current efforts by the UCA forum to define this function.
- Direct connection designs allow the network to support a wide range of relay capabilities. Simple, slow communicating devices can coexist with more complex fast communicating relays.
- The star network is the only design that is truly open and accommodates multiple protocols, multiple baud rates, and multiple network interfaces.
- Communications processors enhance the value of the protection I&C system data by making it available to multiple master systems and other users.
- Substation integration designs that rely on a master connection cannot share data between IEDs when this connection is lost. The IEDs become stranded and do not work in a coordinated manner. The communications processor creates an autonomous coordinated protection system within the substation that does not rely on a master connection and allows mediation of local or remote control of the entire substation.
- SCADA and process control industry products are not designed to meet the same harsh environmental conditions as relays and communications processors.
- As protocol requirements change in the substation, a single device acting as a client/server can be upgraded instead of each of the relays individually. The relays are left undisturbed and in service as a protocol change is made in the client/server. It is also more economical to make this change in a single device.
- The age of IEDs that are in substations today varies widely. Many of these IEDs are still useful but lack the most recent protocols. Rarely is a substation integration upgrade project undertaken where all existing IEDs are discarded. A communications processor that can communicate with each IED via a unique baud rate and protocol can extend the usefulness of IEDs. Using a communications processor for substation integration also easily accommodates future IEDs.
- Networks are made up of direct and multidrop connections. Point-to-point star networks are much more reliable than multidrop networks. It is important to keep in mind that if the mediation of control of data transmission fails, none of the multidropped devices can communicate.
- Interleaved data streams are a simple innovative way that multiple conversations can occur simultaneously. Multipurpose, historical, and time-synchronization conversations can simultaneously occur on a single communications channel.
- A simple communications processor star network and point-to-point relay protection connections with serial channels can perform similar to the UCA 100 Mbit network expectations.
- Troubleshooting communications problems is much faster and more efficient through simple LED indication on direct links than attempting to decipher multidrop networks.
- Protocol standardization does **not** mean that every relay must use the same protocol; it means that each protocol must be explicitly defined to support interoperability.

VII. Appendix 1

As described in detail in references [1] and [2], a fault tree is tailored to a particular failure of interest and models only that part of the system that influences the probability of that particular failure. The failure of interest is called the top event. Consider the top event "Cannot Read Line Data or Control Breaker." For this example, system reliability is quantified by comparing system unavailabilities. The unavailability of each system is created by combining the unavailability of system devices that would cause the I&C system to be unsuccessful in either operating the breaker or acquiring the associated line data. System unavailabilities can then be compared to give the relative reliability of each design.

AND gates represent a combination of components where all must simultaneously be failed in order to cause the top event. The unavailabilities of these components are multiplied together to get their combined unavailability.

OR gates represent a combination of components that can individually cause the top event. The unavailabilities of these components are added together to get their combined unavailability. The unavailability values on the fault trees are displayed without the x 10^{-6} for clarity.

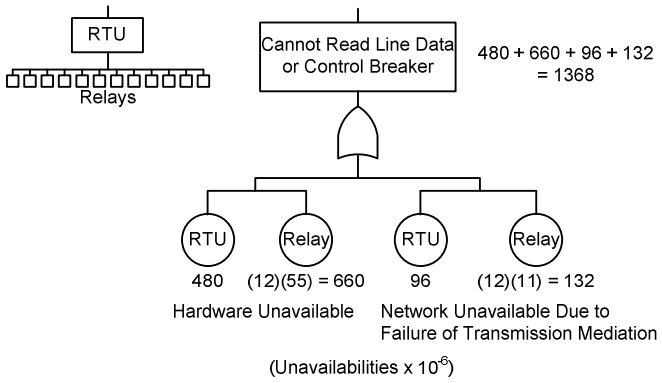

Fig. 4: RTU Multidrop Example – Nonredundant Design

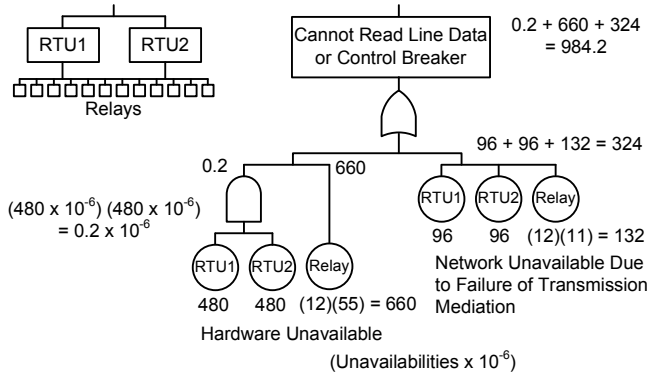

Fig. 5: RTU Multidrop Example – Redundant Design

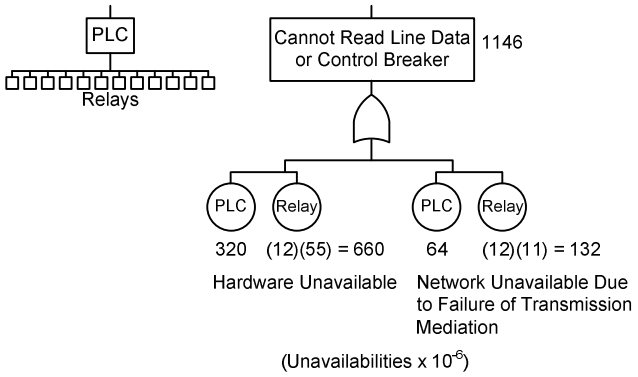

Fig. 6: PLC Multidrop Example – Nonredundant Design

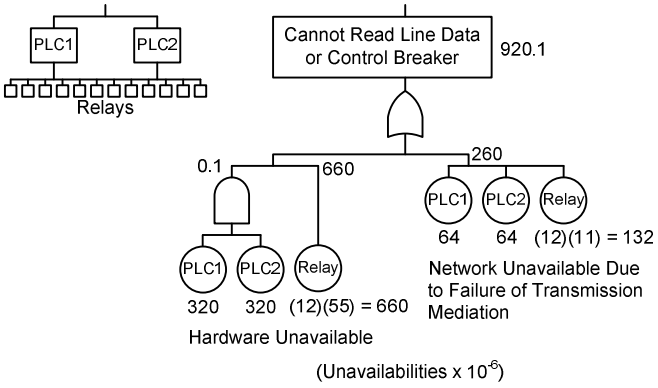

Fig. 7: PLC Multidrop Example – Redundant Design

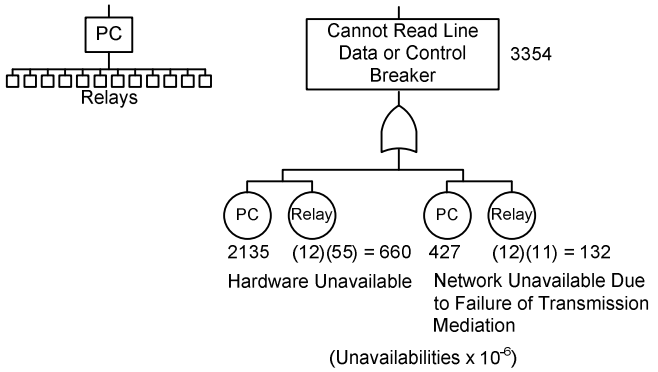

Fig. 8: PC Multidrop Example – Nonredundant Design

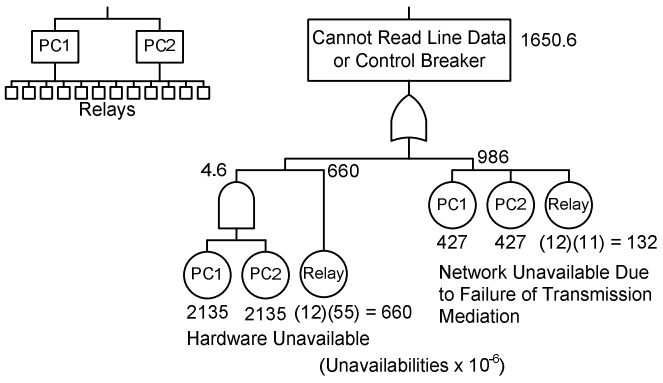

Fig. 9: PC Multidrop Example – Redundant Design

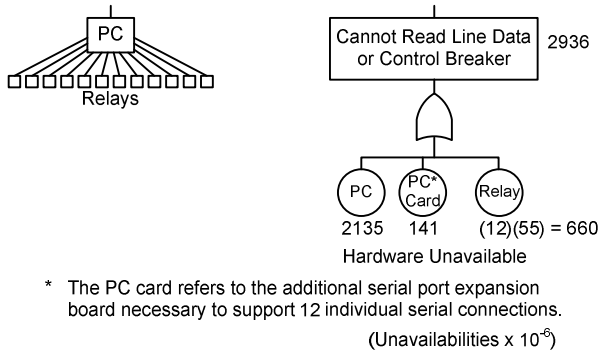

Fig. 10: PC Star Example – Nonredundant Design

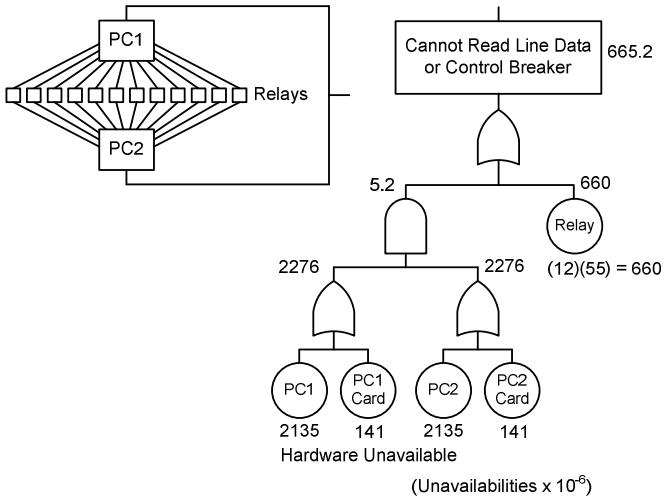

Fig. 11: PC Star Example – Redundant Design

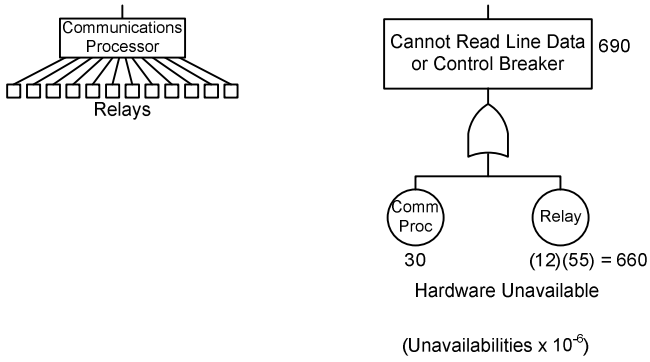

Fig. 12: Communications Processor Star Example – Nonredundant Design

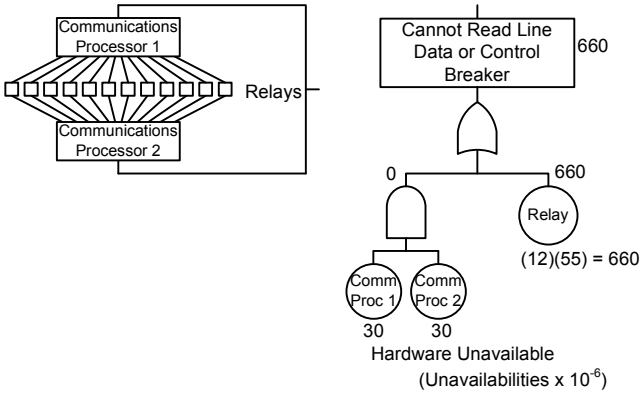

Fig. 13: Communications Processor Star Example – Redundant Design

VIII. References

[1] E. O. Schweitzer, III, Bill Fleming, and Tony J. Lee, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," proceedings of the 24th Annual Western Protective Relay Conference, Spokane, WA, October 21–23, 1997.

[2] Gary W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," proceedings of the 4th Annual Substation Automation Conference, College Station, TX, April 8–9, 1998.

IX. Biographies

David J. Dolezilek received his BSEE from Montana State University in 1987. In addition to independent control system project consulting, he worked for the State of California, Department of Water Resources, and the Montana Power Company before joining Schweitzer Engineering Laboratories, Inc. in 1996 as a system integration project engineer. In 1997, Dave became the Director of Sales for the United States and Canada, and he now serves as the Engineering Manager of Research and Development in SEL's Automation and Communications Engineering group. He continues to research and write technical papers about innovative design and implementation affecting our industry, as well as participate in working groups and technical committees. He is a member of the IEEE and the International Electrotechnical Commission (IEC) Technical Committee 57.

Dean A. Klas received his BSEE from the University of Wyoming in 1984. After graduation, he worked as a development engineer in the defense industry for Texas Instruments, Martin Marietta, and EG&G, Inc. He joined Schweitzer Engineering Laboratories, Inc. in 1992 as a development engineer and has been part of the development team for several relays and PC software packages. He currently is a Development Engineering Manager for SEL's Automation and Communications Engineering group.