

IEC 61850

A Practical Application Primer for Protection Engineers

Bogdan Kasztenny, James Whatley, Eric A. Udren, John Burger, Dale Finney, Mark Adamiak

1. What IEC 61850 is, and what it is not

Substations designed in the past made use of protection and control schemes implemented with single-function, electromechanical or static devices and hard-wired relay logic. SCADA functions were centralized and limited to monitoring of circuit loadings, bus voltages, aggregated alarms, control of circuit breakers and tap changers, etc. Disturbance recording and sequence-of-event data if available was centralized and local to the substation.

With the advent of microprocessor-based multi-function Intelligent Electronic Devices (IEDs) came the opportunity to move more functionality into fewer devices; resulting in simpler designs with reduced wiring. In addition, owing to communication capabilities of the IEDs more information could be made remotely available; translating into fewer visits to the substation.

Microprocessor-based protection solutions have been successful because they offered substantial cost savings while fitting very well into pre-existing frameworks of relay application. A modern microprocessor-based IED replaces an entire panel of electro-mechanical relays with external wiring intact, and internal dc wiring replaced by integrated relay logic. Users retained total control over the degree of integration of various functions, while interoperability with the existing environment (instrument transformers, other relays, control switches, etc.) has been maintained using traditional hard-wired connections. Distributed functions are rare, and restricted mainly to the SCADA realm.

In terms of SCADA integration, the first generation of such systems achieved moderate success especially in cases where the end-user could lock into a solution from a single vendor. Integrating systems made up of IEDs from multiple vendors invariably led to interoperability issues on the SCADA side. Integration solutions tended to be customized. Owners of such systems were faced with long-term support and maintenance issues. During this period two leading protocols emerged: DNP 3.0 and IEC 60870.

Beginning in the early 1990s, initiatives were undertaken to develop a communications architecture that would facilitate the design of systems for protection, control, monitoring, and diagnostics in the substation. The primary goals were to simplify development of these multi-vendor substation automation systems and to achieve higher levels of integration reducing even further the amount of engineering and wiring required. These initiatives have culminated in the release of EPRI-sponsored Utility Communications Architecture, or UCA, specification, a precursor of the 61850 international standard. After decades

of competing protocols and integration challenges, 61850 was created by an International Electrotechnical Commission working group consisting of vendors, utilities, and consultants who were focused on the development of a standard in which devices from all vendors could be connected together to share data, services, and functions.

The vision of 61850 is extremely broad. While starting with a next generation SCADA protocol, the concept encourages and facilitates advanced applications in protection and control, to the extent of blending in non-conventional CTs and VTs into the overall scheme by providing for a standardized way of exchanging information digitally between the producers and recipients of this information. The "61850" phrase became a designator for the next generation substation system with a higher degree of integration, reduced cost, greater flexibility, communication networks replacing hard-wired connections, plug-and-play functionality, reduced construction and commissioning time, and other advantages. While many of these benefits are delivered by the SCADA part of the 61850 alone, there is an expectation that the other visionary elements of the package are also mandatory and ready for extensive deployment.

The 61850 Standard makes extensive use of the concept of virtualization. Data that is produced by IEDs is presented in a standardized format. In this way IED functions become generic from the point of view of the system designer but the underlying functions retain vendor specific characteristics that may be unique and proprietary in nature. The available data is also logically partitioned according to groupings that should be familiar to relay and SCADA engineers (protection, metering, supervisory control, etc.). The data is "self describing" in nature, obviating the need for memory maps and allowing the integrator to "browse" a device for the needed data. Presented data have attributes that are common across vendor platforms.

Additionally, the 61850 series standardizes the mechanisms by which data is accessed and exchanged within the substation. The IEC 61850 concept standardizes SCADA data and services, as well as encourages peer-to-peer exchange of information between the IEDs: Included are mechanisms for reporting and logging of information, mechanisms for passing critical messages such as tripping signals between devices, and mechanisms for transfer of voltage and current samples from process-level devices (microprocessor-based CTs & VTs) to protection devices. The design of automation functions requires a considerable amount of configuration of the constituent IEDs. Currently, when building multi-vendor automation systems, the designer is confronted with one or more configuration tools from each vendor. The 61850 series addresses this by defining a description language for substation configuration (Substation

Configuration Language, SCL). SCL permits the development of tools that can be used to describe the substation at a high level (single line diagram). These tools are also envisioned to configure reports/logs, control commands, critical peer-to-peer messages and sampled analog values. Vendor specific configuration tools must interface with system level tools using standard SCL files.

While the 61850 series facilitates the implementation of functions (protection schemes, control schemes, etc.) that are distributed amongst several IEDs (possibly from different vendors), the specification does not attempt to standardize the functions themselves in any detail. It is left to the end user to impose his or her own engineering practices and philosophies to the particular application. Correspondingly, the 61850 Standard makes few requirements as to which data models and data items are to be made available in a particular IED. The allocation of data models as well as much of the data that makes up the models is left to the IED vendor. This creates a potential disconnect between the vendor and the end-user. It is therefore critical for the system designer to carefully check specifications when selecting IEDs.

Similarly, the 61850 Standard details the attributes of the data exchanged between devices. These attributes include information on the quality of the data and information on the operating state of the source of the data (for example, normal versus test). Decisions on the response of a function that is presented with degraded data are outside the scope of the Standard. Additionally, the Standard permits the configuration of timing priorities for messages passed between devices. It is, for the most part, left to the designer to determine what level of priority is required for the application.

The Standard defines the description language (SCL) to be used by configuration tools, while the functionality of the tools themselves is outside the scope of the Standard. More importantly the overall engineering processes are not defined and are likely to be different than those of the past. Much of the IED settings will remain in the domain of the manufacturer specific IED configuration tool. There will (at least initially) be some conflicts created. Undoubtedly, engineering processes and the corresponding configuration tools will have to evolve in unison.

The IEC standard itself does not offer any particular system architecture to follow. Instead it describes several building blocks with the hope they will fit the future architecture while the latter is conceived. This is not a significant issue for functions integrated between SCADA and IEDs, but presents an obstacle for functions executed between IEDs and their remote inputs and outputs.

Some of the functions that have been implemented in the past will map easily into the IEC 61850 domain. Others will not. In some cases, long-held, underlying principles of system protection will have to be re-examined.

This paper seeks to identify significant issues arising as deployment moves forward, presents possible solutions in some

cases and gives direction for further investigation in others.

2. Industry Trends and Expectations

Today's utilities are under considerable cost pressure. In the realm of protection and control, modern microprocessor-based multi-function devices offer great savings by simplifying panel design, eliminating a number of traditionally installed devices and associated wiring, eliminating RTUs, and simplifying substation SCADA systems.

The cost of a device providing a complete set of Protection and Control (P&C) functions for a given zone of protection has dropped dramatically in the last two decades. Nonetheless, the cost of a finished installed panel with primary and backup protection and independent breaker fail / autoreclose relay still remains in the 50 to 100 thousand dollar range. It is clear that vast majority of this cost is associated with engineering and field labor, and not with the cost of the raw material.

On the other hand, shortages and aging of the experienced workforce coupled with a lack of inflow of new graduates, will create a large-scale problem in the 5 to 10 year horizon. This is within the time perspective of today's utility managers who started to realize that the retrofit schedules driven by the age of the secondary equipment, availability of experienced engineering staff, and the expected cost of retrofits and new projects do not converge.

With reserve margins low in many regions of the globe, outages required to complete retrofits or integrate a new substation, are already, and will remain, difficult to obtain. There is a growing need and expectation of a substantial reduction in the duration of P&C projects.

This need has sparked discussions around new next generation P&C solutions that would reduce the engineering costs, cut the field labor, and shorten the required outage time. Many utilities have decided to set up task forces with the mandate to evaluate existing technologies and trends and to work out more efficient ways of engineering P&C systems. Quite often, the above trends and expectations are labeled "61850". In reality the IEC 61850 implies one of possible solutions by providing set of standardized building blocks, with the hope the blocks will fit the future P&C architecture.

Means to achieve the benefits of the next generation P&C system include eliminating RTUs and associated wiring in favor of using only protection IEDs as interfaces with the primary equipment, standardizing P&C designs for better re-usability, deploying pre-assembled and pre-tested drop-in control houses, simplifying designs by migrating auxiliary devices such as control switches, annunciation, metering and other functions into protection IEDs, replacing stand-alone Digital Fault Recorders (DFRs) and Sequence of Events (SOEs) recorders with distributed records collected from protection IEDs, migrating all substation communication into a single media of Ethernet, etc. This alone allows for substantial cost savings and is being successfully implemented by many utilities using modern IEDs

and existing SCADA protocols for integration and automation.

It seems, however, that under the cost and manpower pressure, the industry is getting ready for more aggressive steps beyond what is being done today by forward-looking utilities. Replacement of switchyard wiring with plug-and-play fiber-based solutions, replacement of inter-IED wiring including critical protection signaling with peer-to-peer communications, real-time sharing of processed analog signals between IEDs for further elimination of the hardware that interfaces with the primary equipment are discussed.

Substantial cost is associated with copper wiring (\$10/point, 100 points on an average panel, tens to hundreds of meters of control cables per panel). Given the bandwidth of fiber-based signaling, the potential for plug-and-play assembly of fiber-based architectures, and much lower cost of fiber versus copper on the per signal basis, the next generation P&C solution is often viewed as eliminating “copper” and replacing it with “fiber”. At the same time, fiber technology has been constantly advancing; driven by high volume applications in both the consumer (e.g. cable TV, Internet, telecom) and industrial (e.g. transportation, factory floor automation) markets. Deploying fiber-based networks no longer requires pioneering approaches, unique skill sets, or expensive, specialized equipment. Instead, off-the-shelf relatively mature solutions have emerged for laying out, patching, and terminating fiber cables. Overall the fiber technology seems to have enough momentum to grow into mission-critical applications including the outdoor high-voltage substation environment.

Considerable cost is perceived to be associated with integration of various devices for automation and SCADA purposes. Savings are expected by migrating to a better, “next generation” protocol compared with the existing DNP 3.0 and IEC 60870. Major areas of improvement that have been identified include object orientation (organization of data), self-description of data, using single high-speed communication media (Ethernet), and better station-level configuration tools.

The leading protocols widely used today recognize the need for improvement and continue to evolve. For example, DNP can be used over Ethernet; and work is under way to incorporate some form of self-description into DNP.

The economic expectation derived from industry convergence on a single global protocol is high, regardless as to how this protocol compares with the existing multitude of protocols. All major vendors tend to operate globally these days. Opportunity to support just one substation protocol would allow them to focus better and invest more effort in a single standard solution.

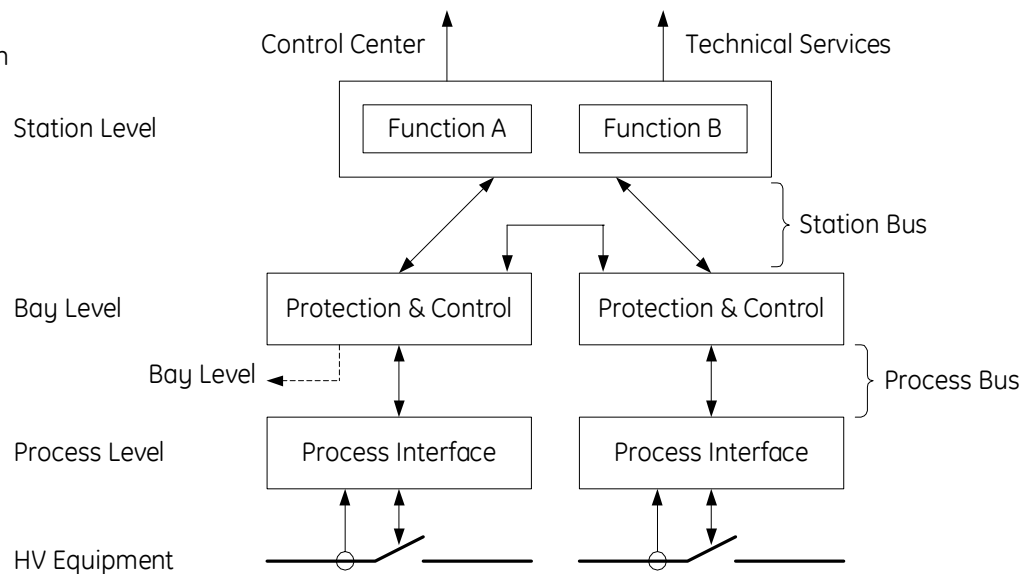
The IEC 61850 is viewed as the single answer to the above expectations and emerging trends.

3. The Vision of IEC 61850

In the beginning, the vision of IEC61850 was to define an interoperable communication system for the exchange of information between devices within a substation. Figure 1 shows the interfaces originally identified to be within scope of the Standard, specifically, process measurement (e.g. – voltages, currents, status) to device, device to station level, device to device, and device to Technical Services. Each interface brought with it different requirements for performance, Quality of Service, and reliability. Identified but not yet implemented interfaces are the Station Level to Control Center and Local Device to Remote Device (other substation) communication.

The structure chosen to implement this system was the International Standards Organization’s 7-layer communication model. Specifically, the goal was to populate each of the layers, when needed, with existing standards that met the identified functional requirements. It was recognized that different communication profiles would be needed for the various communication paths that existed between devices. The primary protocols chosen for the various layers include Ethernet, the Internet Protocol (IP), the Transmission Control Protocol (TCP),

Fig. 1.
IEC 61850 Substation Automation Interface Model.



and the Manufacturing Messaging Specification (MMS). The various profiles actually defined by IEC61850 are shown in Figure 2. Note that the device to station level link which does not have specific performance requirements, uses a traditional TCP/IP transport and network layer whereas the device to device profiles, which requires fast (<4ms) communication, uses direct mapping of the data being transferred into an Ethernet data frame.

Adhering to standard protocols used broadly in other domains brings accelerated maturity, cost savings, potential enhancements generated by other applications, and future-proofing. Being generic, these protocols create a substantial overhead. Previous generation protocols developed specifically for the power industry are much leaner and more efficient.

3.1. Standardized data models

The vision of 61850 was to not only standardize the communication mechanisms but to also define the semantics (meaning and behavior) and syntax (structure) of the data being communicated. To this end, 61850 modeled numerous real devices and functions found in the substation. These models and functions are organized into what are known as Logical Nodes (LN). A specific protection function is then modeled through the logical connection between the logical nodes that exist throughout a substation.

Another key vision of IEC61850 was the ability of a device to describe itself. Self-description allows a server (IED) to send, on request, a textual description of all the data items and attributes known to the server, allowing the client to automatically create a database of data items. This capability enables automatic configuration of multiple remote clients yielding significant time savings (in the SCADA realm) compared to existing techniques.

a distance protection function or a breaker failure function in two different 61850 implementations would use the same data types and will self-describe themselves in a standardized way, but will have different settings, different input and output signals and will respond, therefore, differently. Although the semantics of the data items are standardized, many of the functions are not interchangeable, nor they can always be configured to interact properly for protection purposes.

3.2 Standardized data access

Access to the data items was achieved through the creation of “abstract services”. These services were created independent of any specific application layer and subsequently allowed for the mapping of these services to any chosen application. The concept of abstract services makes the protocol futureproof, as it is migrate-able to whatever the future brings in the way of next generation application layers. Additionally, the layering of the other communication protocols enables migration to new technology as it becomes available. A good example of this is the fact that the present version of the Internet Protocol (version 4) is in the process of migrating to Version 6. Because of its layered implementation, IEC61850 will be able to migrate by changing out only one layer of the overall profile.

3.3 Virtual DC wiring – GSSE and GOOSE

The logical architecture of 61850 permits Logical Nodes to be distributed in multiple physical devices throughout the substation. In order to interconnect these distributed nodes, a fast, distributed, and reliable delivery mechanism was needed. The solution to meet the identified requirements is known as the Generic Object Oriented Substation Event or the GOOSE. The GOOSE was originally defined in the work for UCA and was only designed to carry binary status information (virtual dc wiring over Ethernet LAN). In the migration to 61850, the IEC GOOSE brings with it several desirable new features, namely:

- The ability to directly send analog data values
- The ability to send data via a VLAN (Virtual LAN)
- The ability to set the priority of the message through a switch

The IEC GOOSE, in contrast to the UCA GOOSE, carries a user-defined dataset. The dataset can be configured with any data object in the relay such as Volts, Watts, Vars, breaker status, etc. The data items in the dataset carry the same type (such as Float 32, Integer 16, Boolean, etc) as the original data item. In the application of transmitting power flows, data, in engineering units, can be easily transferred among multiple locations as needed.

With the UCA GOOSE, when the multi-cast packet left the station, the packet would travel anywhere there was an Ethernet switch. This resulted in GOOSE packets being delivered to more locations than they had to be. A new feature supported in the IEC GOOSE is the ability to logically restrict the flow of data to a particular broadcast domain through the creation of

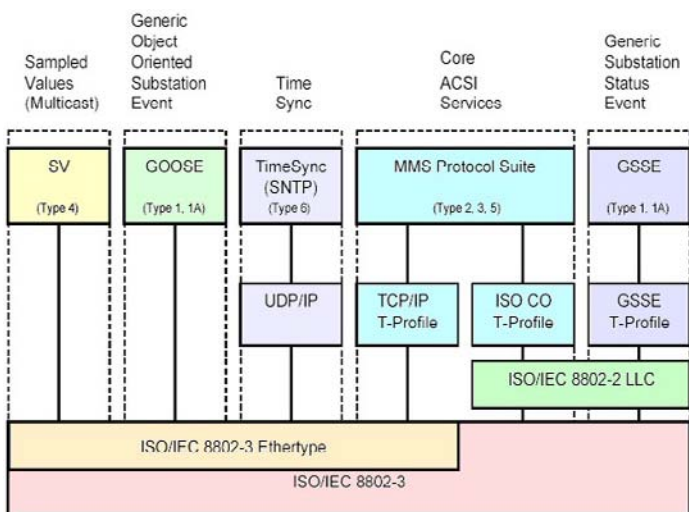


Fig. 2. IEC61850 Communication Profiles.

It is worth emphasizing in this context that the IEC 61850 creates a false illusion of standardized P&C functions. The intent was to standardize the models, i.e. organization of data, and not the data itself or ways of producing the data. For example

a Virtual Local Area Network or VLAN. This dataflow restriction is achieved by adding 4 bytes to the Ethernet data frame per the IEEE 802.1Q standard. Once identified as an extended Ethernet frame, a device (switch/bridge-router) in the network can decode the VLAN ID or VID. This ID is read by the device and directed to those ports programmed with the same VLAN ID thus partitioning the physical network into logical sub-networks.

The third area addressed by the IEC GOOSE is that of Ethernet Priority in communication. Ethernet has traditionally been known as “non deterministic” in that collisions on a shared wire made the delivery time of a message a random variable. With the introduction of Layer 2 full-duplex switch technology, Ethernet collisions no longer exist. Switches receive all messages and store and forward them to the destination locations as programmed. It is possible for a single port to have several messages queued for delivery which would add a certain amount of delay in the processing of a message. Ethernet Priority, however, even removes this delay in most cases. Upon receipt of an Ethernet message with high priority, the received message is moved into a high-priority queue and messages in the high-priority queues are sent before those in the lower priority queues resulting in a higher Quality of Service for the GOOSE messages. However, potential delays of critical messages such as GOOSE/GSSE, all with the same high priority assigned, could be a factor. Guidance for using the provided priority mechanisms and testing to validate the desired performance are not defined yet.

GOOSE messages incorporate quality and test bits. The former are meant to signify the “goodness” of data; the latter are meant to facilitate testing of distributed schemes. The Standard, however, does not mandate the creation of or the response to those bits, leaving such issues to the user.

GOOSE messages typically incorporate channel monitoring by a simple method of sending messages even in the quiescent state. If a message does not arrive in a pre-defined window, communication loss is declared and the incoming signals are replaced by pre-defined values including on, off, last valid, etc.

The UCA binary GOOSE triggered transmission upon state change. Similarly, the IEC GOOSE specifies that a GOOSE message is to be triggered not only on a status change but also on a data change (i.e. – change of an analog value greater than the dead band setting for the data item).

3.4 Virtual AC wiring – Sampled Values

One of the most forward-looking elements in the IEC61850 vision is that of providing an interface between the “process” of voltage, current, and status measurement and the protection and control devices in the substation. This interface is defined in the Standard as the Process Bus. IEC61850 defines how samples of voltage and current can be transmitted over an Ethernet communication channel.

The primary driver for this interface is the continuing emergence of non-conventional current and voltage transformers. Although available for over 15 years, the general

adoption of such devices has been stymied – according to some – for lack of an inter-operable solution.

The concept of a Process Bus has a wider application, though. If elimination of copper field wiring is a target, there will be a need to digitize the raw process information in the switchyard, close to the primary equipment, and ship it digitally between devices in need of this information. This applies to traditional CTs and VTs as well as other mostly binary (on/off) information in the yard. This capability is essential for success of the process bus concept, since the utility industry cannot make a business case for replacement of all the existing instrument transformers at the same time that protection and control systems in the control buildings are being upgraded.

It seems that the existing version of the Process Bus (Parts 9-1 and 9-2) is primarily driven by a much narrower application with non-conventional CTs and VTs.

3.5 Interoperable Format of IED and Substation Configuration

The 61850 Standard hints at a set of engineering tools that address various tasks required in the design and implementation of a substation automation system. These include project design, configuration and documentation tools. The Standard does not attempt to define the tools themselves. Instead, it defines a model of the IEDs and their communication services and defines a common file format for the description of this model. This standardized file format is used for the exchange of information between the various engineering software. These files have the potential to replace the schematics, wiring diagrams and point lists currently used to develop and document the substation design.

Project design tools are used in the planning stages of a substation automation system. The system designer can specify the substation primary equipment in the form of a single line diagram. The high-level functional requirements of the system are defined here as well as the signaling requirements to the primary equipment. At this point, pre-configured devices (IEDs) that will be used to implement the automation system may also be selected and assigned.

Configuration tools are used to parameterize the various IEDs to produce a working system. This task may be further broken down into the configuration of substation level functions and parameters (system configurator) and the configuration of autonomous IED parameters (IED configurator). The system configurator makes use of the specifications developed in the project design tool. The system configurator also utilizes standardized files that describe the capabilities of the IEDs. These tools also are responsible for the transfer of the configuration to the IED and for management and archiving of IED configurations.

Documentation tools are responsible for the automatic generation of standardized documentation that is specific to the substation automation project. These tools are again subdivided

into tools for documentation of the external equipment (i.e. CAD tools) and tools for documentation of IED parameters. CAD tools are used to develop AC and DC schematic diagrams for functions that are external to the IEDs and to document (list) the physical connections to the substation automation system. IED parameter documentation includes lists of signals that interface with substation equipment, internal logic, and parameters.

3.6 Envisioned Design Process for IEC 61850 P&C System

One could envision a greatly streamlined design process using the tools described in the previous subsection. The ultimate design process could be envisioned as follows:

The design standards group converts its standard substation design into a 61850 document. This file would consist of a single line diagram showing the primary equipment populated with logical nodes representing the required functionality for the substation.

The projects engineer would use this master file to create a design for a specific substation using a generic project design tool. This could entail copy-and-paste operations to add additional bays, for instance. The resulting file might become a tender document distributed to various substation automation vendors. The engineer involved in bidding would import the document into a system configuration tool and map the logical nodes to physical devices of choice. The modified file may become part of a bid document showing the location of IEDs and their associated functions.

After the project has been awarded, detailed engineering would commence. The substation integrator would import the file used for bidding into a substation configuration tool. At this level, the communications services of the IEDs would be configured for the implementation of distributed functions. Data sets could be created by drilling down into specific logical nodes to select the desired data (self-described). The resulting GOOSE messages could interconnect devices through a simple drag-and-drop process. Report applications (SCADA) and sampled value applications (process bus) would be implemented in a similar fashion.

After all system level functions have been implemented, the output file would be exported to the IED configuration tool. Here the remainder of the IED parameters would be configured. The output file from the IED configurator would be ready for download into the IED and could be used to automatically generate the documentation for the project.

The above describes a process in which little engineering effort is duplicated or repeated, and the entire project is delivered in an electronic format that starts as a bidding document and grows into detail design equivalent to IED settings as it goes through various design stages.

4. Unanswered Questions – What’s Missing?

From the beginning, the scope of the IEC 61850 project was to define a protocol for the communication of information. Specifications for the actual design, commissioning, operation and maintenance aspects of a complete system architecture appropriate for integrated substation applications were not part of the scope. This section will attempt to highlight some of the areas where further development is required in order to facilitate delivery of a complete, working system capable of utilizing the vision of IEC 61850.

4.1 High-Level Requirements for Next Generation P&C System

Given the way protection and control systems are deployed and operated today, the following are highly desirable features of the anticipated next generation protection solution. The following statements apply mainly to the protection aspect, and not to the relatively complete, and mature client-server (SCADA) portion of the 61850 set of protocols. A key element in any design is to first establish the basic functional requirements; these in turn will permit development of appropriate solutions. The following items are intended to address some of these requirements:

Availability. The protection architecture of an integrated system shall have availability equal or better than today’s systems. Given the extremely high reliability of instrument transformers, connecting cables, and interposing/lockout relays, today’s availability is primarily driven by the failure rates of multi-function IEDs, and is expected to be in the range of 100 years of MTTF. There is a dramatic impact of the count of electronic devices comprising a fully integrated system (“merging units”, Ethernet switches, time synchronization sources) on the availability of the system. A successful architecture will have to be engineered to retain equivalently high availability regardless of the number of devices in the scheme. Not meeting this requirement will be damaging to the concept and its present momentum, and may result in erasing all initial savings by increasing the subsequent cost of ownership.

Cost-efficiency. Microprocessor-based relays have been adopted despite the reduced performance of early models compared with the preceding generation of static and electromechanical relays, because of their attractive initial price equation. A successful architecture will have to prove significant reduction of the total cost of installation and ownership. This shall account not only for the initial engineering, construction and material cost of a solution meeting all other requirements, availability in particular, but also for cost of maintaining extra electronic equipment that replaces virtually maintenance-free items such as cables and associated drawings, pushbuttons, interposing relays, etc. It is the cost equation that separates what is technically possible from what is eventually manufactured, given a chance to mature, and be deployed in the field.

World Class Protection Training at your Fingertips

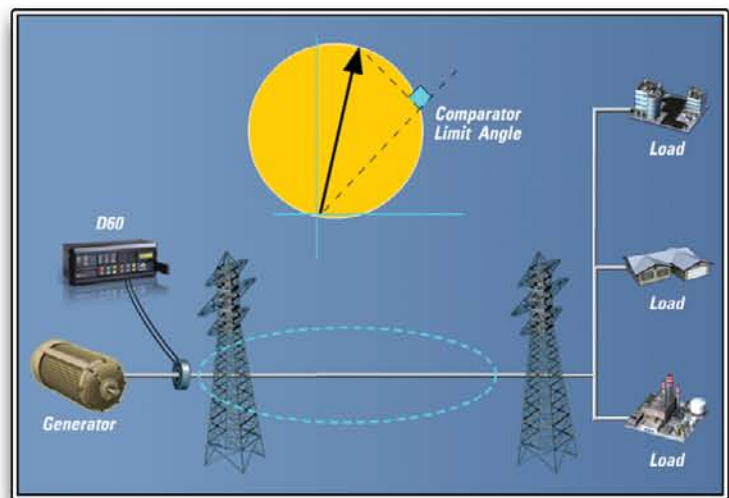


Fundamentals of Modern Protective Relaying Interactive Learning CD

- Learn at your own pace
- Review material as often as necessary
- Keep as reference material for future assistance

Topics Covered Include:

- Zones of Protection
- Distance Protection
- Generator Protection
- Line Current Differential
- Transformer Differential
- Motor Thermal Modeling
- Overcurrent Coordination
- Power System Fundamentals
- BusBar Low-Impedance Differential



Looking for More Training?

View our line of Training CD's and in-class courses at www.GEMultilin.com/training



GE Multilin

Worldwide: 905-294-6222
North America: 1-800-547-8629
www.GEMultilin.com/training

ASPEN

software

*...get the job done right, **effortlessly.***

Utilities engineering software *Proven in over 250 utilities worldwide.*

OneLiner™

Short circuit and relay coordination for transmission systems.

Power Flow™

Full-featured power flow for transmission systems.

Relay Database™

Customizable database for relay information.

Breaker Rating Module™

Checks breaker rating using IEC and ANSI/IEEE standards.

DistriView™

Load flow, short circuit, relay coordination and motor starting for distribution systems.

Line Constants Program™

Calculates electrical parameters for lines and cables.

Purpose-driven design. Implementation details, the intended focus of the 61850 Standard, are secondary compared with the challenges of architecting a robust system. The overall system design should be purpose-driven, with cost and simplification being primary targets.

Switchyard wiring offers the biggest saving opportunity. With non-conventional CTs/VTs being adopted very slowly, the practical solution for cost-efficient substitution of the yard copper wiring focuses around placing electronic devices in the yard to interface with physical secondary signals at their origin. This presents a challenging task in terms of architecting the system particularly in the area of redundancy. Presently the IEC 61850 Standard specifies that a single failure shall not take down the communication but the document does not address the issue of architectures required to obtain a high degree of availability. Additionally, issues such as stand-by data, dynamic data substitution, etc. are not addressed. Much work remains to be done to turn these concepts into reality so practical systems can be delivered.

Another significant saving opportunity is in the area of lockout relays. The Standard does not acknowledge existence of lockout relays, nor does it address the issue of practical implementation of the lockout functionality in the soft space.

Overall, the cost and simplification benefits need to drive practical architectures, and those architectures should drive the interoperability standards. When reversed, the unfortunate result may be a lack of important features and/or the introduction of concepts that will never be used.

Another aspect of a purpose-driven design is to use right tools for a given problem. This requires in-dept knowledge of protection and control engineering and must not be done from a generic and oversimplified perspective of moving real-time data between various devices. A successful system will have to be designed to overlap with and take advantage of the way the primary equipment is designed, operated, and regulated by various agencies, i.e. taking into account this particular “process to be controlled” known as a power substation.

Advancements in technology must be closely monitored and old assumptions must be critically re-visited. For example:

- With a limited number of signals belonging to a given zone of protection (characteristic of the process), and the cost of fiber being very low already (evolving technology), what is the role of Ethernet switches on the process bus level, i.e. in the real time critical network intended for protection?
- Or, assuming secondary signals are produced by traditional instrument transformers, and elimination of the yard wiring is one of the primary targets for the new architecture, while systems A and B remain independent, what is the value of interoperability for the sampled values?
- Or, if interfacing with physical signals at their origin is a part of the solution, why does the envisioned communication protocol seem to be heavily biased towards uni-directional transmission of fast analog values, instead of bi-directional transmission of

co-existing binary and analog values?

Segregation of Functions. Today’s solutions show a great degree of separation. Protection systems A and B are separated; zones of protection within each system are separated; a given zone can be protected with a single device manufactured by a single vendor; a given IED can be maintained with minimum interactions with other devices (breaker failure is a rare exception); firmware upgrades can be performed with little or no interactions with other devices; a given application can be engineered using minimal and well defined interfacing points with other applications; a given IED can be set up using a single set up software, etc. The above is too often taken for granted, but could be jeopardized when using communication-based solutions that go too far. A successful architecture will have to maintain simple separation boundaries between elements, or users will become overwhelmed with complexity and interactions while engineering their protection and control systems.

Separation of Secondary Equipment/Manufacturers. There is a practical value in limiting the number of pieces of secondary equipment interacting with one another, and reducing or simplifying the interactions themselves while fulfilling the mission critical task of protecting the power system. Today’s architectures depend on a small number of devices or signals for protection. In particular in order to protect a given zone, it is required to synchronize measurements for the few signals that bound the zone. This is done internally to the relay, and does not involve synchronization to an absolute time, or synchronization among all signals in the substation. Also, today’s solutions do not require third party devices to produce and move data required for protection. Dependency on such devices must be considered substandard in terms of overall availability of the system, complexity, separation of functions and equipment manufacturers, upgradeability, etc. and shall be avoided at all cost unless necessary to achieve a more valued goal. Today relay manufacturers attend to all sorts of underlying processes taking place in a modern relay. Such a complex product is controlled by a single firmware, tested as a whole, engineered to work optimally as a system, supported by a single set up program, and guaranteed by a single vendor. Some concepts promoted by the IEC 61850 seem to go in the opposite direction. For example, a solution that requires four devices (merging unit(-s), Ethernet switch(-s), protection IED(-s), and source(-s) of time/synchronization) coming from several vendors; having each its own firmware and a step up program, may face significant acceptance problems. Building tightly coupled systems out of several microprocessor-based devices by several vendors brings extra risk and complexity probably doubling with each new type of device, or new vendor adds to the equation. For example consider the exercise of troubleshooting a GPS-supported line current differential scheme, with communication converters, and multiplexers. When one assumes that each of the four system components could be supplied by different vendors, the significance of this issue becomes evident – all parties may comply to applicable standards, and still the system may have problems. The user is ultimately accountable for making it work. Maintaining control of type test integrity becomes very convoluted and

from a responsibility standpoint, nobody is in charge. There is no easy way to control the impact of a change in any one element, especially after the system goes in. The overhead cost associated with working with several other vendors while developing or modifying products will get eventually passed on the user. Given the complexity of the 61850 proposals the initial product fine-tuning phase is not going to subside quickly.

Maintainability. Today's systems are engineered by users to meet their operational and maintenance criteria. This is possible after decades of accumulated experience and owing to common denominator interfaces between the relays in the form of copper wires or simple serial protocols, and relative indifference of the way the relays, including IEDs, are designed, on the operational and maintenance procedures at various utilities. By migrating the input and output signals into communication media, the user experience and training base will have to be significantly re-visited. Even more, the issue of maintainability and testability of the system will shift towards inner workings of the IEDs, putting more burden on manufacturers in order to facilitate the processes traditionally under the full control of users. Both the new architectures and communication protocols will have to be designed to aid this process. The IEC 61850 Standard does not address this issue – it restrains from suggesting any practical architectures and stops short of mandating the response of compliant devices to test values or substituted data, making these concepts of a very low value. The above assumes that users would accept testing or isolation performed in software. Those who would insist on physical testing and/or isolation are left without any practical suggestions.

Determinism. Protection is considered a mission critical task, designed for worst-case scenarios in both primary and secondary systems. As such it requires high level of determinism, and must be designed assuming worst-case scenario within the secondary system itself. Determinism is required to make the engineering task possible (example: worst-case message delivery time for calculations of the coordinating timer in a blocking scheme, or a trip time of a breaker fail scheme); but also to guarantee that the initially commissioned version does not deteriorate as the system is expanded, devices replaced with different models or from different vendors, firmware is upgraded, critical communication settings are altered, etc. A solution that requires re-engineering or re-testing of large portion of the scheme each time a firmware on an Ethernet switch is upgraded, or a new bay is retrofitted and added into the highly integrated communication based P&C system will face acceptance problems if determinism cannot be guaranteed. Lack of determinism and/or lack of future-proof solutions could result in extra engineering, troubleshooting, and testing after the system is initially commissioned to the extent that initial cost savings will be jeopardized.

Right degree of interoperability. Today users accept “proprietary” solutions as long as the size of the proprietary subsystem is small enough, practically limited to a single zone of protection. Indeed, today's transformer or line IEDs are entirely proprietary in terms of collecting their data from standardized analog interfaces, processing it, and executing their controls.

The need for digital interoperability within the substation exists in two areas only: client-server SCADA protocol, and peer-to-peer binary signals for interlocking, breaker fail initiate, auto-reclose initiate, closing and perhaps tripping. A successful solution needs to deliver on interoperability in the areas that are required while addressing all practical aspects such as performance, ease of use, future-proofing, determinism, testability, and maintainability.

Clear design responsibilities. By proposing certain communication-based concepts for exchanging real-time protection-critical information between devices, but restraining itself from providing any architectural proposals for the new system, or addressing specific operational requirements, the IEC 61850 Standard invites various parties from users, through equipment vendors, to independent software companies, into a group design activity for the mission critical system known as power system protection. Involvement of users shall be noticed – the concept was meant to address the problem of understaffed utilities, high cost of engineering, and lack of standardized P&C solutions.

Given its complexity and performance requirements, a successful solution will have to come from parties focused on the complete system, not on its detached elements. Substantial development cost may be required to complete the task, with the outcome being a considerable paradigm shift facing acceptance challenges from both users and regulators. Close cooperation and risk sharing between users and manufacturers will be required for the concept to succeed.

Again, the preceding observations apply to protection functionalities, and not to the relatively simple and mature client-server (SCADA) portion of the 61850 set of protocols.

4.2 Allocation of IEDs and P&C Functions to Zones of Protection

Protection engineers are accustomed to long-standing rules for applying protective relay units, more recently multifunctional boxes, to the various zones of protection. Some of these rules are based on hardware unit failure impact criteria that remain relevant regardless of how the relays are networked for data communications. However, the combination of design features in the latest generation of microprocessor relays, and the control connectivity of IEC 61850 communications (especially GOOSE/GSSE messaging) provide the tools to meet these criteria in better ways and with less equipment than before. Note that the IEC 61850 Standard advises the user that redundancy will be required, but it does not specify how to architect or interconnect the relays and IEDs. In the ensuing text, interconnection architectures and other issues are illustrated.

It is assumed that, for a critical bulk power transmission substation or line, two totally isolated redundant systems will be required so that there is no credible single point of failure that can disable both systems. We call these System A and System B rather than Primary and Backup, since either must be capable of the entire protection job if the other has failed or is

out of service. NERC reliability criteria demand this redundancy to guard against the impact of single failures, and NERC offers specific implementation guidelines. It is noted here that some of those guidelines are derived from traditional protection and control architectures, and that the technical requirement for no single point of failure can be met by entirely different approaches.

Some utilities use more than two redundant systems, but adding more equipment than needed does not always help – it certainly increases the number of failures and repairs to deal with. The technical capabilities of a P&C system based on a 61850 LAN has technical features that can reduce the justification for these third and fourth tiers of redundant relays, as we explain further below.

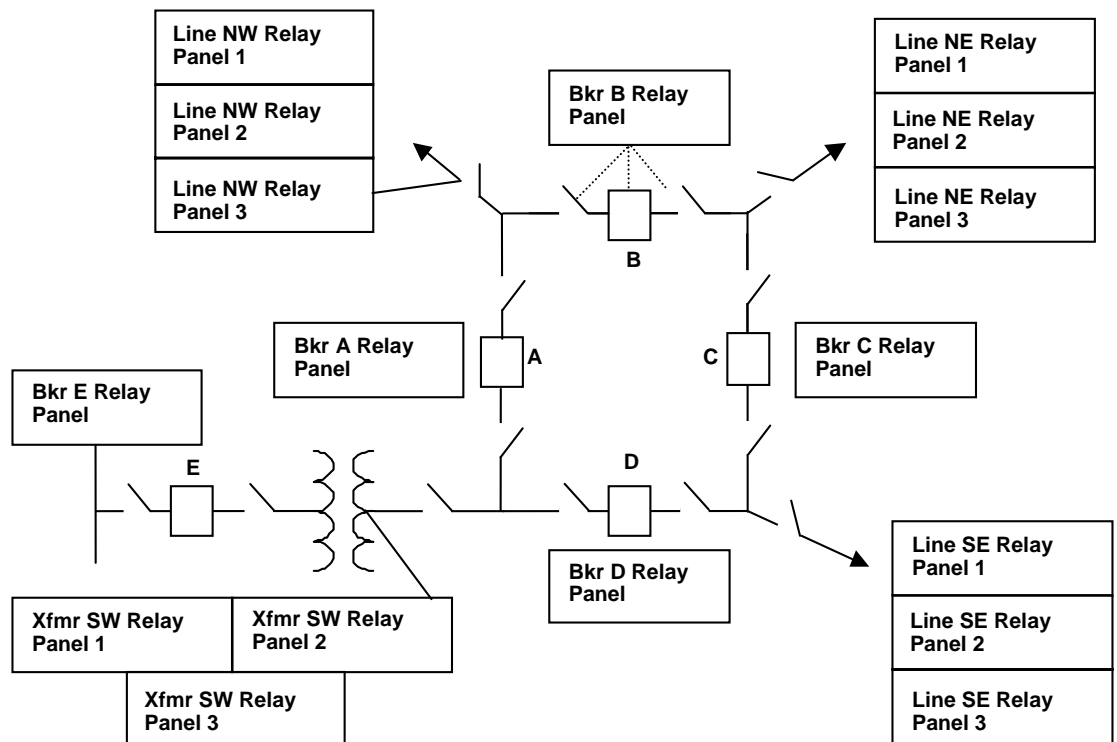
Refer to Figure 3. Here we see a typical ring bus with three lines and a transformer connected. Ring buses or breaker-and-a-half buses are notable for the fact that each zone of protection – a line, bus, or transformer – is fed by multiple breakers. Each breaker must have its own control and protection features. Accordingly, the traditional architecture for such a substation features zone protection panels, having only the relay(s) and control auxiliaries that apply to that line, bus, or transformer. For each zone that is important to power system security, there are at least two separate redundant relay panels. There are separate breaker panels, one per breaker, where all the breaker-oriented

panels for the breakers connecting to the zone.

Looking at this standard design, it is clear that early-generation microprocessor relays with line protection plus breaker failure and reclosing were not useful (they are potentially useful for less critical subtransmission and distribution applications where a line is fed by a single breaker from the bus, and a common failure of line and breaker protection will have only localized impact on the power system). However, the latest generation of microprocessor relays from several manufacturers have breaker functions for two breakers, with a separate set of current input channels for each breaker. Zone currents are summed from the breaker inputs.

These next generation relays can be applied in the newer architecture of Figure 4. Here, the breaker functions reside in the zone relay boxes, eliminating the breaker panels and the separate breaker control and protection equipment. While the failure of a relay unit can also take out the breaker functions included in it, note that there are now redundant functions for each breaker – not a feature of the old Figure 3 architecture. Therefore, the new architecture meets agency reliability criteria for no single point of failure, and with far fewer relay units than before. In many cases, there are four redundant breaker function groups for each breaker – more than we need; some can be turned off for simplicity.

Fig. 3.
Conventional Architecture
for Zone and Breaker
Panels.



protection and control functions and auxiliary devices are installed. These typically include breaker and disconnect switch controls for operators, breaker failure protection, automatic reclosing, and lockout switches for breaker failure actions. As Figure 3 shows, a breaker panel interacts with each of the two adjacent zone protection panel pairs, for example to receive breaker failure initiation or reclosing initiation. Similarly, each protection panel pair interacts with the two or more breaker

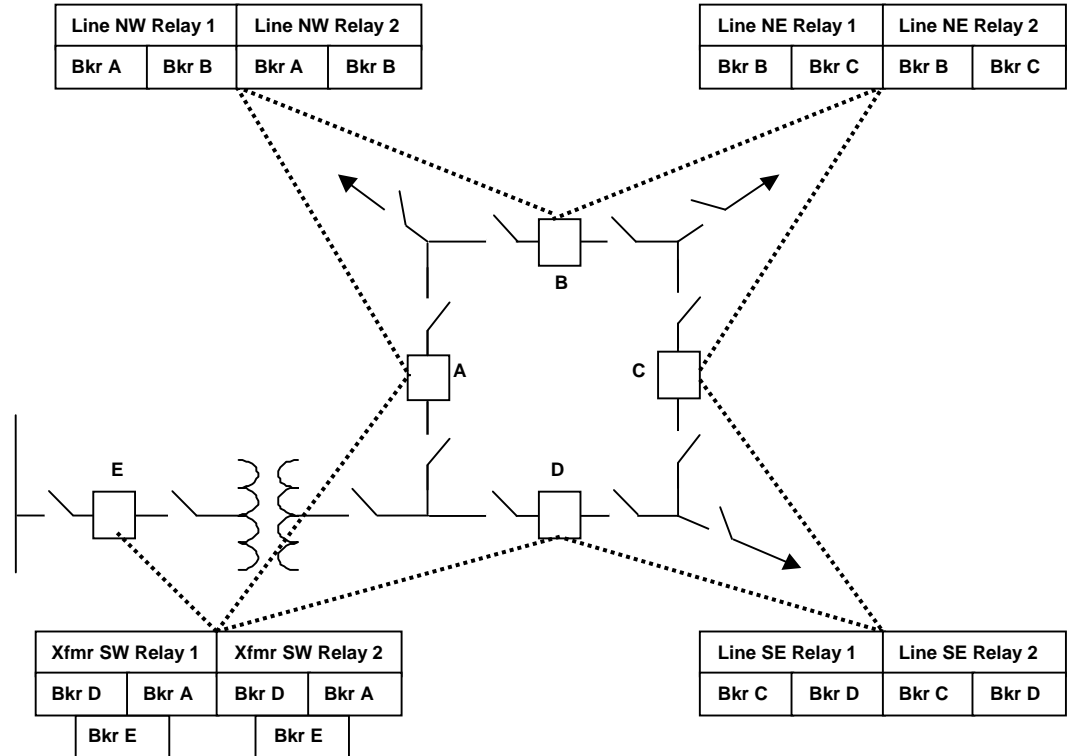
None of these new arrangements for distribution of breaker functions are directly related to use of a LAN with IEC 61850 messaging. However, a pair of redundant 61850 Ethernet LANs provides the means for communications and control among the breaker and zone functions that would require complex and confusing wiring and mounting of auxiliary devices. GOOSE/GSSE high-speed control messages are especially suited for breaker failure initiation, breaker lockout actions when a breaker

failure occurs, reclosing initiation, reclosing function control transfer if the normal relay with line reclosing responsibility fails, and assignment of local manual control functions to relay pushbuttons (as a backup to a substation computer that would be designed into a modern substation for operator use). It is these architectural opportunities and the cost savings they yield that help users to make a business case for the benefits of designing a new substation using 61850 LAN communications. In the example here, we eliminated five breaker panels, and a mass of wiring and auxiliary devices, finishing with an installation having only 8 zone relays on a small number of panels.

Note that conventional wiring and lockout switches have no such overall self-monitoring capability. Furthermore, functionally testing a device like a lockout switch is so awkward and disruptive to power system operation that it is rarely if ever done – we tend to hope these devices will be trustworthy and reliable, but we are not sure about them. Because of the ability to demonstrate that two redundant systems are sure to work, and can rapidly repair one that fails, we have a case for avoiding the use of three or four redundant systems. Taking this simplification cuts the purchased equipment by a third to a half, reduces long-term maintenance costs by a similar amount, and yields floor space, inventory management, and settings/coordination management benefits.

There is another important benefit of the new architecture

Fig. 4.
Use of Microprocessor Zone Relays with Multiple Breaker Functions Included.



with its dual redundant 61850 LAN communications that is not apparent from the figures. An important feature of the GOOSE or GSSE messaging is that messages are transmitted periodically from each relay that broadcasts, to all of the subscribing relays on the network. Normally, the messages are telling the receiving devices that nothing unusual has happened and that nothing need be done. However, the periodic transmission of these no-action messages monitors the performance of the control connection, and any failure of a relay or a LAN component (e.g optical fiber, or Ethernet switch port) can generate an immediate alarm to maintenance personnel. While the second redundant system and its LAN continue to protect, the failure of the first can be rapidly repaired.

While the developers of 61850 were aware of these opportunities and designed the system to bring them to users, they are not written into the Standard, or other public domain publications. It takes some application experience and insight to get these important benefits.

4.3 AC Signals

The cost of copper cabling typically applied by most utilities (engineering, drafting, materials and installation) represents a significant fraction of the total cost of a substation. Digital solutions that replace many copper cables with relatively few fiber optic communications cables are therefore very attractive and have the potential to save considerable amounts of money.

On top of this capability, the relay processes these GOOSE messages through the same hardware and outputs that are used for other protective operations. Therefore, if the relay processor is running, and is routinely operating its output for zone protection or for manual SCADA control, then we know that we have a completely monitored and tested chain of functions that will carry out a major lockout action if needed.

Long cabling applied today has some impact on quality of the used AC signals. CT saturation is the prime example. However with the extremely low burden of modern microprocessor-based relays dramatic reduction of AC cabling does not make much difference. Other non-ideal behavior associated with instrument transformers affecting AC signals, such as

frequency and transient response are typically dealt with via improved protection algorithms that can better cope with signal distortions attributed to long cabling.

Non-conventional instrument transformers promise better signal quality, but those benefits are not dependent on using digital communications to distribute the signals. Lesson learned from successful adoption of microprocessor-based relays makes one believe that it will be unquestionable cost saving rather than better performance that would bring the non-conventional transformers into the mainstream application.

Safety issues such as rising potentials are more of a problem and could be eliminated or reduced when using communications-based AC signals. In this context, despite their 15 years of existence, the non-conventional transformers are yet to see their widespread adoption.

It is important to consider how fiber systems can be deployed without sacrificing the high reliability currently enjoyed with copper. Important considerations are the number of devices connected to any one communications link, time synchronization, response to loss and recovery of the synchronization source, dependence on any one master clock that could be unavailable, element removal for maintenance, availability of test software, and ultimately, user acceptance.

A significant unanswered question is the actual design methodology required, both at the system and device levels, to make the change from the traditional copper cable approach to carrying AC signals to the digital alternative. When making this transition from traditional substation practice employing many copper cables individually wired to instrument transformers, an important consideration is the type of AC signal to be carried and the associated performance requirements. AC Signals used by P&C systems fall into two general categories – time averaged and instantaneous.

Time averaged signals are those that inherently undergo some sort of integration process as part of the basic signal acquisition or later as part of the calculation or application where the signal is used. Examples of time averaged signals are operating measurement telemetry, such as per-phase Amperes or three-phase Megawatts. Time averaged signals typically experience latencies in the range of 1 to 4 seconds, with no detriment to the end application or user. Applications based on remotely accessed time average values on the client-server basis have been used for decades initially via RTUs and recently using protection IEDs.

Instantaneous signals are those which are utilized in time-critical applications such as protective relay algorithms and typically contain sampled values of power system AC quantities sent in real-time. An example of an instantaneous signal is the secondary voltage of a capacitive voltage transformer used in a distance relay algorithm. In this case, permissible data latency may be less than 100 microseconds.

It is taken for granted that copper based signals can easily be shared. It is not so with communication based signals. One

of the fundamental architectural issues is how to provide for overlapping zones of protection, with mandated redundancy, but without multiplying the number of required IEDs of various types (merging units, Ethernet switches, time synchronization means, IEDs) to the extent of ridiculously low reliability / availability of the complete system. The point-to-point 61850 process bus suggestion (part 9.1) calls for an unreasonably high number of merging units. The switch-able (LAN-based) 61850 process bus suggestion (part 9.2) yields a convoluted scheme with time synchronization, LAN, testability and maintainability issues.

When carried on a communications network, signal latencies are introduced by the communications medium itself, in addition to latencies introduced by the signal acquisition interface and end processing application. At any given time, these latencies may be static or random, depending on the communications topology deployed. Latencies may also change as a result of system re-configuration or fail-over, for example following a communications device failure in a redundant system. Communications latencies are therefore of considerable concern in the design of any substation LAN-based or point-to-point topology because these extra delays, if not carefully examined, may fundamentally alter or impair the performance of the end application. Complicating matters is the fact that communications latencies are often difficult to measure or even predict. LAN architectures and issues are discussed later in this section.

The usual approach to managing communications latency with time averaged signals is to factor the worst-case expected latency into the overall response required by the application. The solution is not so simple with instantaneous AC signals. Practical usage of instantaneous signals requires accurate synchronization of measurements at all involved locations. For example a distance functions requires the voltage and current signals be synchronized. If delivered by two independent devices, these signals must be referenced to the same time base. Time synchronization issues are discussed later in this section.

Treatment of lost data is a significant aspect in the “line up” algorithm. As each expected packet can be lost or arrive after a variable time delay, the algorithm must be smart enough to wait for pending data and abandon at a given point in time when the maximum delay time is exceeded.

Another consideration when making the transition from P&C systems using individually copper cabled instrument transformers to solutions relying on digital communications is fault tolerance. The existing copper solutions have the advantage of being extremely reliable from the overall station point of view, because there are very few common failure modes, short of a fire in a cable trench. Availability of distributed P&C architectures utilizing fiber-based AC signals are discussed later in this section.

All of these issues are solvable and must be resolved in parallel with the IEC 61850 Standard, but the quest to realize the potential cost savings will require concerted engineering effort.

A weakness of the 61850 vision in the context of the process bus, is the absence of workable architectures that would satisfy a long list of technical, operational, and regulatory issues. Acceptable architectures may require specific tools, or broadly defined rules for communications. These rules are obviously not there, and what has been specified only enables lab-projects for connecting a merging unit to a compliant IED.

4.4 DC Signals

Another unanswered question is how to effectively implement a digital alternative to the conventional hard-wired connection of discrete DC signals within the substation. DC signals used by P&C systems also fall into two general categories – those that indicate the current state of an element or system, and those that represent time-critical actions, such as protection trips.

The first category includes signals such as alarm and status points used by SCADA systems and the state of discrete conditions such as switchgear interlocks, position of reclosure selections, etc., but does not include the status of breaker auxiliary switches used in breaker failure and other critical protection applications. Signals used by control systems are generally one order of magnitude less critical with respect to delivery time than those used by primary protection systems. Inherent latency times for status signals are typically in the range of 15-20ms, whereas alarm and condition states may have acceptable latency times of 1.0 s or more. Existing communications performance in practically any topology (point-to-point, star LAN, bus LAN, etc.) is quite capable of meeting this level of performance in control systems of up to 1000 points or more.

The second category poses a much more significant design and application challenge for emerging communications-based alternatives. This category includes most input and output signals used by primary protection and teleprotection systems. Backup protections generally do not require this level of performance. Category two signals are considered to be those that require reliable delivery in less than 4.0 ms, under the worst-case guaranteed system traffic conditions. If we assume that the portion of protection circuitry between existing relays and the associated switchgear is implemented with auxiliary relays and miles of wire and cable, the fastest protection trip signal times are typically 4.0 ms and are determined by the choice of auxiliary relay used for high-speed applications. This is frequently used as a benchmark when evaluating digital alternatives. Developers of the current generation of IEDs have generally met this level of performance for the execution of discrete internal logic, analogous to separate auxiliary relay logic. However, current substations still use many thousands of dollars worth of DC cable to interface IEDs to switchgear and other devices in the switchyard and within the relay building.

From a cost point of view, the same incentive exists to eliminate or reduce DC copper cabling as there is with AC cabling. Similar communications latency considerations apply also, except the need for time stamping is generally limited to the appropriate identification of discrete events. In the case of discrete protection trip signals, communications performance

is impacted by the extremely random nature of this traffic. For example, say a substation runs normally for two years and then suddenly a bus fault occurs, followed by a breaker failure. Immediately, many IEDs start sending huge amounts of traffic and the communications infrastructure suddenly reaches 110 % of capacity. Some signals may therefore experience delay or even become lost if the design doesn't anticipate this type of response.

Converting discrete signals formerly carried via copper wires to their LAN-based equivalent messages also significantly changes the failure mode from the perspective of the receiving device. In a traditional wired circuit, a contact closes at the sending end and an auxiliary relay coil picks-up at the receiving end. The auxiliary relay remains energized for the entire length of time the sending contact is closed. The length of time the sending contact is closed also conveys information and in fact is the basis for many time co-ordination and backup-schemes. In a LAN-based scheme, this transaction is replaced by discrete commands sent digitally over the network. A message is sent signifying the "on" state and another message may be sent later signifying the "off" state. The receiving application must keep track of the context of these messages. If, for example, the system fails and the "off" message is never received, the receiving application could be "stranded" in an undesirable state for an extended period, unlike the wired system in which the receiver will "fail safe" and turn itself off. Therefore, a practical message delivery system for a substation-LAN based messaging protocol must include additional features such as a regular heartbeat message or other equivalent strategy to identify the continuity of the sender. The receiver also needs to have a strategy permitting it to go back to the reset or default state upon loss of the heartbeat message.

An additional factor affecting reliable message delivery is the choice of the LAN architecture itself and the various redundancy strategies that may be established. For example, simple networks connected with shared media switches may cause collisions to occur between messages sent nearly simultaneously, thus impairing message delivery of one or all of the sending stations. Switch networks greatly improve the situation, but each system type still needs to be carefully evaluated with respect to the performance of critical traffic.

The network architecture or topology also has a bearing on the reliability of message delivery in a digital substation. For example, many older SCADA architectures were based on the master-slave concept, in which the slave devices essentially are data senders and discrete I/O devices only. Many newer substation integration architectures are based on the peer-to-peer concept, in which system elements exchange information but are also capable of autonomous behaviour on their own.

Solutions that replace DC cabling with fiber optic communications solutions are becoming available. It is paramount that the application topologies proposed carefully consider and ultimately specify explicitly the maximum performance any given combination of IEDs, field acquisition devices and communications elements is capable of. Simple application rules are required for consistent deployment on actual projects.

Appropriate redundancy or equivalent strategies are also required to guarantee acceptable overall system reliability despite the consolidation of signals on a multiplexed bearer media instead of over many simple and discrete wires. Fiber alternatives also offer significant advantages over DC cables with respect to immunity against (induced) interference and transient (capacitive) effects that tend to be troublesome with the current generation of IEDs and teleprotection equipment. The potential exposure to battery grounds is also significantly reduced.

4.5 LAN Architectures and Issues

As communications in the substation (and beyond) takes on a more critical role in the protection and control tasks of the utility, the enterprise communication architecture must be designed to meet the same critical design requirements of the equipment with which it is connecting. Specifically, the communication equipment must meet the same environmental and electrical specifications as the protection and control equipment.

In addition to the electrical and environmental specifications, the communication system must be available to communicate between the various IEDs in or between substations. The design for high-availability starts with redundancy in the communications from the IED. Redundancy in the IED can be achieved either through redundant port or redundant media. With redundant ports, there are two completely independent Ethernet ports built into the IED with each port having its own Ethernet MAC address and separate IP addresses. With two sets of addresses, the IED must constantly monitor both ports for information received and channel it to the appropriate process.

A second option for redundancy is that of redundant media. In this implementation, there is only one Ethernet port (one MAC address, one IP address) that is dynamically switched from a primary fiber port to a secondary output port. The switching is based on the loss of Ethernet link pulses on the primary connection.

Given redundant Ethernet on the IED, the next area to address with redundancy is the Ethernet connection junction. In today's implementations, it is almost a given that the

connection between Ethernet ports will be performed by an Ethernet Switch. A switch operates at a logical level in the communication hierarchy, that is, a switch receives an Ethernet packet, reads the contents, and then decides how the contents should be processed and forwarded. In the processing of the packet, the switch first determines if the packet should be processed at all (a security feature to inhibit just anyone from unplugging an IED and plugging in a laptop in a substation). If the packet is to be processed, should it be processed with priority (a Quality of Service feature of Ethernet) and should it be delivered to only specific ports (Ethernet Virtual LAN option)? In the redundant architecture, each Ethernet output of the IED should be connected to different switches so that if a switch fails, communication to the IED can automatically be transferred to the back-up communication port on the IED. The two switches now need to be linked together so that a message received on one switch can be transmitted to any device connected on the other switch.

In order to optimize communication between switches, it is recommended that the up-link port be operated at a higher speed than that of the feeder ports. For example, if the feeder ports operated at 10MB, it is recommended that the Link ports between switches operate at 100MB or faster. Similarly, if the feeder ports are operating at 100MB, it is recommended that the Link ports be operated at 1GB.

Typically, an Ethernet switch can connect from 12 to 16 IEDs. For substations containing more IEDs than this value, multiple switches need to be linked together on a primary and secondary port basis, again with a connection between the group of primary and back-up switches. This configuration has a drawback in that if one of the switches being used to connect the primary group of switches to the back-up group fails, the connection to the back-up group is lost. This failure mode can be eliminated by connecting the groups together at both ends, effectively forming a loop. In general, Ethernet does not operate in loops; however, most switches in use today operate an Ethernet algorithm known as Spanning Tree. This algorithm is designed to detect any loops and to logically break the loop at a point. More specifically, there is a variant of the Spanning Tree algorithm known as Rapid Spanning Tree that can detect rings and fix breaks in structures in as little as 5ms. The resulting LAN architecture is shown in Figure 5.

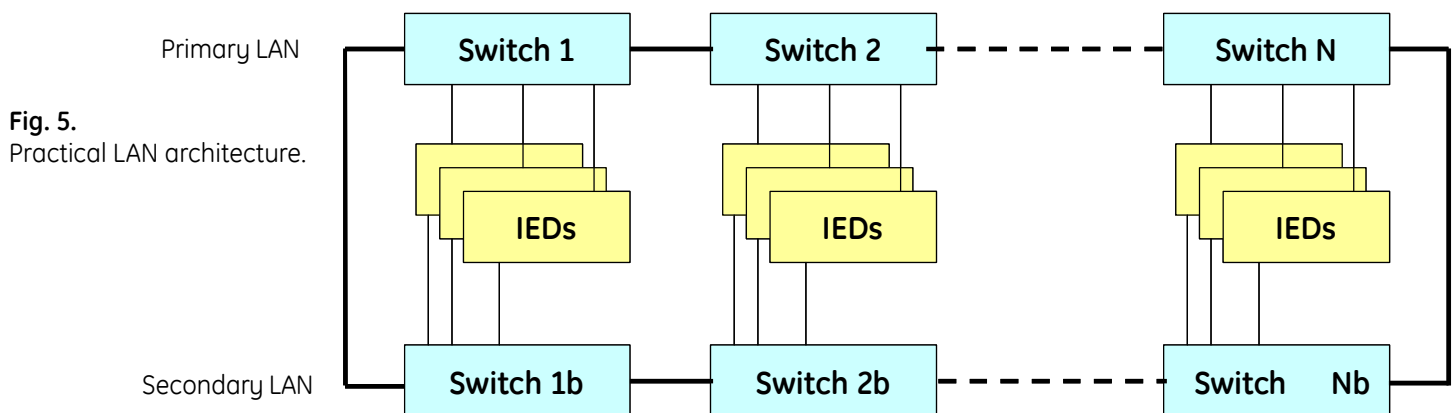


Fig. 5. Practical LAN architecture.

Many experienced protection engineers find discussion of these data communications issues to be dense and perhaps intimidating, because until now they have not faced the need to understand the behavior and performance characteristics of substation components like Ethernet switches. Furthermore, there is no part of the IEC 61850 Standard that guides designers and users on these network architecture subtleties. We encourage users to recognize that unavoidably, as P&C design technology moves forward, the behavior and characteristics of components like Ethernet switches will be as important to understand as those of protective relays if the P&C system is to achieve its availability, dependability, security, and maintainability goals. It is important for protection engineers to understand that the basics of IT networks are not difficult to understand, and that learning how to handle networking issues is no more difficult than learning about any new generation of relays. Incidentally, P&C engineering groups need to achieve peace and mutual understanding with the utility IT department, which can help with substation-enterprise integration, and which needs to understand the features of substation LAN messaging that are critical to power system security.

We explained above the existence of multiple ports in a typical modern managed switch, each port having its own queue of incoming and outgoing messages so that we never face the problem of collisions and lost messages. We also explained how new switches complying with the Ethernet standard IEEE 801.2Q can recognize priority and VLAN fields in the message packets (e.g. GOOSE messages) and can express-route or selectively route critical messages. There is more to consider from a relaying point of view. For example, full utilization of the two redundant P&C systems require that GOOSE messages pass between them, and that substation host devices and interfaces to the utility WAN be able to communicate with devices in both System A and System B. To do this, the designer needs to take advantage of the isolation that the ports of the Ethernet switches in System A and in System B can provide, and to interconnect them in a way that avoids single points of failure that could interfere with data communications in both Systems A and B. The designer needs to consider not only passive failures, like a broken fiber, dead port, or failed switch ; but also active failures of communicating devices that jabber unwanted message traffic or turn on emitters continuously. Switches and networking equipment could provide tools to handle these contingencies.

Maintenance personnel also will need to gain enough understanding of communication architectures including both physical topology and control mechanisms for data. For example, consider a relay that has primary and failover fiber connections to two different ports on two different Ethernet switches in System A as we described above. A technician who disconnects the primary fiber, or turns off the switch to which it is connected, may think that he has disabled backup tripping GOOSE commands from this relay to others on the LAN. He then may proceed to test the relay in ways that generate backup tripping request messages. He needs to understand that the relay may have detected the disconnected primary channel and failed over to the completely functional backup fiber and switch – all the messages will be delivered on time to subscribed

relays in Systems A and B, possibly yielding unexpected and undesired tripping from the testing work.

4.6 Time Synchronization Architectures and Issues

A very important unanswered question is how will accurate, coordinated time services be delivered to all elements and processes within the whole integrated system? Advanced concepts within the IEC 61850 set of standards suggest digitizing protection input signals, currents and voltages, at the place of origin and providing the protection and control system with real-time stream of samples using a standardized protocol (process bus).

The idea of further reducing wiring substations by substituting switchyard cables with fiber optic cables is very attractive economically. This could be accomplished by applying non-conventional CTs/VTs and moving analog signals via fiber into merging units for de-coding, and subsequent digitization and presentation as the process-bus data. Alternatively, traditional secondary signals could be connected to dedicated interfacing devices in the yard for digitization and transport via digital fiber into the control house.

In both instances, protection relays as known today will be presented with information taken at various physical locations by various interfacing devices. This requires data taken at independent locations to be time aligned. Protection functions responding to signal magnitudes, such as overcurrent or undervoltage, do not require time alignment. But a vast majority of functions would not operate properly if their input signals were not time aligned. For example, a distance function requires voltages and currents to be aligned; a synchro-check function requires the two compared voltages to have a common reference; transformer differential calls for all the used currents to be time aligned as well, etc.

Today, the requirement of time alignment is achieved by synchronous sampling of all input signals of a relay inside the IED itself. This idea could be carried forward only if a given merging unit processes all signals required by a given IED. This would basically create one-to-one correspondence between merging units and IEDs, and poses a question of why not combine the merging units with the IED, yielding a new type of IED that works with analog, fiber-based inputs produced by high voltage sensors of non-traditional CTs/VTs.

The operation of time alignment can be understood either as “hard” synchronization with respect to time, or “soft” synchronization of devices with respect to one another. It could be implemented as precise time stamping of otherwise asynchronously taken samples, or taking samples of all signals exactly at the same time instant.

In either case, availability of protection is dependent on synchronization. This is a vital, often overlooked issue impacting the system architecture and overall reliability of the scheme. In fact, this is one of the central technical challenges that need to be resolved to effectively implement the process bus concept.

The recipient devices must be designed to cope with lost data and potentially variable time latencies for packets coming from different sources. Complexity of existing line current differential schemes is a good extrapolation of the technical challenges in this area. The IEC standard does have cognizance of this issue and does require the manufacturer compensate for filter delays but the implementation details are left to the manufacturer.

The start up procedure when the device wakes up and start communicating while synchronizing itself is particularly exigent, especially if the involved pieces of equipment come from different vendors.

A protection scheme based on external source of synchronization depends entirely on availability and quality of such synchronization source. In the reliability model, this source is connected in series with the other elements and substantially impacts the overall reliability of the system. In order to avoid diminishing the reliability such a source would inevitably have to be duplicated. Duplicating the synchronization clock is not a trivial task as the two clocks will have to maintain mutual synchronism so that when one of them fails and recovers, the system rides through such conditions without a glitch. Additionally, loss of synchronization of one clock with the GPS satellites while the other is still connected needs to be addressed.

The IEC 61850 concept addresses the issue of time accuracy and defines five different levels of time accuracy. The Standard permits usage of SNTP for time synchronization over network for time stamping for SCADA purposes. The SNTP method, capable of reaching about 1ms accuracy, is not precise enough for samples of currents and voltages and the Standard does not offer solutions as to how to achieve the required accuracy. Options to be considered are: an externally provided IRIG-B synchronization signal; a precise, network-based open standard such as the IEEE 1588; or a proprietary network based protocol.

It seems that complying with the high-accuracy time specifications of IEC 61850 requires using an external synchronization source, i.e. IRIG-B inputs. This in turn, requires delivering (redundant) time signal(-s) to all devices that need to be synchronized. Such signals must be driven from two independent (redundant), but mutually-synchronized clocks (contradictory to some extent). If these clocks are driven from the GPS receivers to provide for absolute time reference, issues arise when the GPS signal is lost and recovered. Obviously the protection system does not require absolute time to work properly (except some applications of line current differential relays), and should function normally without the GPS signal. If the GPS signal is lost and subsequently recovered, the redundant clocks will have two, partially contradictory control goals: catch up to the actual absolute time, and prevent any time jumps for the devices synchronized using the timing lines. This adds unnecessary complexity into the system.

Alternatively, the two clocks (either IRIG-B or network-based) do not have to be synchronized, but would switch-over should one of them fail. Again the process of switching over will

have to be well designed in order to provide for a robust and safe solution. The IEC 61850 assumes the synchronizing and synchronized devices to be independent pieces of equipment, typically design by different vendors and still work flawlessly for this mission-critical system.

Some IED manufacturers are probing the idea of using the IEEE 1588 network time synchronization protocol for the process bus applications. This creates problems for interoperability – all devices would have to adopt this method, or use their own alternative method of synchronization. If the latter concept is adopted, the user is affected by extra complexity and vendor-specific solutions. Also, one needs to make sure devices non-compliant with the IEEE 1588, are not inadvertently affected by the embedded, network based time synchronization protocol. The IEEE 1588 method requires Ethernet switches to support it, and in today's technology, this creates extra cost for the switch manufacturers.

Another theoretically possible alternative is to use a solution in which all devices on the network synchronize slowly to each other (no master or absolute time) using a phase lock loop approach and large inertia of their internal clocks. This may be an excellent solution for an isolated deterministic network of 2 or 3 devices, but would not work well in a large non-deterministic network with tens or hundreds of devices. Not to mention that such a method is not mandated by the IEC 61850 Standard as a universal, compliant way of time synchronization for the process bus, and will have to remain proprietary.

Presently the issue of time synchronization is solved internally to an IED. Reliability of the technical solution is already included in the overall Mean Time To Failure (MTTF) of the device. The user does not need to engineer or maintain any protection-grade time synchronization means. And availability of protection is not subject to availability and quality of external time sources. It would be beneficial if these attributes were retained in new protection architectures.

The minimum requirement for time alignment in the protection realm is to align signals within a given zone of protection. Moreover, only relative alignment is needed. Given the response time of protective relays, this calls for relative time stamping with an arbitrary time index that could roll over after one or two power cycles. This could be achieved in much simpler ways compared with a generic, hard synch off all devices in the substation to a source of absolute time.

In the implementation of the Process Bus (part 9-2), the Standard has the option of either a relative time stamp or an absolute timestamp. In this application, a full absolute timestamp of 64 bits is typically unnecessary information but is required if the information is to be used as part of a Synchrophasor calculation. In the initial implementation agreement, only a relative time stamp, based on the Fraction of Second, is used. When applying this information to Synchrophasors, information on leap second (one full second can be added or deleted by the GPS system to adjust to planetary rotation) and time quality is also required. Additionally, when correlating sample data between multiple merging units (especially between

substations), complete absolute time information and time quality will be required. Careful engineering decisions on how to accomplish this will be needed as the Standard moves forward. The full timing information is not required by protection, but if embedded it could cause harm by revealing weaknesses in the applied IEDs, and the need for extra testing.

4.7 Reliability and Availability of Protection

Availability and reliability of protection are not impacted when using microprocessor-based protective relays as known today, and applied to both protection and control within the SCADA realm of the IEC 61850.

When pursuing distributed architectures based on the concept of a process bus with the intent of eliminating copper wiring in the yard and replacing it with fiber optics solution, availability and reliability of protection is a fundamental consideration, and one of the key barriers to overcome.

For example, consider Figure 6 showing a benchmark substation of Figure A-1, and focus on AC signals associated with protection IEDs around breakers CB-1 and CB-2. This example pictures realistically the concepts of overlapping zones of protection, redundancy and separation of the A&B systems (for simplicity lockout relays are neglected, just two trip coils are shown, the breaker fail devices are separate from the zone relays and are not redundant). The figure clearly illustrates the reason for extensive field wiring: redundancy and overlapping protection zones.

Figure 7 presents a hypothetical architecture in which each AC signal is digitized by a separate merging unit. Separate MUs are used to provide for the DC signal interface (MU-11 through 14). The A&B systems are kept separate. Consider the availability of the LINE 1 protection system A. This zone

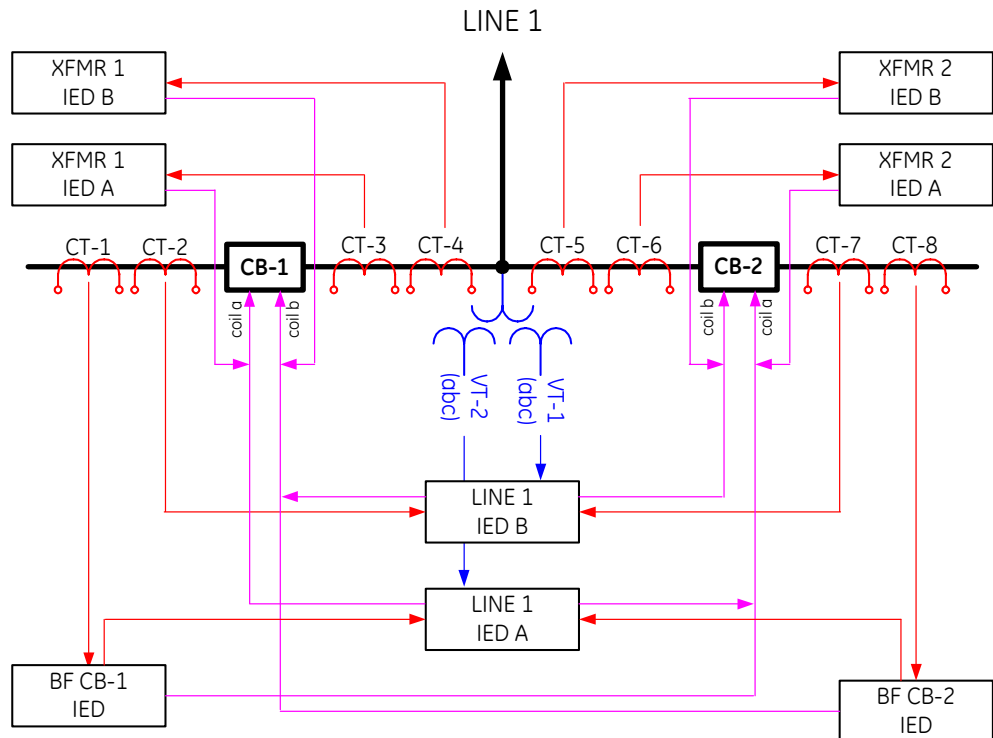
depends on availability of MUs 1, 8, 10 for measurement and MUs 11 and 14 for tripping, Ethernet LAN A for communications, and Line IED for overall processing - not to mention the time synchronization source for the AC related MUs (1,8 and 10). Composed out of seven of today's IEDs such a line protection system would have an MTTF on an order of magnitude lower compared with today's relays (see Annex B).

Figure 8 presents a sample architecture with one breaker IED (MU) that interfaces two currents and DC signals. Now only two MUS per breaker are required. Still the line protection is a system involving five IEDs (MUs 1, 3, 6, Ethernet switch, IED). Note that the BF function depends on three devices (MU-1, LAN A, BF IED). This becomes a flaw that reduces dramatically availability of the BF function, and calls for solutions in a form of redundant hardware, or equivalent.

Figure 9 further eliminates MUs 5 and 6 by wiring the voltage signals to MU-3 and 4 (typically a relatively short distance compared with the distance from the yard all the way to the control house). Still the line protection depends on four IEDs or five counting the time synchronization source. As explained in Annex B, the expected reliability of the scheme is not there. Besides – MUs 3 and 4 become equivalent to today's microprocessor-based relays in complexity. They support current and voltage inputs as well as digital inputs and output contacts. The question arises: why not provide the complete functionality in such a yard device, eliminating the need for all the other IEDs. The obvious acceptance and maintenance issues may be easier to overcome compared with the solutions of Figures 6 through 9.

It is strongly recommended that concepts building around the process bus and substituting copper with fiber, particularly for the yard wiring, are presented in the context of actual count of CT, VTs, giving consideration to overlapping protection zones, redundancy and separation of the A&B systems. Once the

Fig. 6.
Selected breaker from the benchmark of Figure A-1.



architecture is presented, an IED count can be approximated, and reliability study should be conducted in order to validate the solution.

Annex B calculates Mean Time To Failure values for several hypothetical systems based on the process bus concept assuming arbitrary MTTF data for the system components. It could be seen that the MTTF calculations drive a certain vision

of a distributed protection system.

Annex B proves what is intuitively obvious: a process bus protection system set up with off-the-shelf components (merging units fed from non-conventional instrument transformers, explicitly synchronized via their IRIG-B inputs, and communicating via Ethernet network) would have reliability numbers decimated by an order of magnitude compared

Fig. 7.
A hypothetical process bus architecture for the system of Fig.6.

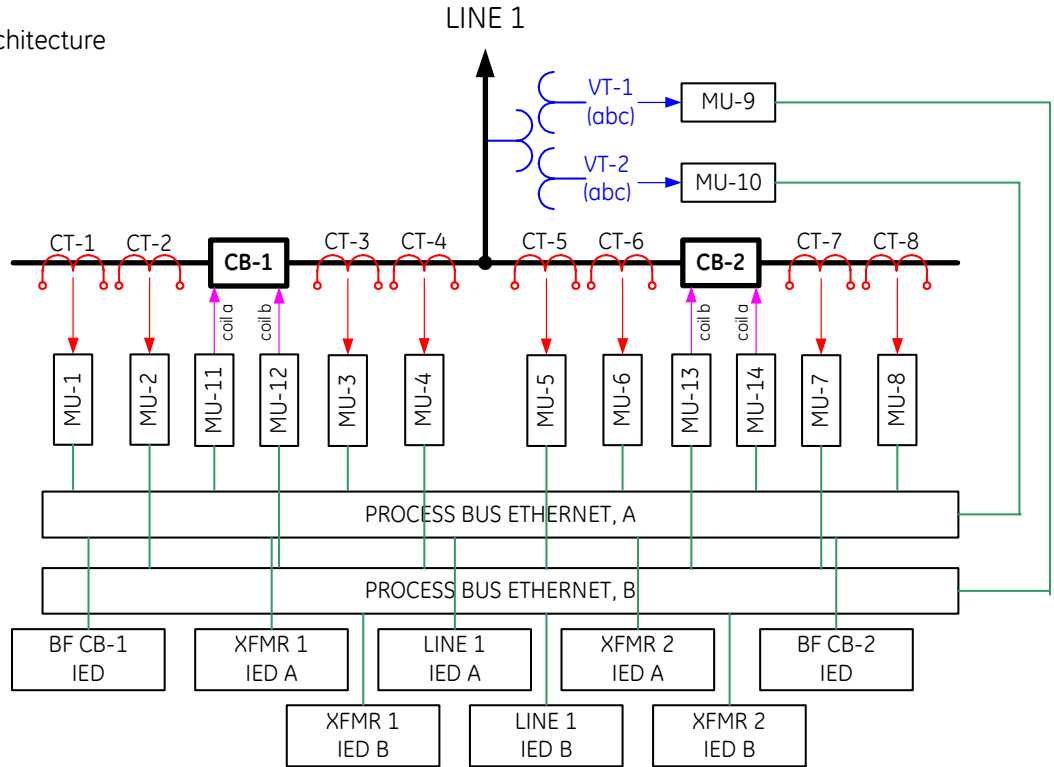


Fig. 8.
A hypothetical process bus architecture for the system of Fig.6.

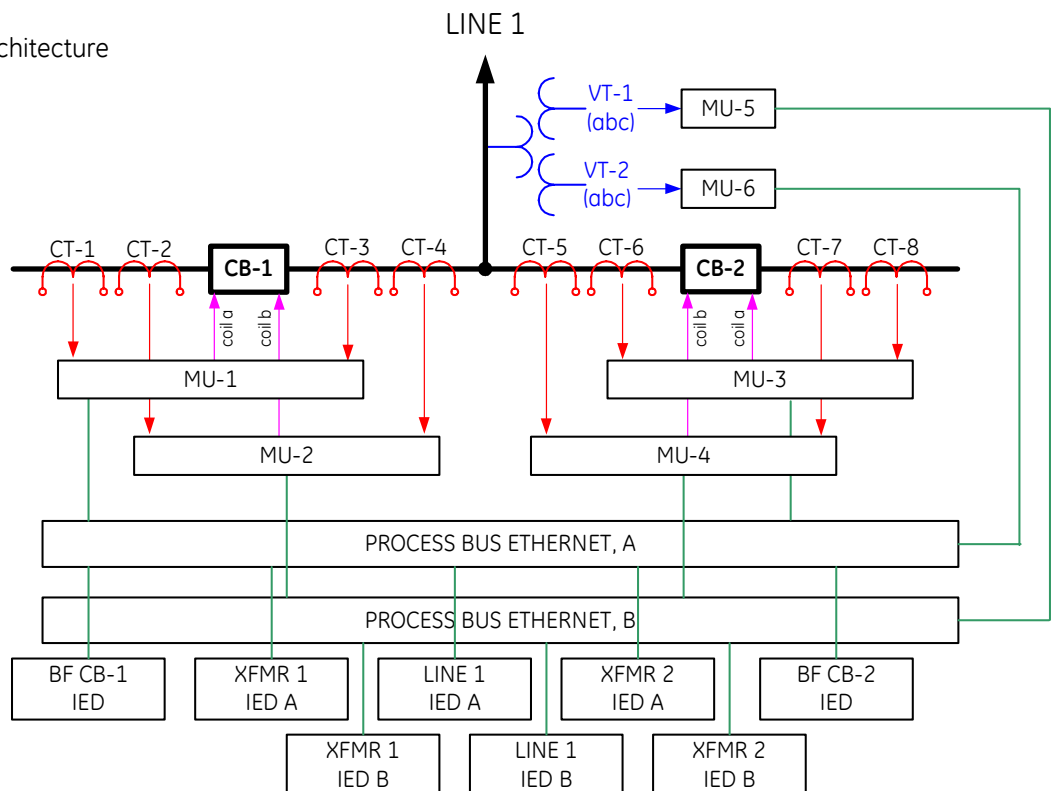
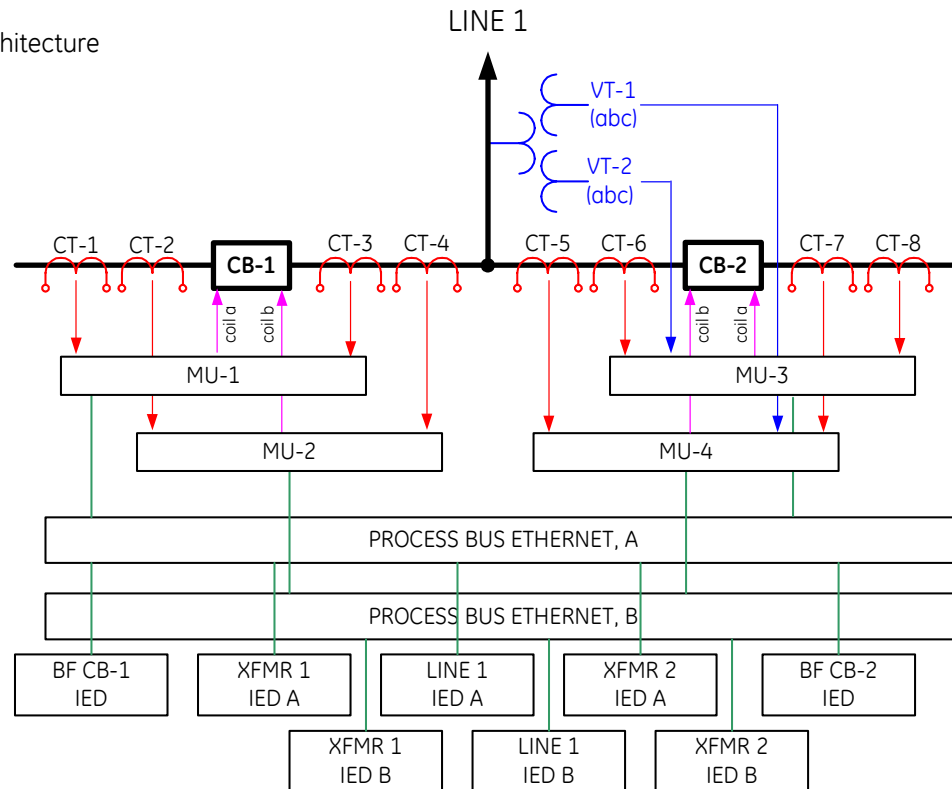


Fig. 9.
A hypothetical process bus architecture for the system of Fig.6.



with today's microprocessor-based relays. This is because of substantial increase in the total part count and complexity of such a distributed system as compared with today's integrated microprocessor-based relays. A successful system for replacing copper wires with fiber optics would have to keep the total part count and complexity at the level of today's relays.

There are challenges in designing such a system primarily time synchronization, and sharing data from merging units to multiple IEDs without an explicit network, while keeping the total count of merging units (interfacing devices) at a reasonable level.

It is justified to assume relay vendors have already conceptualized or are working on the solutions. It is quite obvious that the interoperability protocols of the IEC 61850 in the areas of process bus and peer-to-peer communication are of little help in solving this architectural/reliability puzzle.

4.8 Overall System Performance

Another unanswered question is that of determining and verifying the overall level of performance of a set of interoperating IEC 61850-based devices as a complete system. Although the 61850 Standard does classify the performance of an individual IED with respect to the required response times for individual message types (as would be determined in a benchmark conformance test of an individual IED), there is currently no guidance available on how to characterize message delivery performance across a whole integrated system. As an example, consider an integrated P&C system for a 230 kV transmission substation with say 12 circuit breakers. There are currently no simple and easy to apply design metrics that would allow the designer to determine on paper in advance if the integrated design as a complete system will actually work

for this particular topology or architecture. Based on current practice, the system would very likely have to be pre-assembled in a factory or lab setting and undergo a series of complicated tests before delivery to site.

The question remains as to how would the same exercise be repeated in say five years when the in-service station needs to be expanded to 16 breakers? This ad-hoc type of process would be very expensive if it had to be repeated for each and every project, with no quantifiable guarantees of overall performance, especially for protection-critical trip and initiation signals. The cost and difficulty of executing these tests might also inadvertently place an artificial limit on creative design because each novel idea could undermine the experience base developed around a previously known configuration, creating a disincentive to its adoption.

Practical system level application advice is totally missing. It is therefore essential that simple, easy to apply and consistent IEC 61850 design rules be developed so users can determine with certainty that a collection of W IEDs from X manufacturers configured in one of Y topologies will work for a switchyard of up to Z power system elements.

4.9 Failure Management

System integrity and failure management is another unanswered question. Consider for example, the portion of an integrated system consisting of a bus protection that trips say 10 breakers via 10 individual breaker IEDs. These same breakers' IEDs are also shared with breaker failure and reclosing functions as well as providing the interface for SCADA operational control and telemetry. Now consider that one of the 10 breaker IEDs has failed because, for example, its communications interface has

been interrupted. All of the applications requiring that IED and its functions have now been disabled. There are many possible consequences, depending on how the system is designed. For example, the system could be 100% redundant and the loss of any one element isn't critical as long as its condition is alarmed. Parts of the system might not be redundant, for example SCADA, so the missing element does constitute a critical failure. Elements needing the missing IED could also revert to an alternate device upon detection of loss of communications.

There are obviously many ways to treat such a failure. The next question is how to safely and consistently isolate the failed device to permit troubleshooting and replacement? How would the maintainer quickly acquire the knowledge of what logical associations are involved with the failed device and the impact of each? What test and maintenance tools would be required to perform this work? At present, no uniform system level functional object definitions or concepts have been defined to cover these types of issues involving the contingency status and operation of an integrated IEC 61850-based substation.

The definition of such concepts and the appropriate software to effectively use them are essential. This will enable users to take advantage of a consistent set of tools and procedures without risking an accident or inadvertent trip to the power system. As we explained in 4.5 above, those users also can and must learn the behavior and characteristics of Ethernet communications links and networking devices to diagnose and safely repair failures.

4.10 Application Gaps

Quite often implementing existing functions using communication-based solutions is not trivial and requires substantial amount of engineering and testing. Once the solution is found, users realize that the proper way of achieving the functionality would have been via standardized functions and services, and not via user programmable logic.

This section illustrates this problem better by presenting issues and solutions related to the lockout functionality implemented in software, as a distributed function, when replacing physical lockout relays and eliminating the associated wiring.

Utilities usually lock out the breakers surrounding a permanent equipment failure. This is done for internal transformer faults, bus faults and failures of breakers. One or more protection devices may initiate operation of a lockout relay (ANSI 86). This is a bi-stable device that remains in the operated state after reset of the initiating protection. The lockout relay provides sustained tripping commands to all of the breakers making up the zone and blocks all the possible means of closing said breakers. The intent is to prevent re-energization of the equipment until a local inspection has been carried out. Accordingly, the lockout relay is usually hand-reset. Due to its simplicity, the lockout has a high reliability. Monitoring of the lockout coil (either by placing a lamp in parallel with the initiating device or through the use of a coil monitoring relay) further increases the availability.

Lockout relays often trip extended zones made up of several

breakers. As such, moving this function into the digital domain presents a significant opportunity to reduce device count and wiring complexity. For this analysis assume that transformer bank-1 of Annex A, Figure A-1 is to be protected. A fault requires locking-out of CB-1, CB-2, CB-5, and CB-6.

The basic functional requirements for lockout, whether electromechanical or IEC 61850 based, are:

- Initiation method
- Distribution to multiple relays that control affected breakers
- Presentation to local and remote operators
- Lockout-clearing protocol or standard operating procedure
- Non-volatility
- Independent handling of multiple lockouts on the same breaker (e.g. transformer fault followed by BF)
- Data exchange between substation control and relays.

Two scenarios are considered: (A) a transformer zone IED and dedicated breaker IEDs and (B) CB-5 & CB-6 breaker functions merged into the transformer zone IED and the remaining breaker functions merged into the line zone IEDs. Implementation of the lockout function is shown in Figure 10.

The latches, residing in each IED, together with the messaging passed over the station bus constitutes a "distributed" lockout function. The latches should be non-volatile and located in the IED that is connected to the breaker in order to ensure that the signal is maintained should there be a communications failure. The location of the manual reset may be at the transformer zone IED as shown or may be located at a central HMI. The latter may seem as a violation of the very nature of the lockout, but with advancements in remote inspection (cameras, access to measurements and records), it may become an acceptable solution.

The logic as shown assumes a non-redundant system where the only path for control is through the IED. If the IED responsible for tripping and closing fails, its contacts will reset. However, since there are no other paths for control, the rules for lockout are not violated.

If redundancy is required (as it often is) then the scheme must be modified. Assume that the logic of Figure 10 is implemented in two sets of IEDs (denoted system A & B for this exercise). One possible solution is to use IEDs with bi-stable output contacts for tripping and close supervision. IEDs with outputs of this type are available but are not common. The block-close signal from each scheme would be combined externally with the close commands; leading to increased wiring complexity. This solution raises a new dilemma: It is not possible to reset the lockout if the IED fails after operating (not a problem with conventional lockouts).

Another solution is to cross connect the lockout function of each system. The A & B Transformer IEDs would each operate both the A & B lockouts. The presumption in this case, is that the station busses of each system are interconnected. For some

this may be seen to be decreasing the overall reliability of the system since it's conceivable that a communications problem could cause a failure of both systems. Properly designed network devices should mitigate this risk. In another sense this system may be considered more reliable since it can deal with double-contingency events such as the simultaneous failure of the A transformer IED and the B lockout IED in scenario A.

Note that the logic described above is for a single lockout (transformer zone). Picking CB5, it can be seen that lockout functions for the B1 Bus Zone and CB6, CB8, CB1, & CB3 breaker failure zones must also trip this breaker. Therefore the logic shown in Figure A-1 must be duplicated for each of these zones.

Developing and testing such logic poses a significant problem for an average user. Absence of well-designed application templates for various standard protection elements such as lockout function, tripping using GOOSE, testing GOOSE-based

paramount concern to consider what form of testing is required and in fact what is the purpose of testing? For example, many well-designed IEDs now incorporate extensive self-testing features which make the likelihood of a spontaneous software change remaining undetected by an internal monitoring task practically nil. However, the IED does not know that the overcurrent setting should have been entered as 500A and not 600A. That is a user mistake that can currently only be caught by external quality assurance procedures. Therefore, initial commissioning of any system will remain an important activity. But what about testing following the initial in-service? The industry and regulatory trend to increase maintenance intervals for IED-based systems is in fact based on self-monitoring capability and when maintenance is actually done, the focus is on checking overall functional performance, such as by doing a live trip test where possible.

There are several key considerations emerging in substation communication-based systems. The first issue is the ability of

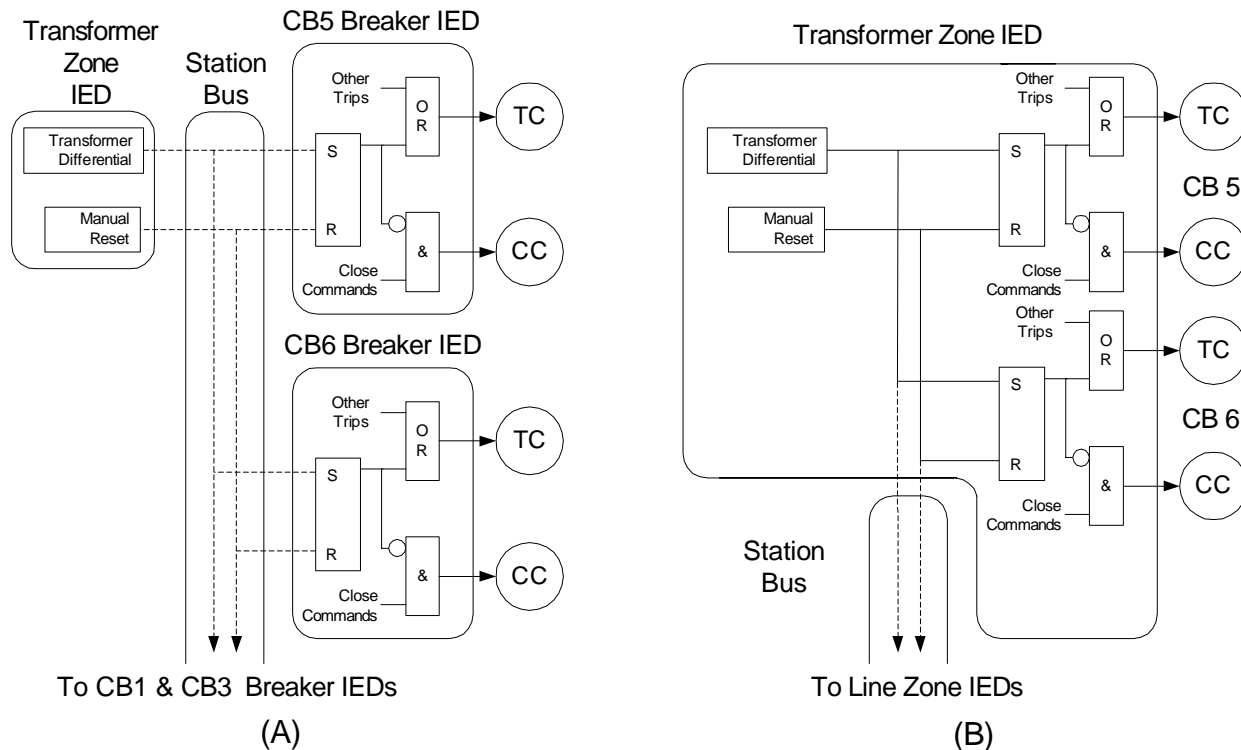


Fig. 10. Possible solution to the lockout functionality.

breaker fail initiate signals, etc. is one of the obstacles to wider application of basic peer-to-peer elements of the 61850 Standard.

4.11 Testing and Test Facilities

Another unanswered question with respect to deployment of an all-digital substation is how will commissioning and routine maintenance be performed and what test tools will be required to do it?

As new P&C technologies emerge that use advanced communications and other features to reduce both the number of devices and physical interconnections (wire and cable) it is of

the user to validate the system will initially work as a whole, if all hard-wired signals are replaced by their digital equivalents. By this it is meant that unless extensive factory acceptance test (FAT) and related simulation testing is performed on the actual site-specific configuration, how will the user know with certainty that, for example, 99 % of the time, all protection trip messages will be received in less than 4 ms and the other 1% of the time they will be received in say 6ms? The answer is that this is not a practical or economical exercise for most companies, due to the difficulty of postulating the explicit worst-case conditions that will break the system during the test, the fact that this test needs to be performed on each and every project, all of which translate into higher cost. It is therefore essential that the overall industry come up with standard performance metrics for all parts of an integrated substation system and specifically

a way of guaranteeing these metrics on paper for each device type and system architecture. In this way, the user will be able to determine in advance with certainty that any proposed system will work, without having to resort to extensive simulation evaluations. Note that this does not imply that an overall FAT is not required; just that the FAT can concentrate on overall correct device configuration and successful message delivery from point to point, treating all IEDs as “black boxes”, without having to count bits on the LAN.

The second issue concerns the routine isolation of IEDs that are members of an all-digital substation for test and maintenance, assuming that no matter what the technology, sooner or later something will fail. For example, consider an IED that performs a bus protection function and trips six breakers via individual IEDs associated with each breaker. When the maintenance person wishes to block the bus protection, does she block the trip outputs at the bus IED alone, the six destination IEDs, or at all places? What if the six destination IEDs also perform other functions that are not required to be blocked with the bus zone? What if the six interoperable destination IEDs are of a different make and model and therefore use different user interface software? It is therefore clear that standardized test procedures and interfaces are required to enable the user to gain an efficient, accurate overall perspective of the system as a whole. Otherwise, errors and confusion will result.

A third issue concerns the maintenance of the substation LAN as a whole. Although it is assumed that suitably reliable architectures are available, again, sooner or later, some part of the LAN infrastructure will have to be maintained. The implication is that many IEDs, spanning multiple protection zones, could be affected, not only by the communications outage itself, but by the fact that the environment will have to safely support the test and restoration of the affected LAN element itself without disturbing the attached IEDs.

A new category of required test is also emerging as a result of the use of higher level substation communications protocols such as IEC 61850. This test is known as a Compliance Test or Conformance Test and is designed to evaluate the communications performance of an individual IED against a standard benchmark, for all standardized functions claimed to have been implemented. These tests are similar to Type Tests, but the focus is on communications. For example, a device implementing the GOOSE message for protection tripping would be exercised against a standard test system to determine if the response to all applied stimuli is exactly as defined in the Standard. Unlike a Type test, a Conformance Test would not necessarily be able to uncover a flaw in an internal protection algorithm that produces states to be transmitted by the GOOSE message. These tests therefore reflect the extent to which individual devices may interoperate correctly via their communications interfaces. Since these tests involve only one device at a time, these tests are not a measure of how an entire system of devices using the tested protocol will perform, especially in areas such as traffic loading (congestion) effects, optimum use of polled commands vs. unsolicited messages, etc.

Testing of distributed schemes utilizing GOOSE (virtual DC wiring) is a separate problem. Consider a classical case of a breaker fail initiate signal distributed by a bus protection to individual BF IEDs. The 61850 Standard supports the concept of test bits – each transmitted signal can be characterized as real (R) or test (T). Unfortunately, the Standard does not mandate how these attributes are asserted, nor how the receiving devices shall respond to such signals. As a result the user is left to configure those bits manually when needed using programmable logic. When integrating various devices the users will have to examine the hard-coded or programmable response of the involved IEDs to the test bits, and finish the application by writing their own logic to ensure the desired response of the entire scheme.

Overall, the idea of test and response requires more development. One could imagine a concept in which both real and test values are processed in parallel or together so that the real values are available for immediate protection action if required, while the test values facilitate testing. This is technically a challenging task. In order for the user to settle on heavy usage of the test bits, the surrounding functions will have to be hard-coded and guaranteed by the vendor who conforms to the Standard. This is not the case today.

The point here is not to discourage potential IEC 61850 users, but rather to raise some important considerations that need good solid solutions to ensure successful and practical application and acceptance by the largest number of users worldwide. Solutions will and are being developed. In the future, engineers will look upon our present practices as archaic, compared to what they will be employing.

4.12 Human Interfaces

Appropriate HMI capabilities combined with the substation LAN infrastructure will allow the IEDs to be the only devices directly connected to substation equipment. In turn, these HMI functions provide the capability to control and monitor the substation both locally and remotely. Traditional hardwired control switches and associated equipment can be totally eliminated. Therefore, the role of traditional functions that are part of established operational procedures such as physical lockout relays needs to be re-considered in this context. With appropriate functional specification and equipment design, all conventional functions may find a logical equivalence in devices incorporating IEC 61850 communications capability. It is recognized that the path to change may not be easy, especially with long established processes and procedures in place. However, in order to achieve progress, it is paramount that users do not confuse existing solutions to functional requirements with the functional requirements themselves.

Adapting to solutions that take advantage of the IEC 61850 based communications is as much a diplomatic and organizational communications problem than a technical one. As new designs are created, it is critical to involve design and field personnel, since they will need time and understanding to make the transition. Many of them are so steeped in the existing solutions (like pistol-grip control switches, lockout

switches, dedicated meters, and separate breaker panels) that they will need time and training to focus on those functional requirements that underlie the existing design, and to accept that they may be able to achieve safe and effective operating procedures with station computer monitor displays, and backup buttons and lights on relay panels. The new design may require human-factors design experts to yield a design that minimizes confusion and risk of error. Few P&C engineers have true human-factors design skills, even though they think they have them.

Flexible HMI capabilities are also emerging that allow, when used with networked devices, a choice of redundant IEDs for primary and backup control, using logic that responds to pre-determined priorities and/or may also automatically switch data channels based on data integrity. This type of application may lead to less expensive and more reliable control architectures where functional duplication can be had for a fraction of the price of past approaches.

It is anticipated that the content of the HMI may expand. Today's coverage includes primary equipment and a very limited amount of information related to the secondary circuits (IED health for example). An integrated substation incorporating any significant replacement of hardwired connections with their digital equivalents should have more sophisticated additional HMI interfaces to allow users to focus on the overall substation at the integrated system level instead of just at the device level. Communication network visualization and monitoring tools are one of the most important aspects. For example, simple to use HMI packages with the necessary underlying functional modules need to be developed to allow quick identification of the overall operational status of all networked IEDs in a station or group of stations. Such a package would be used to recover and display any off-nominal or maintenance-related alarm messages pertaining to the network infrastructure, and its connected devices.

5. Deployment Strategy for IEC 61850

Given the need to develop appropriate system based architectures, tools and procedures for a complete IEC 61850 based substation, the question arises of how to proceed in a managed way so at least some of the benefits of integration may be obtained now.

At present, a very low risk strategy is to utilize IEC 61850 for SCADA applications. Utility grade Ethernet hardware capable of meeting the general response times required for control applications is available off-the-shelf. The end device could be a conventional RTU and conventional operation and maintenance procedures could still apply. Remote retrieval of records (SER, DFR), using the RTU database or an external element such as a gateway to the relay IEDs, is also practical and is the least time critical of any substation application. Data servers with an appropriate power system context are commercially available to implement multi-user systems.

With increasing user demands for remote access to substation

data and the use of generic networking techniques, security also becomes an important issue. Again, adequate technology is available off-the-shelf to implement measures appropriate to an IEC 61850 substation.

With suitable adaptation of operation and maintenance procedures, a migration towards the shared use of protection IEDs incorporating control functions can also be easily achieved now. IEDs that support the necessary functionality and logic are already commercially available. The biggest stumbling block to this approach is not technical at all but is due to the rather long and independent design traditions of these two disciplines. In fact, it is only in the last 10 years or so that protective relays with appropriate system integration capabilities, logic and processing power to achieve this application synergy became available. Many utilities and their suppliers have previously supported the two separate disciplines with legions of specialist staff. Protection and control systems had extremely simple interfaces, usually limited to relay contacts, so designers did not need to know a great deal about the internal intricacies of their counterparts' systems. The challenge is now to recognize the economic and technical opportunities made possible through system integration of all-microprocessor based devices and make appropriate opportunities for staff training and familiarity to make this synergy happen.

The next level of technical achievement is that of carrying time-critical protection trip and initiation signals through the substation LAN and/or process bus. For this to take place, appropriate design performance metrics, along with suitable system level test and maintenance tools and procedures, need to be developed. The ultimate stage is the complete replacement of physically wired ac signals with sampled value data carried digitally. Again, procedural development is required. Both of these concepts will also need the collective approval of the utility industry and its regulators. Such approval may only be obtained through sound engineering specifications and designs, combined with appropriate experience gained through proof of concept projects.

The 61850 Standard requires ten large sections just to define objects and communications services and stacks that support the dramatically new substation design approaches described in this and other application papers. The long development time of the Standard itself (since 1995), and the very gradual introduction of products now leaves users with little practical experience on which to lean so far, even though major and significant 61850 substation projects are now under construction or commissioning. It should be noted that those who implemented UCA based solution do have a foundation on which to build. Overall, how to succeed with 61850 is still a question not answered by the contents of the Standard but only through experience with implementation.

6. Functioning in the IEC 61850 Environment

6.1 Configuration Management

The 61850 Standard presents the opportunity to migrate the

GE Consumer & Industrial
Multilin

IEC 61850

GE Multilin first to market and the only vendor with IEC 61850 across all protection and control applications.

- IEC 61850 across a full product line . . . the Universal Relay
- Embedded IEC 61850 . . . no external Protocol converters
- Builds on 7 years of GE Multilin leadership in open communication standards
- Easy upgrades as new IEC 61850 features become available

IEC 61850 is the new international standard for information exchange and interoperability between intelligent devices within a substation. IEC 61850 lowers the costs and simplifies the engineering, commissioning, operating, and maintenance associated with substation protection and control applications. GE Multilin, the industry leader in open communication standards for protection relays, is best positioned to fully capitalize on the benefits of IEC 61850 through the flexibility, scalability, and common platform of the Universal Relay family.

For more information about IEC 61850, please contact
GE Multilin or visit our website at www.GEMultilin.com/61850



 imagination at work

Simply Advanced...



D90^{Plus}

Advanced Line Distance Protection System Providing Extensive Power Management Solutions

D90^{Plus} intelligent power management solution provides complete and secure sub-cycle distance protection as part of an extensive power management capability. This incrementally scalable system designed for transmission (HV, EHV) and sub-transmission applications converges multiple device functionalities into one easy to use platform.

The difference D90^{Plus} makes for your operations

- Incrementally scalable system based on protection, control, automation, communications, digital fault recording and equipment management requirements
... **Less cost, more value . . . just the right options for your application**
- Simplified modular construction
... **Easy expansion, upgrade and service . . . no stranded investments**
- Remote and local dual-layer security authentication avoids unauthorized access
... **Best in class and beyond security requirements**
- Secure Sub-cycle tripping time to protect critical assets
... **Increased system loading, stability and security**
- True convergence of multiple devices in one platform
... **Reduced external devices, wiring, engineering, commissioning, maintenance and capital costs**

For more information on D90Plus or URPlus, please contact GE Multilin
or visit us at www.GEMultilin.com



imagination at work

large majority of the engineering effort into the configuration of devices. Software tools are envisioned to address almost every aspect of the design process. Existing discussion on the 61850 is almost entirely focused on the design phase – very little attention is given to the post-commissioning activities. The following items are important for effective development as well as management of the 61850-based P&C systems.

Visualization – An important characteristic of 61850 is the free allocation of sub-functions (logical nodes) to any physical device. This introduces the potential for more variability in the IED configuration than was found in pre-61850 devices. As a consequence it is important that new tools present the design in an unambiguous way. Graphical capabilities will aid in this as will the capability to isolate single functions as they might extend across several physical devices.

Collaboration – It is likely that several engineering entities may concurrently develop functions that will reside in the same IED. As such there will be a need for mechanisms that facilitate this. The ability to lock the configuration file or portions of it against editing seems a must. Built-in archiving, revision control and revision history will also be required.

Documentation – Ideally, project documentation should be automatically generated once the initial configuration or modification process is complete. Among other things, this documentation should include all of the information necessary for daily operation of the substation including: descriptions of alarms and their derivations, and interlocking of devices.

Compatibility – Much of the IED configuration will continue to be carried out in the IED configuration tool. For parameters that could be considered as automation-related, there should be no confusion as to where that parameter is configured (in the IED tool or substation configuration tool). Configuration tools should also be capable of importing and exporting relevant data to substation wiring software (CAD) and EMS configuration tools.

Integrity & Security – With more configuration data migrated from hard-wired connections into software parameters, integrity and security of configuration becomes very critical. The vision of 61850 is aimed at fast and easy configuration and modification of the setup. This implies a danger of fast and easy unintended modifications. Archiving at multiple independent data storage centers, strict revision control, strict access, automated compare functions run on the entire configuration and producing change reports for peer reviews are just examples of the new functions that will have to emerge for safe operation of the 61850-based solution.

A fundamental question to be asked with respect to such all-encompassing and heavily relied on substation-level tools is about the market forces eventually yielding mature products. It is obvious that the promised tools aimed at eliminating substantial amount of manual engineering work will have to be quite sophisticated. Given the relatively low volume demand from the power industry, the maturity curve for such tools is questionable.

On the other hand such tools will have to be fully trusted or will not be used at all. Too much is at stake when critical interactions between protection devices such as trip commands

or breaker fail initiate signals are established in software. When altering such signals in a today's hard-wired world, many users re-commission the scheme. Equivalent procedures for reconfigurations done in software will have to be established. This needs to cover both the merit of the change as well as the tools used to implement the change. In today's world the tools are low-tech and are not considered as a factor (hard-wired connections or UCA GOOSE configured by a simple IED level tools).

The substation-level configuration tool is a central piece of software interfacing with multiple software or devices via various files or direct on-line services. This brings the issue of software versions of all the interacting tools, and guaranteed interoperability of the tools each time one of the vendors issues an upgraded version or a patch.

6.2 Firmware Management

Firmware change management is a real and important problem today. The industry is taking the first steps in working out rules for vendor-user interaction in terms of notification of found problems, notification of new firmware versions, advise related to risk of using versions with identified flaws, workarounds versus firmware upgrades, advise regarding amount of re-engineering, re-testing and re-commissioning after upgrading to a new revision, etc [36].

Architectures built upon several IEDs each running an independent firmware, exaggerate this problem exponentially in proportion to the number of independent pieces of firmware.

Assume a stand-alone merging unit is used by several IEDs, and a critical problem is identified in the former forcing its firmware upgrade. Should the firmware change of the merging unit trigger re-testing or re-commissioning of all the IEDs?

Or assume an Ethernet switch requires firmware upgrade to take advantage of new features in the area of message priority queuing, or self-healing capacities (rapid spanning tree). How does one ensure that this upgrade does not affect operation of protection schemes that utilize this particular switch? How does one easily verify that the message priority scheme of the switch works properly after the upgrade?

Obviously these questions apply already to some substation applications, but typically not to the mission-critical protection functions. In the 61850 implied architectures users will face such questions when operating P&C systems that apply high level of integration among truly independent devices (multiple firmware) with not enough segregation into detached portions (interaction between firmware). Note that the high-level goals of the next generation P&C system do not explicitly call for using independent devices from multiple vendors. The goal can be achieved without multiplying the number of interacting pieces of firmware: either by reducing the number of independent instances of firmware or by reducing interactions between them.

The 61850's answer to the problem is outlined in Part 10 of

the Standard, and is based on standardized interoperability testing. It is assumed that compliance of a given device with the “golden sample” of test procedures and scripts, guarantees automatically unchanged performance in the real-life environment and applications.

Three issues can be identified with respect to this approach.

First, a large number of permutations are to be covered while testing for conformance. To certify a device for any possible application, one would have to exercise substantial amount of combinations resulting from various applications and their possible configurations, variability in the interacting external equipment during the test, reference conditions in the areas of networking (other data traffic), or power system response (avalanche models). Such testing would be extensive, require considerable time and effort, and thus generate an extra cost. Self-certification by a vendor – as a possible solution to the time and cost implications – is of little value strictly speaking. An independent certification/re-certification is a new step compared with today’s practice and would have to be factored into the cost and project completion time equations.

Second, independent certification testing of building blocks does not necessarily guarantee proper response of the large system. One reason for this is that the fact of compliance has already many shades. Tens of technical issues (“T-issues”) have been already identified in the body of the 61850 Standard. An electronic on-line data-base has been created to catalog and manage those errors, ambiguous items, or proposed enhancements. Assume 100 T-issues being active. In theory each conformance certificate shall list all T-issues and spell out compliance with respect to every single one, in order to provide complete information regarding the test subject. This, in theory would result in 2^{100} shades of compliance ($1.2677 \cdot 10^{30}$). In practice the situation is obviously simpler as any given application limits the relevance of any particular T-issue. The task of tracking and sorting out the relevant and not relevant compliance items remains, however, in front of the user. It seems that by design, at least for some time, compliance with the 61850 is a moving target. This might be acceptable for SCADA applications, but would face acceptance issues in the protection world.

Third, the concept of reference tests has some weakness in it too. The 61850 Standard is a broad collection of rules for communication. Updates, clarifications, and enhancements will be a big part of it for a period of time. In addition, vendors and users are to decide what and how to implement in the areas not mandated by the Standard. This would put the test software and hardware under the constant pressure to evolve in order to catch up with modifications and clarifications of the Standard itself (T-issues) as well as developments in the existing products. As a result, a complex and evolving software (IED under test) is tested against another complex and evolving software (test facility). In the low probability / high impact domain of protective relaying the above scenario will not necessarily be easily acceptable. Again, the above remarks relate to mission-critical protection functions, and not to relatively simple SCADA portion of the 61850 package.

6.3 Routine Testing

Test facilities are required in a P&C system in order to verify that:

- The hardware is healthy.
- The firmware functions as specified.
- The device has been configured correctly.

In the past the interface between relays were hard-wired through test switches that provided convenient points for injecting and monitoring. New schemes that incorporate peer-to-peer signaling over a local area network require equivalent internal points for forcing and monitoring of signals. These should permit the testing without the requirement to change the configuration of the device. Additionally, these points should not be impacted by the IED configuration; implying that they be embedded within hard-coded functions (Figure 11).

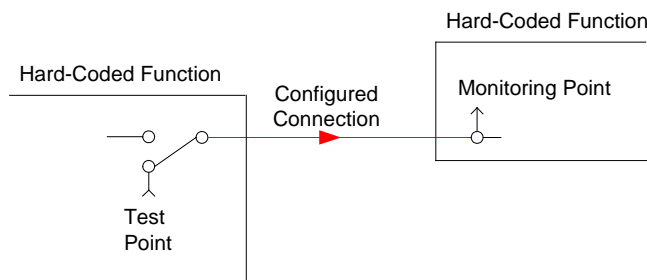


Fig. 11. Embedded test facilities.

Test facilities should also permit testing to be carried out in a staged manner. For example, in a system with redundant A & B protections, one scheme may safely be removed from service while leaving the breakers in-service.

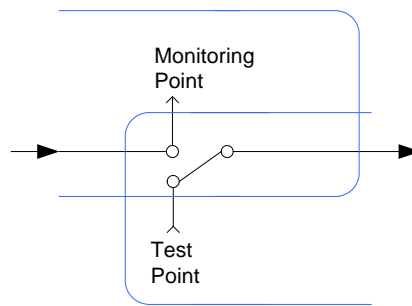


Fig. 12. Overlapping test facilities.

The trip and breaker failure initiate signals are tested up to an open test point. At a later date, a breaker may be removed from service and the remainder of the signaling path can be verified. This capability requires an overlapping of test facilities as shown in Figure 12.

61850 allows for the free allocation of logical nodes to physical devices. Accordingly there is the potential for more variability in the design of the system. As such, the facilities should be flexible enough to permit convenient testing of any scheme.

Traditionally, test switches were physically located adjacent to the associated protection. This was done in order to reduce human errors when operating in live stations. For instance, in

the transformer zone example of section 4.10, test switches would be placed between the lockout relay and the outgoing breaker trips. Referring to the distributed lockout logic it is seen that this point now extends into another physical device that may be located on a different panel. A solution to this problem is to send a message to the remote device to indicate that the distributed function has been locally placed in test. The function would operate normally but its outputs would be inhibited.

Finally, a well thought-out user interface should be provided that clearly presents the test state of the device, gives access to internal test points and displays the results of a test. Ideally,

are still missing pieces, new products announced but yet to be launched, and a host of unanswered questions; with architecture, reliability and application gaps topping the list.

How does a prospective user proceed without undue risk? If the utility is looking at either an all-new (Greenfield) substation project, or a complete replacement of the P&C at an existing station (such as a new drop-in control building), it is relatively easy to make a business case, and to plan on a simple hardware configuration that minimizes wiring and fully utilizes the 61850 opportunity. If one plans on installing such a system, there is no easy fallback to conventional P&C panels, so it is critical to

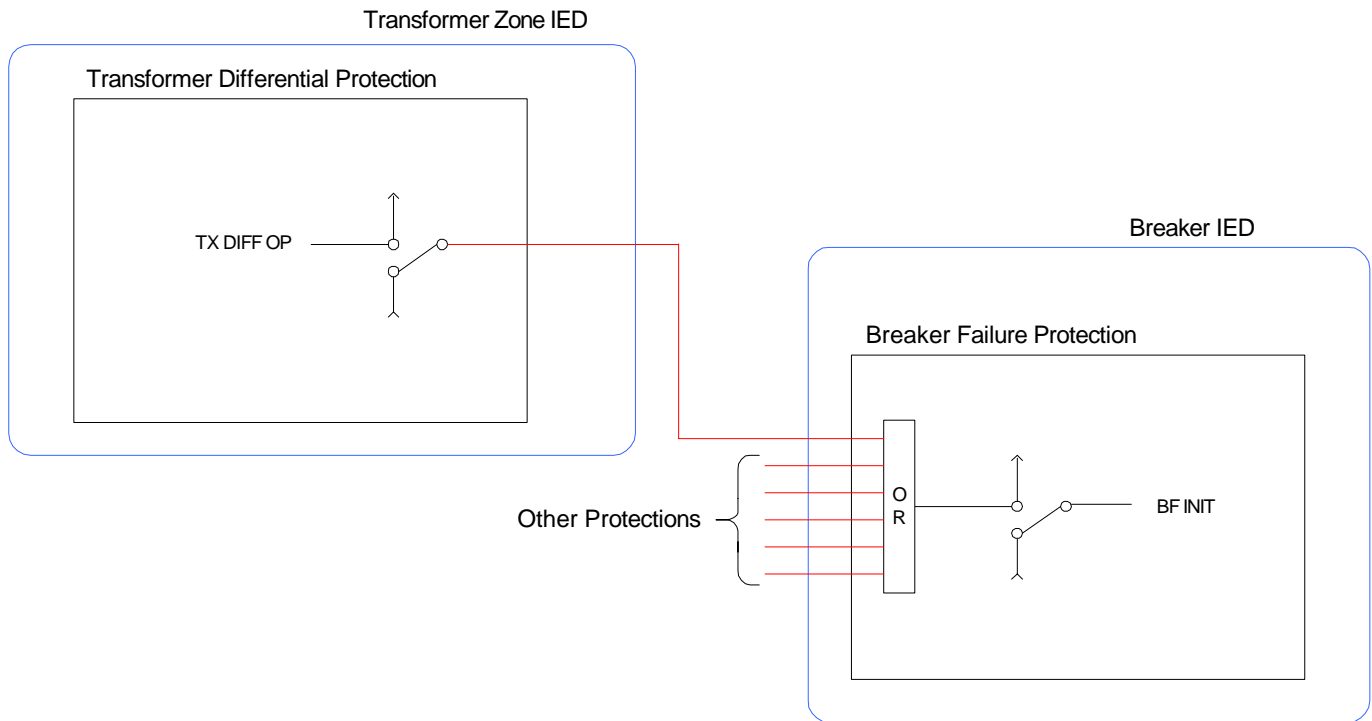


Fig. 13. BFI example.

the interface should support the development of automated tests and should be interoperable with the latest generation of secondary injection sets. The interface should also be designed to minimize the chance of errors. Solutions such as the ones described need to be examined in detail by authorities who operate and maintain these systems since they have significant impact on the final architecture of the substation automation system.

7. Conclusions and Recommendations

It is clear that the concept of IEC 61850 offers a powerful opportunity to save utilities money through the higher integration and interoperability of historically separated and individually hard-wired systems. Now, significant attention needs to be placed on practical application design, operation and maintenance considerations from the user perspective.

It has become clear to a number of utilities that development has reached the point where it pays to commit to substation design based on IEC 61850 communications. That said, there

work with vendors and integrators who are willing and able to guarantee that the critical components will be available and tested before the substation commissioning date. Confirm the following when selecting equipment and service vendors:

- A. For 61850 LAN-based protection and control with reduced wiring and panel equipment, the most critical 61850 component that must be complete and work correctly is GOOSE/GSSE control messaging, so focus most heavily on the development status of these services in the relays or IEDs to be used. If the design depends on LAN control in lieu of wiring and GOOSE is not working, there is no fallback position.
- B. For communications of operational (SCADA/EMS) and non-operational (maintenance, asset management, operations logging and recording, etc.) the station can function either with 61850 object communications, or with older protocols that function on an Ethernet LAN, so there may be temporary or permanent fallback positions for 61850 shortfalls.

- C. If the vendor is pressed to develop a needed capability and the development schedule seems optimistic or aggressive, identify in advance what a fallback position is (e.g., talk to SCADA with DNP3 messages that require manual configuration, rather than with convenient self-configuring and self-describing 61850 objects). Identify a date by which a decision must be made if the fallback implementation is to be available on time. If the new 61850 feature is not ready and proven by that date, carry out the fallback plan and wait for the next station to use the new feature.
 - D. Keep in mind that communications of 61850 defined objects requires both servers and clients. For example, the selected relays may have a full implementation of 61850 object communications, but the SCADA/EMS concentrator or host device must have the ability to request data it needs according to 61850 methods. The same is true for a local user interface computer.
 - E. Note that 61850 protocol packets and other types of Ethernet traffic can coexist on the same LAN – there is no requirement that every message be in 61850 format. It is critical to understand and accept this if some services cannot be initially commissioned using 61850.
 - F. Among the many devices to be integrated at a modern substation, many will certainly not offer 61850 communications yet. 61850-capable relays or relay concentrators are available now. But consider transformer gas-in-oil analyzers, top-oil temperature sensors, weather stations, or capacitor bank controllers – few will have Ethernet communications of any sort, and the protocols will be older standards like Modbus or DNP3. The P&C architecture must provide some network interface devices on the LAN that can convert these older or serial protocol messages to a LAN 61850 or other message format.
 - G. Use off-the-shelf products, which the vendor has demonstrated at other sites, if available.
 - H. For new products, obtain management-level guarantees from the supplier that the equipment will be ready for testing and commissioning according to the utility construction and operating schedule, with some concrete consideration to insure delivery and performance.
 - I. For first-time use of new products, the user can drastically reduce risk by engaging the manufacturer and/or integrator to deal with product settings and communications interfacing issues, and to commission a working system on schedule, as part of the job. If the user buys products and commits to carry out the system integration in-house on this first use, there is high risk of problems and delays for which the vendor may not assume responsibility.
 - J. The user who wants to introduce a 61850 LAN-based substation P&C system in a conservative utility environment must be a diplomat and be sensitive to the organizational issues caused by change. There must also be an adequate budget for introduction of the new technology. Stakeholders around the organization need to be educated on the benefits of 61850 and the reasons for the design changes. Inputs must be sought and discussed, as the 61850 proponents fight hard to get acceptance of the new design approaches and resist fallback to replication of old designs in new equipment. Field personnel will need serious involvement in changes of their work rules and operating procedures, and must become comfortable with new field troubleshooting tools and techniques. A pilot project of meaningful scale, with participation by the most progressive personnel in the organization, can set the pace for future change.
 - K. Plan for tools, training, and utility-site simulators as part of the initial projects.
 - L. Pilot project demonstrations that are not connected to actually do the P&C job (tripping for faults; reporting to SCADA/EMS) tend to fail for lack of attention to detail.
 - M. At many utilities, the P&C organization is disconnected from or at odds with the utility IT organization, not unlike the split between relaying and SCADA/EMS seen at some utilities scores of years ago. For long-term success, the protection and IT personnel need to reach the mutual respect and understanding that will lead to cross-training and mutual support as substation LANs connect to corporate WANs. Transfer of 61850 and other data to the enterprise to run the business better is an important part of the business case for 61850.
 - N. A new 61850 based substation will yield massive data on the daily operations and events at the substation. Design work should include planning for efficient transmission, storage, management, and automated processing of this data to improve utility operations, and to avoid overwhelming personnel who were used to older systems with less to report.
 - O. New 61850 based relays with LAN control have settings or configuration files that define the functionality in the way the panel wiring did in older stations. The user needs a tightly-managed and controlled repository for settings and configuration data, that also ties in product firmware versions and hardware platform issues. The IEEE Power System Relaying Committee is preparing a detailed report on management of relay settings and configuration data. Draft versions are available on-line [35].
- Utilities are applying these methods to engineer new, highly integrated P&C installations.

While this list of issues and cautions may seem daunting,

any new substation design is a big project and requires clear goal definition, in depth planning, and rigorous management to ensure success.

8. Bibliography

- [1] Adamiak, M., Baigent, D., Moore, R., Kasztenny, B., Mazereeuw, J.: "Design of a protection relay incorporating UCA2/MMS communications", Proceedings of the 7th International IEE Conference on Developments in Power System Protection, April 9-12, 2001, pp.98-101.
- [2] Adamiak A., Kulshrestha A.: "Design and Implementation of a UCA-based Substation Control System", Proceedings of the 2001 Georgia Tech Protective Relay Conference, Atlanta, Georgia.
- [3] Amantegui, J., Ojanguren, I., de Carlos, C., Cobelo, F., Quintanilla, R.: "Automation of HV substations in Iberdrola: experiences and plans", Proceedings of the 58th Annual Conference for Protective Relay Engineers, College Station, TX, April 5-7, 2005, pp.194-200.
- [4] Andersson, L., Brunner, C., Engler, F.: "Substation automation based on IEC 61850 with new process-close technologies", Proceedings of the 2003 IEEE Power Tech Conference, Vol.2, June 23-26, 2003.
- [5] Apostolov, A., Brunner, C., Clinard, K.: "Use of IEC 61850 object models for power system quality/security data exchange", Proceedings of the 2003 CIGRE/PES Quality and Security of Electric Power Delivery Systems International Symposium, October 8-10, 2003, pp.155-164.
- [6] Apostolov, A., Ingleson, J.: "Verification of models in protection related analysis programs", 57th Annual Texas A&M Conference for Protective Relay Engineers, College Station, TX, March 30 -April 1, 2004, pp.339-349.
- [7] Apostolov, A., Muschlitz, B.: "Object modeling of measuring functions in IEC 61850 based IEDs", Proceedings of the 2003 IEEE Transmission and Distribution Conference and Exposition, Vol.2, Sept. 7-12, 2003, pp.471-476.
- [8] Apostolov, A., Vandiver, B.: "Functional testing of IEC 61850 based IEDs and systems", Proceedings of the 2003 IEEE Transmission and Distribution Conference and Exposition, Vol.2, Sept. 7-12, 2003, pp.640-645.
- [9] Apostolov, A.P.: "Distributed protection, control and recording in IEC 61850 based substation automation systems", Proceedings of the 8th IEE Conference on Developments in Power System Protection, Vol.2, Amsterdam, April 5-8, 2004, pp.647-651.
- [10] Apostolov, A.P.: "IEC 61850 distributed analog values applications in substation automation systems", Proceedings of the 2005 IEEE Power Engineering Society General Meeting, June 12-16, 2005, pp.2991-2998.
- [11] Apostolov, A.P.: "Integration of legacy intelligent electronic devices in UCA based digital control systems", Proceedings of the 2002 IEEE Power Engineering Society Winter Meeting, January 27-31, 2002, pp.648-653.
- [12] Apostolov, A.P.: "Requirements for automatic event analysis in substation automation systems", Proceedings of the 2004 IEEE Power Engineering Society General Meeting, June 6-10, 2004, pp.1055-1060.
- [13] Baigent D., Adamiak M., Mackiewicz R.: "IEC 61850 Communication Networks and Systems In Substations: An Overview for Users", Proceedings of the VIII Simposio "Iberoamericano Sobre Proteccion de Sistemas Electricos de Potencia", Monterey, Mexico, 2005.
- [14] Baigent D., Adamiak M., Evans S.: "Practical Considerations in Application of UCA GOOSE", Proceedings of the 2000 Georgia Tech Protective Relay Conference, Atlanta, Georgia.
- [15] Brand, K.-P., Ostertag, M., Wimmer, W.: "Safety related, distributed functions in substations and the standard IEC 61850", Proceedings of the 2003 IEEE Power Tech Conference, Vol.2, June 23-26, 2003.
- [16] Brand, K.-P.: "The standard IEC 61850 as prerequisite for intelligent applications in substations", Proceedings of the 2004 IEEE Power Engineering Society General Meeting, June 6-10, 2004, pp.714-718.
- [17] Brunello G., Kasztenny B.: "An Application of a Protection Relaying Scheme using the UCA/MMS Standard", Proceedings of the 2002 IEEE/ PES T&D Latin America Conference, Sao Paulo, Brazil, March 2002.
- [18] Chaturvedi, M.: "Substation IED communications", Proceedings of the 2002 IEEE Power Engineering Society Winter Meeting, January 27-31, 2002, pp.569.
- [19] Crispino, F., Villacorta, C.A., Oliveira, P.R.P., Jardini, J.A., Magrini, L.C.: "An experiment using an object-oriented standard-IEC 61850 to integrate IEDs systems in substations", Proceedings of the 2004 IEEE Transmission and Distribution Conference and Exposition: Latin America, Nov.8-11, 2004, pp.22-27.
- [20] Dood, M.J.: "Integration of non-UCA devices into UCA networks", Proceedings of the 2002 IEEE Power Engineering Society Summer Meeting, July 21-25, 2002, pp.291-293.
- [21] Dupraz, J.P., Schiemann, A., Montillet, G.F.: "Design objectives of new digital control and monitoring of high voltage circuit breakers", Proceedings of the 2001 IEEE Transmission and Distribution Conference and Exposition, October 28 - November 2, 2001, pp.1088-1093.
- [22] Gohokar, V.N., Dhande, T.M., Kabra, S.S.: "Application of information technology in substation automation", Proceedings of the 2004 IEEE Power Systems Conference and Exposition, October 10-13, 2004, pp.635-639.

- [23] Hoga, C., Wong, G., "IEC 61850: open communication in practice in substations", Proceedings of the 2004 IEEE Power Systems Conference and Exposition, Vol.2, October 10-14, 2004, pp.618 – 623.
- [24] Hrabliuk, J.D.P.: "Interfacing optical current sensors in a substation", Proceedings of the 2001 IEEE Power Engineering Society Summer Meeting, July 15-19, 2001, pp.147-155.
- [25] IEEE Std 1646-2004, "IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation".
- [26] IEEE Std C37.115-2003 "IEEE standard test methods for use in the evaluation of message communications between intelligent electronic devices in an integrated substation protection, control and data acquisition system", 2004.
- [27] Jakovljevic, S., Kezunovic, M.: "Software for enhanced monitoring in integrated substations", Proceedings of the 2003 Power Tech Conference, June 2003, Vol.4.
- [28] Keyou Wang, Peichao Zhang, Weiyong Yu: "Applying object-orientation and IEC 61850 standard to architecture design of power system fault information processing", Proceedings of the 2004 IEEE International Conference on Electric Utility Deregulation, Restructuring and Power Technologies, April 2004, pp.785-788.
- [29] Kezunovic, M., Djoki, T., Kosti, T.: "Automated Monitoring and Control Using New Data Integration Paradigm", Proceedings of the 38th Annual Hawaii International Conference on System Sciences, January 3-6, 2005, pp.66a.
- [30] Kezunovic, M., Taylor, H.: "New solutions for substation sensing, signal processing and decision making", Proceedings of the 37th Annual Hawaii International Conference on System Sciences, January 5-8, 2004, pp.59-67.
- [31] Kostic, T., Preiss, O., Frei, C.: "Towards the formal integration of two upcoming standards: IEC 61970 and IEC 61850", Proceedings of the Conference on Engineering Large Power Systems, May 7-9, 2003.
- [32] McDonald, J.D.: "Substation automation. IED integration and availability of information", IEEE Power and Energy Magazine, Vol.1, No.2, Mar-Apr 2003, pp.22-31.
- [33] National Institute of Standards and Technology, Engineering Statistics Handbook, Assessing Product Reliability (<http://www.itl.nist.gov/div898/handbook/apr/apr.htm>).
- [34] Ozansoy, C.R., Zayegh, A., Kalam, A.: "Interoperable CORBA middleware design for substation communication system", Proceedings of the 8th IEE Conference on Developments in Power System Protection, Vol.2, Amsterdam, April 508, 2004, pp.705-708.
- [35] Power System Relaying Committee, Working Group C3 "Process, Trends, and Issues with Relay Settings" (<http://www.pes-psrc.org/> under Subcommittee C)
- [36] Power System Relaying Committee, Working Group I3 "Microprocessor-Based Relay Firmware Control" (<http://www.pes-psrc.org/> under Subcommittee I)
- [37] Reckerd, D., Vico, J.: "Application of peer-to-peer communication, for protection and control, at Seward distribution substation", Proceedings of the 58th Annual Conference for Protective Relay Engineers, College Station, TX, April 5-7, 2005, pp.40-45.
- [38] Roussel, P., Dupraz, J.P., Montillet, G.: "Non-conventional current transformers on live tank circuit breakers", Proceedings of the 2001 IEEE Power Engineering Society Winter Meeting, January 28 – February 1, 2001, pp.306-311.
- [39] Sagareli, S., Gelman, V.: "Implementation of new technologies in traction power systems", Proceedings of the 2004 ASME/IEEE Rail Conference, April 6-8, 2004, pp.141-146.
- [40] Sanz, R.: "Embedding interoperable objects in automation systems", Proceedings of the 2002 IEEE 28th Annual Conference of the Industrial Electronics Society (IECON 02), November 5-8, 2002, pp.2261-2265.
- [41] Schubert, H., Wong, G.: "IEC 61850 - The future global standard for seamless and vendor-independent communication within substations", Proceedings of the ASDCOM International Conference on Advances in Power System Control, Operation and Management, November 11-14, 2003, pp.462-466.
- [42] Serizawa, Y., Satoh, S., Tanaka, T., Oikawa, A., Miyazaki, K., Izena, A.: "Preliminary case studies on common information exchanges for power system management", Proceedings of the 2004 IEEE Power Systems Conference and Exposition, October 10-13, 2004, pp.263-268.
- [43] Shephard, B., Janssen, M.C., Schubert, M.: "Standardised communications in substations", Proceedings of the 7th IEE Conference on Developments in Power System Protection, Amsterdam, April 9-12, 2001, pp.270-274.
- [44] Skeie, T., Johannessen, S., Brunner, C.: "Ethernet in substation automation", IEEE Control Systems Magazine, Vol.22, No.3, June 2002, pp.43-51.
- [45] Skeie, T., Johannessen, S., Holmeide, O.: "Highly accurate time synchronization over switched Ethernet", Proceedings of the 2001 18th IEEE International Conference on Emerging Technologies and Factory Automation, October 15-18, 2001, pp.195-204.
- [46] Steinhauser, F.: "New challenges with substations utilizing communication networks", Proceedings of the 2003 IEEE Power Tech Conference, Vol.2, June 23-26, 2003.

- [47] Villacorta, C.A., Jardini, J.A., Magrini, L.C.: "Applying object-oriented technology to project hydroelectric power plant SCADA systems", Proceedings of the 2003 IEEE Power Engineering Society General Meeting, July 13-17, 2003, Vol.2.
- [48] Wang, K., Zhang, P., Yu, W.: "Implementing research for IEC 61850-based fault analysis system", Proceedings of the 8th IEE Conference on Developments in Power System Protection, Vol.2, Amsterdam, April 508, 2004, pp.772-775.
- [49] Yalla, M.; Adamiak, M.; Apostolov, A.; Beatty, J.; Borlase, S.; Bright, J.; Burger, J.; Dickson, S.; Gresco, G.; Hartman, W.; Hohn, J.; Holstein, D.; Kazemi, A.; Michael, G.; Sufana, C.; Tengdin, J.; Thompson, M.; Udren, E.: "Application of peer-to-peer communication for protective relaying", IEEE Transactions on Power Delivery, Vol.17, No.2, April 2002, pp.446-451.
- [50] Yin, Z.L., Liu, W.S., Qin, Y.L., Yang, Q.X.: "The investigation of the serial communication between the process level and the bay level of the substation automation system", Proceedings of the 8th IEE International Conference on Developments in Power System Protection, April 5-8, 2004, pp.718-721.

Annex A.

Protection and Control Today – Back to Basics

This Annex discusses some of the basics of protection and control as successfully used for decades. Majority of these general requirements will have to be retained by new communication-based solutions. It is important to distinguish between the key need, and the present way of accomplishing the need (current implementations are ways of meeting functional requirements, not the functional requirements themselves). While users will have to re-think and adapt to different ways of accomplishing the basic requirements, architects of the new systems must factor in all the basic principles that constitute the protection and control engineering field.

This Annex touches on several key aspects, and proposes a simple arbitrary benchmark (Figure A-1) for discussing both the principles and new solutions. Too often proposals for communications based protection systems tend to neglect the actual number and location of CTs, disregard the principle of overlapping zones, maintainability, redundancy, and other practical aspects. This paper encourages using benchmarks such as the one in Figure A-1 when presenting new P&C architectures, particularly solutions involving merging units and similar approaches.

A.1 Zones of Protection

The zone of protection refers to that primary equipment for which faults are detected by a given protection scheme. The protection scheme is defined by the relays and their measuring CTs and VTs. Interrupting devices (circuit breakers, circuit switchers, etc.) that are operated by the protection scheme must be arranged remove all sources of energy from within the protection zone. Ideally, a protection zone is confined to a single primary device such as a transformer or a bus. Limitations on the location of instrument transformers and interrupting devices may result in larger zones. Protection zones must overlap in order to provide coverage for all primary equipment. This typically results in breakers falling into multiple zones.

A.2 Allocation of IEDs to Zones of Protection

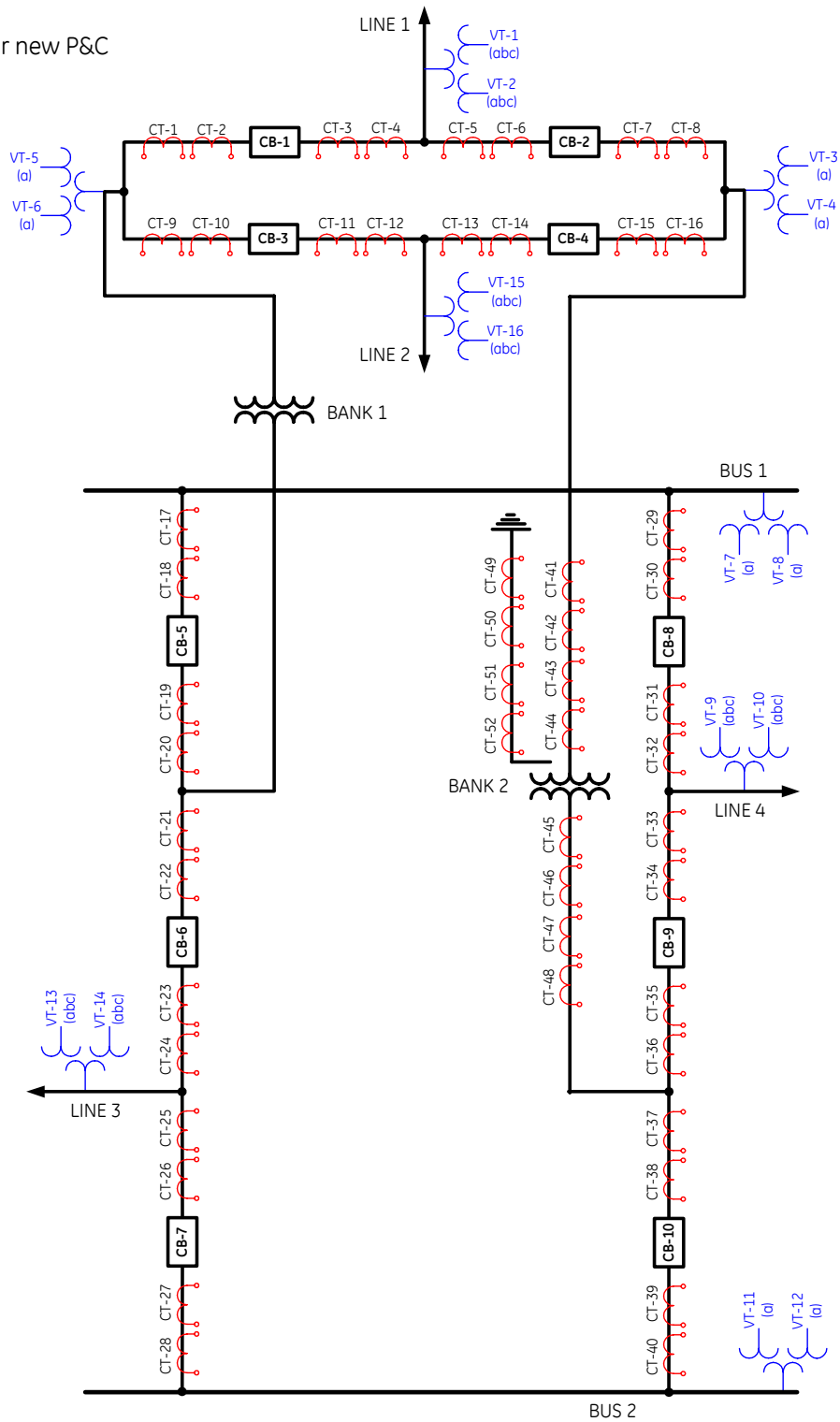
Typically an IED or relay is dedicated to the protection of a single zone. In this way a failure of this device or its algorithms compromises a single zone. IEDs may provide backup protection to other zones. In this case coordination is often required. When required, redundant IEDs may be assigned to the same zone. Redundancy may also be extended to the DC supplies, measuring CTs, breaker trip coils, relay panels, and cable routings. Redundant IEDs may use different operating principles or be manufactured by different vendors. Redundant protection generally provides increased reliability and shorter clearing time when compared with backup protection at the expense of increased cost and complexity. Redundant protection also allows one IED to be taken from service for maintenance while the primary equipment remains in-service, protected by the other IED.

The requirement to keep primary equipment in-service also affects the topology of the substation itself. For instance 1½ breaker, ring bus, or double bus configurations are often implemented at higher voltage levels. In these cases it may be useful to allocate IEDs to breakers as well as to protection zones. For instance, a 1½ breaker, line terminal may consist of redundant line distance or line differential IEDs protecting the transmission lines and an IED for each of the associated breakers. The breaker IED is responsible for breaker failure, auto-reclosure, synchronized closing and interlocking. In future, the breaker IED could be considered to be the sole interface point for all protection and control functions associated with the breaker, including SCADA.

Routine maintenance can be carried out on each of the redundant line protections (one at a time) with all primary equipment in-service. Additionally each breaker and its associated IED can be taken from service (one at a time) for maintenance purposes.

Fig. A-1.

Possible benchmark case for new P&C architectures.



There is a value in separating protection functions and keeping them aligned with the zones of the primary equipment. Some reasons for maintaining this separation are the avoidance of common-mode failures, maintenance of a clear separation of systems under test and to facilitate easy expansion and/or retrofitting the system in modular blocks.

A.3 Allocation of P&C Functions to IEDs

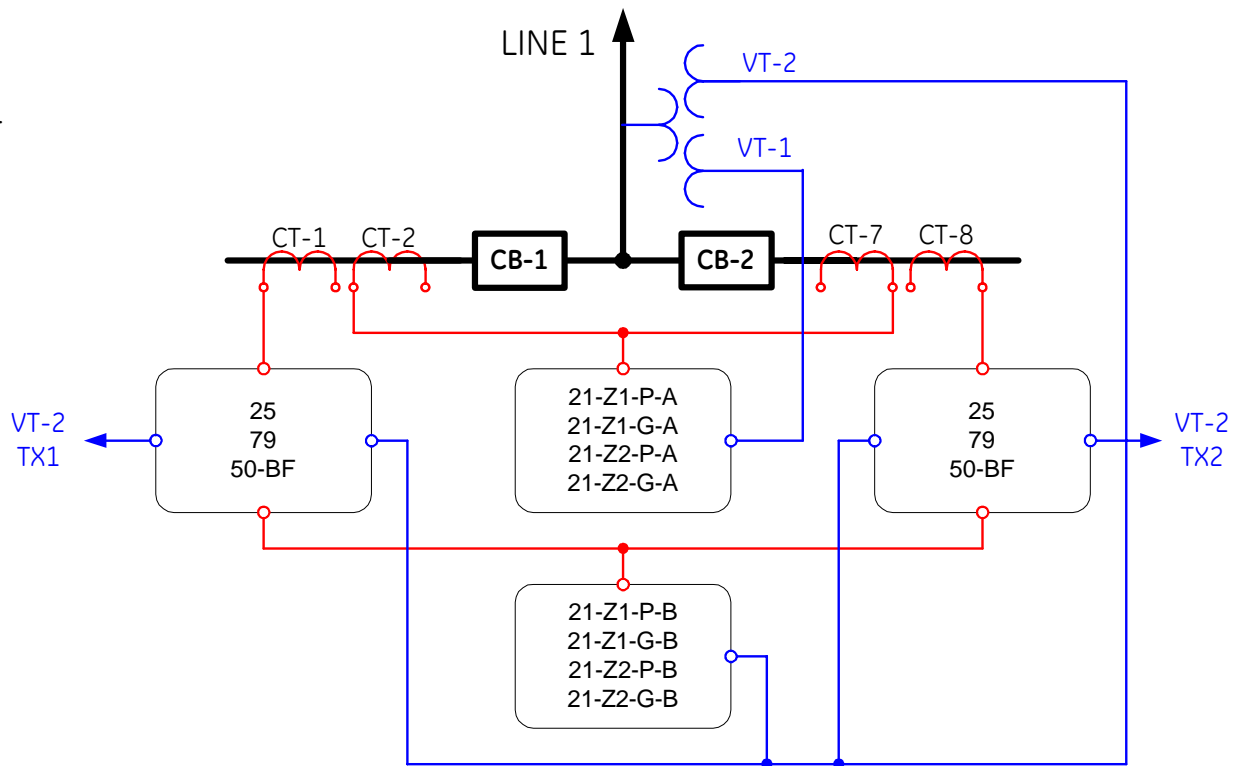
Conventional protection schemes were initially developed using electro-mechanical relays. These devices often performed one or two functions only on a per-phase basis. While these schemes required a lot of panel space and wiring, they also benefited from inherent redundancy. For example, a feeder scheme could consist of three single-phase IOC/TOC relays and a ground IOC/TOC relay. This meant that 2 relays were expected to operate for many fault types (with the exception of a low magnitude

ground fault). In microprocessor relays much of this inherent redundancy is lost. As such, when the protection designer is assigning functions to a multifunction device, he/she needs to consider the implications of the loss of all these functions when the IED fails. Conversely, integrating more functions into a single device results in fewer IEDs and a simpler overall design. Historically, functions were separated within one protection group because there was no other choice. Integrating functions within a group doesn't necessarily lessen reliability in a fully-duplicated scheme because common failures have always existed. For example, losing the A-system DC supply breaker,

A.4 AC Signals

Most protection schemes utilize voltages and currents measured via conventional CTs and VTs. CTs typically have nominal secondary current ratings of 1A or 5A. VTs typically have nominal secondary phase-neutral voltage ratings of 57V to 120V. CTs may serve several IEDs wired in series. If so, the protection designer needs to consider the consequence of a failure of a cable or CT on the overall scheme. Test facilities (see A.6) should also be designed in such a way that an IED may be isolated from the system without interrupting the current to other IEDs. The IEDs of

Fig. A-2.
Example of
allocating P&C
functions to IEDs.



could affect two panels worth of discrete elements just the same as it would affect the functionally identical scheme implemented in one completely integrated IED in a 4N case.

For another example one can consider again the line terminal shown in Figure A-2. Traditionally the functions shown in the breaker IED (synchrocheck, auto-reclose, and breaker failure) were not duplicated. The protection designer may decide to reduce the number of IEDs by merging these functions into one of the line protection IEDs. If so, consideration must be given to the interruption of these functions during routine maintenance. Another consideration is the potentially large tripping exposure to a mal-function. It is probably warranted to duplicate these functions in both IEDs. However, this approach may require careful consideration. For example, allowing two auto-reclose schemes to operate in parallel could lead to unexpected and unwanted behavior especially for single-pole tripping.

redundant systems are often fed from separate CTs. The cabling may be routed over different paths for additional redundancy. If the redundant IEDs share the same panel, the cabling may then terminate on different sides of the enclosure. VT signals are more likely to be shared by multiple IEDs. If so, fuses are typically installed throughout the circuit. These devices must coordinate in order to ensure that a fault in the voltage circuit impacts as few IEDs as possible. VT fuse fail schemes should supervise protection schemes that are predisposed towards false operation for a failure in the voltage circuit.

Almost all protection applications require their input AC signals to be time-aligned. This calls for synchronization of measurements of these signals, either with respect to one another or with respect to the absolute time. Today, this requirement is achieved by bringing all signals into a single IED and processing them synchronously within the device with respect to an internal arbitrary time

scale. With the exception of some line current differential applications, protection functions today do not depend on any external time synchronization source.

A.5 DC Signals

Protection schemes often utilize signals from other schemes or from field devices (circuit breakers, etc.). Contacts are wetted from the station battery to feed auxiliary relay logic or the inputs of IEDs. In large stations, miles of control cabling are sometimes required to route these signals. As such, station batteries are typically ungrounded and are equipped with battery ground detection in order to allow station personnel to detect and repair cable faults. Even so, incorrect status information due to faulty circuitry is inevitable and must be planned for in the design. In general, a protection scheme should not produce a critical response (i.e. trip a breaker) based solely on a status input. For example, in line distance applications, permissive transfer tripping is more secure than direct transfer tripping because the former requires a protection element to pickup simultaneous to receipt of the permissive signal. In applications where this principle cannot be adhered to, the scheme should use multiple status signals for additional security. For example, a scheme that uses both the normally open and normally closed breaker status contacts can be designed to discriminate between correct and abnormal indication.

In the redundant systems the signals for each scheme are usually derived from different devices or field contacts. These signals are segregated onto separate cables. The cables may be routed via different paths within the station. In very critical stations there may be separate batteries for the redundant systems. This reduces the system exposure to battery grounds.

Critical dc signals such as trip, close or breaker failure initiate can be equipped with test facilities to allow safe isolation of those signals from the rest of the system.

A.6 Testing and Test Facilities

Provisions are made in every protection scheme to facilitate commissioning, routine maintenance, and troubleshooting. Switches are often inserted between the measuring VTs and CTs and the IEDs. These serve as points at which the relay can be isolated for troubleshooting or for secondary injection testing. They also serve as measuring points for the secondary currents and voltages. Switches are also often inserted into the DC circuits. These may be used to isolate trip and close commands to breakers. They may also be placed at intermediate points within the protection scheme logic or between protection schemes in order to verify specific functions or logic.

Facilities may also be provided by the IEDs themselves in the form of monitoring points, targets, or LEDs. In some cases dedicated schemes are designed using rotary test/normal switches, pushbuttons, and indicating lamps. An example of this is the transmit/receive test facilities associated with the pilot scheme of a line terminal. As protection schemes become more integrated and IED counts go down, there will be a greater need for internal IED test capabilities. Internal facilities must be designed in such a way that the user will have the same degree of confidence in the outcome of the test as was attained with external test facilities. They should also be flexible, user-friendly, and give unambiguous feedback on the state of the test.

In general, it is worth considering the six general categories of tests traditionally applied to existing P&C systems and the reasons for each.

Type Tests are extensive tests usually performed by the manufacturer and are intended to uncover basic flaws in the design of a product or system. Type tests include a full range of performance and environmental tests that subject the equipment under test to the maximum possible stresses it is likely to ever experience in-service. Type tests are also intended to prove that a particular system actually meets its stated functional and performance specifications. A major part of testing digital systems is the verification of software performance under a variety of externally simulated conditions designed to uncover any weaknesses at the specified performance levels. In tests of protective relays, external digital simulators capable of modeling actual power system behavior are used to drive power amplifiers supplying actual signals in the correct range of the CT and VT inputs of the relay under test. In this case, the relay under test is treated as a "black box". Type tests are generally complicated and expensive to perform and are therefore done only at the time of initial product design and any subsequent major revisions.

Production Tests are tests performed on a regular basis on every unit produced and are intended to uncover variations in product quality due to manufacturing tolerances, assembly errors, etc. Production tests are usually performed by connecting sub-assemblies or the complete unit to a test jig that exercises the system using a pre-determined test script. For example, a communication port might be tested by presenting a series of test messages and looking for certain expected responses within a specified time window and with all transmission parameters within specification. A complete "black box" test (reduced in scope relative to a type test), may be performed at final assembly.

Commissioning Tests (also known as a site acceptance test or SAT) are tests performed during the initial commissioning of a P&C system in the field. Commissioning tests are intended to uncover errors in wiring and other installation errors. Commissioning tests are also used to uncover errors in entering the applied relay settings, for example a circuit breaker trip contact was not linked to the output of a distance zone 1 element, but are not intended to verify the design of the relay internal software itself. This is a point that sometimes uses up much utility time and effort. Once a particular relay has passed its type tests and the design is frozen, the programming and basic performance of all its internal elements cannot subsequently change. The effectiveness of commissioning tests on software is essentially limited to verifying that the user-accessible configuration settings have been entered and function as intended for the particular application. Commissioning tests done in the field per se can not uncover power system calculation errors leading to an incorrect choice of, for example, zone 1 reach setting. Certain consistency checks such as simple rule of thumb calculations are easy to do and may uncover errors in the settings. Commissioning tests are often concluded by performing a live test trip of the protected zone to absolutely ensure that all circuit breakers will trip as intended.

Maintenance Tests are tests performed at routine intervals of typically every four years or more to uncover any deterioration in the overall performance of a P&C system. Historically, maintenance intervals were shorter when P&C systems were largely comprised of electro-mechanical elements that were subject to the effects of dirt, oxidation, heat, etc. However, the advent of digital systems with extensive self-monitoring capabilities has significantly lessened the requirements for routine tests of the P&C system itself. For example, once commissioned and placed in-service, IED self-checks such as memory checksum routines ensure that a digital relay will perform its mission indefinitely without any degradation in the settings configuration possible. Certain parts of the IED, such as the analog to digital converter subsystem, may be subject to small drifts in gain over long periods. Many IEDs also incorporate mechanisms such as standard value tests that are automatically applied on-line, thus essentially eliminating the need to test the A/D converter on a routine basis. In order to take full economic advantage of the capabilities of modern P&C systems, the most important consideration when contemplating a maintenance test is to test only those parts of the overall installation that can actually change while in-service. The parts that can not change unless manually interfered with such as software may generally have the maintenance substantially reduced to a broad overall functional check.

Factory Acceptance Tests (FAT), as the name implies, are tests typically performed in the factory on an overall integrated system, such as a collection of protection IEDs, communication interfaces and control components comprising the complete installation for an entire substation or major sub-division thereof. FATs typically use either standard or customer-specific performance targets and are intended to ensure that the whole assembly will perform as expected in the field. Typical areas considered are I/O loading, buffer capabilities and overflows, communications performance and in some cases, environmental performance. The main difference between a production test and a FAT is that the production test is usually concerned with one item at a time, such as an IED, or individual modules going into an IED; whereas an RTU or equivalent unit is usually a composite of several individual items or modules that are assembled into a cabinet for a project-specific application.

A.7 Lockout Relays

Utilities usually lock out the breakers surrounding a permanent equipment failure. This is done for internal transformer faults, bus faults and failures of breakers. One or more protection devices may initiate operation of a lockout relay (ANSI 86). This is a bi-stable device that remains in the operated state after reset of the initiating protection. The lockout relay provides sustained tripping commands to all of the breakers making up the zone and blocks all the possible means of closing said breakers. The intent is to prevent re-energization of the equipment until a local inspection has been carried out. Accordingly, the lockout relay is usually hand-reset. Due to its simplicity, the lockout has a high reliability. Monitoring of the lockout coil (either by placing a lamp in parallel with the initiating device or through the use of a coil monitoring relay) further increases the availability.

A.8 Human Interfaces

Human interfaces are necessary to provide status on the operational state of the scheme. Often both local and remote indications are required. Targets, LEDs, and annunciator panels capture operational information such as the particular element that has operated, the phases involved, and whether or not reclosure was successful. Status is also provided on the health of the protection scheme; including IED failure, loss of DC, VT fuse failure, and trip coil failure. The interface is typically nonvolatile and capable of capture of fleeting events. The human interface usually permits limited reconfiguration of the protection scheme such as setting group control or blocking of autoreclose. Sequence of event systems (either centralized or integrated to the IED) provide a

time stamped record of important occurrences within the substation. Disturbance recorders (either centralized or integral to the IED) capture raw voltage and current waveforms during system faults or other disturbances. This data may be used for operational purposes or to verify the performance of protection systems.

Also, various means of operating the equipment are provided via reliable interfaces such as pushbuttons, pistol-grip switches, etc. These devices are known to the existing work force and extremely reliable.

A.9 Availability of Protection

The reliability of the protection scheme is a function of the reliability of the individual components and the inter-relationship between these components. The earliest protection schemes were built from single function, electromechanical protection & auxiliary relays that were hard-wired for the particular application. Due to the simplicity of the constituent elements, the reliability of these schemes was very high. However, a component failure could go unnoticed until maintenance was carried out or a fault occurred.

A protection scheme of the current generation may consist of a single multifunction IED and its associated wiring. The IED has many more components than the simple devices of the past. Therefore the IED should have a correspondingly higher rate of failure. This disadvantage is offset by the fact that microprocessor-based devices are capable of performing self-diagnostics. In a properly designed system, most IED failures will be quickly identified, the failed component replaced, and the system returned to service in a minimal period of time. The availability of such a scheme can be much better than otherwise anticipated.

As protection schemes continue to evolve our notions on system availability should reflect the underlying components. Redundancy may be added in areas where it was not previously required, however, the total installed cost of the installation could still be much lower than in conventional practice.

With all protection functions allocated between one or two IEDs, availability of such IEDs is directly reflecting on availability of protection for the zone. Typically redundant, independent systems are deployed. Within each system, a zone is protected with the availability of about 100 years of Mean Time To Failure (MTTF). This number is driven by the fact of providing key protection from a single, integrated device. Typically, a failure of such device impacts a single zone of protection, and does not spread into larger portions of systems A or B protection.

Similarly, such a device could be intentionally taken out of service, and the affected area is both contained and well defined.

Today's protection functions do not depend on sources of time or communication equipment for extensive peer-to-peer communications. If used, the time synchronization and communication devices are treated as a part of the scheme, and are typically isolated from other zones of protection so that their failures or maintenance have limited impact on the overall substation protection system.

Annex B.

Reliability and Availability Calculations

A Poisson distribution is a reasonable model for the failure of components for a "back of the envelope calculations" [33].

The probability distribution function of the failure of a component is typically assumed as:

$$f(t) = \lambda \cdot e^{-\lambda t} \quad (1)$$

The probability of a component failing by time t , or the portion of a population of components that will fail by time t , is given by:

$$F(t) = \int_0^t f(t) \cdot dt = 1 - e^{-\lambda t} \quad (2)$$

The reliability function, the probability that a component will not fail by time t , is given by:

$$R(t) = 1 - F(t) = e^{-\lambda t} \quad (3)$$

The Mean Time To Failure is the expected value of the probability distribution:

$$M = \int_0^{\infty} t \cdot f(t) \cdot dt = \frac{1}{\lambda} \quad (4)$$

Next, one needs rules for series and parallel composition.

In a series composition, an assembly is built from two components, both of which must work in order for the assembly to work. In a parallel composition, the assembly works if either of the components works.

For series composition of two components, the mean time to failure for the assembly is related to the mean times to failure of the components, M_1 and M_2 , by:

$$M_{series} = \frac{1}{\frac{1}{M_1} + \frac{1}{M_2}} = \frac{M_1 \cdot M_2}{M_1 + M_2} \quad (5)$$

For parallel composition, the relation is:

$$M_{parallel} = M_1 + M_2 - \frac{1}{\frac{1}{M_1} + \frac{1}{M_2}} = M_1 + M_2 - \frac{M_1 \cdot M_2}{M_1 + M_2} \quad (6)$$

Next we turn our attention to availability, which is a separate question from reliability. The question of reliability in the context of this discussion is focused on how long it takes for the system to fail, assuming that the system is not repaired as components fail. On the other hand, availability addresses what percentage of the time the system is operational, and includes temporary outages such as loss of power, noise, and temporary loss of communications.

Each subassembly of the system is characterized by the fraction of the time that it is available:

$$A = \frac{\text{up time}}{\text{total time}} \quad (7)$$

Equivalently, a subassembly can be characterized by the fraction of the time that it is unavailable:

$$D = \frac{\text{down time}}{\text{total time}} = 1 - A \quad (8)$$

Next, we need rules for composition. For a series assembly of two independent components, the availability of the assembly is given by:

$$\begin{aligned} A_{series} &= A_1 \cdot A_2 = (1 - D_1) \cdot (1 - D_2) \approx 1 - D_1 - D_2 \\ D_{series} &= 1 - A_1 \cdot A_2 = 1 - (1 - D_1) \cdot (1 - D_2) \approx D_1 + D_2 \end{aligned} \quad (9)$$

The approximations are valid for small values of D.

For a parallel assembly of two independent components, the availability of the assembly is given by:

$$\begin{aligned} D_{parallel} &= D_1 \cdot D_2 \\ A_{parallel} &= 1 - D_1 \cdot D_2 \end{aligned} \quad (10)$$

It is intuitively obvious, and proved by the above equations, that the reliability of components is generally much higher than the reliability of the system. Therefore, the system will fail much sooner than the expected end of life of any of its components.

Consider a system of Figure B-1a. An IED working as a protection relay receives data via network from three

merging units (transformer relay, for example). Each merging unit is synchronized via independent connections from a source of time. Merging units, network, the IED and the synchronization source are designed and manufactured for 150 years of MTTF (1 out of 150 devices fails in a year). All the connections are assumed to have 300 years of MTTF (1 out of 300 connections fails over one year).

In such a system, all components must work in order for the system to work. For such a series assembly, the MTTF is 15.8 years (1 out of 16 systems will fail in a year). This is well below today's standards and will not be accepted by users.

Assume the relative MTTF data for all the components of Figure B-1a remain the same. In order to guarantee 100 years of MTTF for the system, the absolute MTTF values for the components will have to be as in Figure B-1b. For example, the merging units, IED and the network will have to be of 950 years of MTTF, while the connections will have to have a reliability of almost 2,000 years of MTTF. This example is based on arbitrary numbers, but nonetheless illustrates the magnitude of the problem.

Reliability of the system can be improved by eliminating components from the system, providing redundant components, or increasing reliability of individual components. As illustrated in Figure B-1b, the last solution is not a practical one.

Consider alternative architectures shown in Figure B-2.

Figure B-2a assumes the source of synchronization is provided via network. This eliminates connections from the synchronization source to the merging units. There is no redundancy added to this scheme, but the number of components in the system is reduced by two connections (3 removed, 1 added). This increases the system MTTF from 15.8 years to 17.6 years.

Figure B-2b assumes all connections in the scheme to be fully redundant. This implies separate fiber cables and diverse routing of the cables so that the failures are truly independent. Based on equation (6) a redundant component of equal MTTF increases the original MTTF by only 50%. In the case of Figure B-2b, two connections of 300 years of MTTF each yield an assembly of 450 years of MTTF. If so, 1 system of Figure B-2b out of 20 systems would fail within a year (19.6 years of MTTF).

Figure B-2c assumes the synchronization source and the network to be redundant. This brings their arbitrary 150 years of MTTF to 225 years for the system calculations. Now, the architecture of Figure B-2c has the MTTF of 21.4 years.

Figure B-2d eliminates the synchronization source. It is assumed that the host IED is driving synchronization

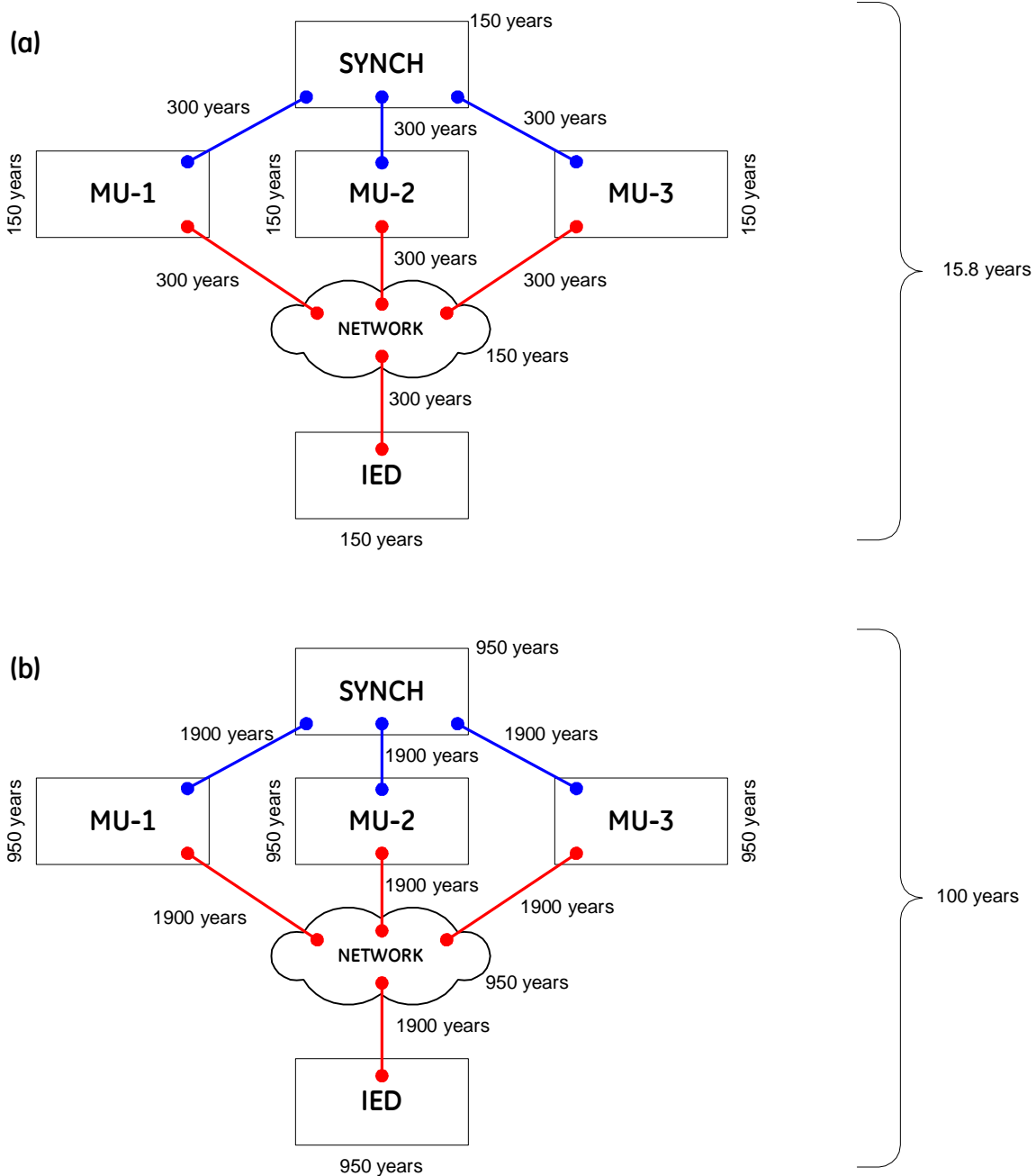


Fig. B-1. A sample process bus based protection application with arbitrary MTTF values of components (a). Required MTTF levels leading to 100 years of MTTF for the system (b).

for its merging units. This eliminates 2 components from the system (synchronization clocks and their redundant connections) and increases the MTTF to 25 years.

Assume further variants as depicted in Figure B-3.

The system of Figure B-3a eliminates the explicit network, and connects the IED with its merging units. This removes several components from the system, and increases its MTTF to 30 years.

Figure B-3b probes the impact of redundant connections. If the redundant connections are removed, the system degrades to 27.3 years of MTTF.

Figure B-3c assumes redundant merging units and

redundant connections. Each merging unit and its connection has a MTTF of 100 years. This subassembly is duplicated in the architecture of Figure B-3c yielding 150 years of MTTF for the merging unit data. The system requires all 4 elements to work (IED and 3 redundant merging units), resulting in the overall MTTF of 37.5 years.

Assume the arbitrary relative MTTF data for the components of the system in Figure B-3c. In order to achieve 100 years of the system MTTF, the IED and merging units will have to be characterized with 400 years of MTTF, and the connections with 800 years between failures.

The above numbers are within the reach of today's technology. It is important to realize that today's IEDs are

Fig. B-2.
Alternative solutions
using simplification
or added
redundancy.

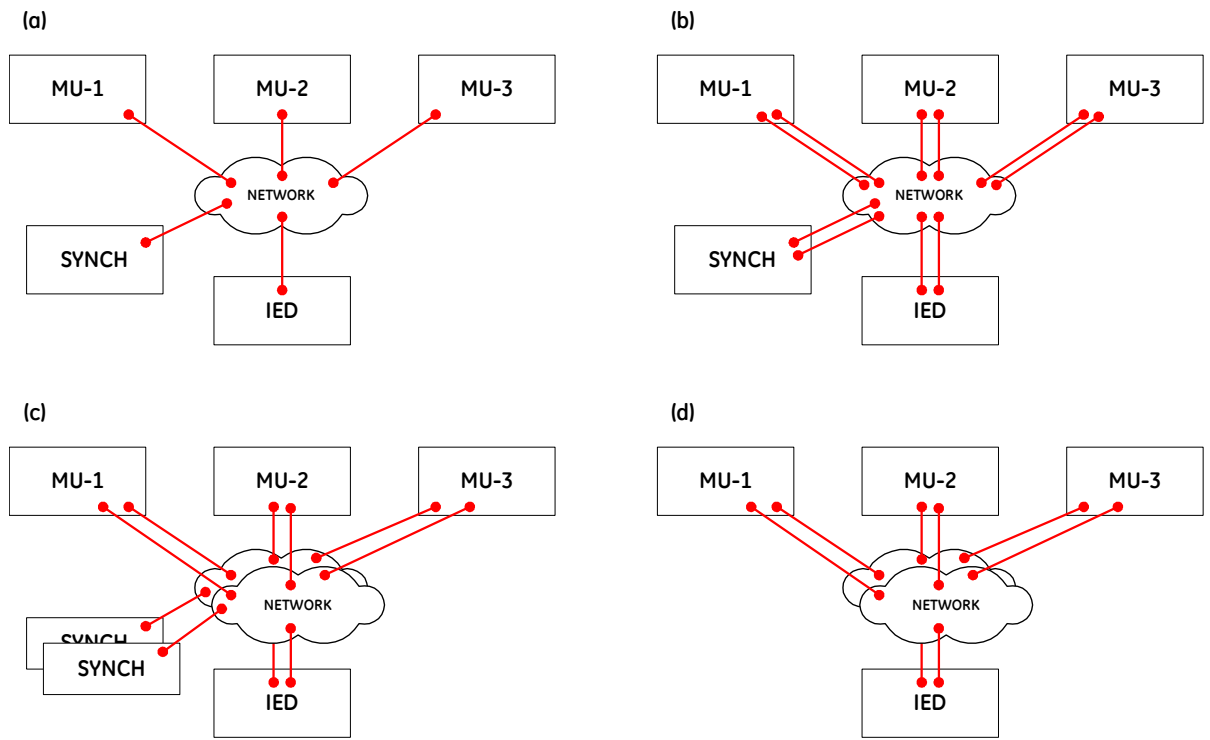
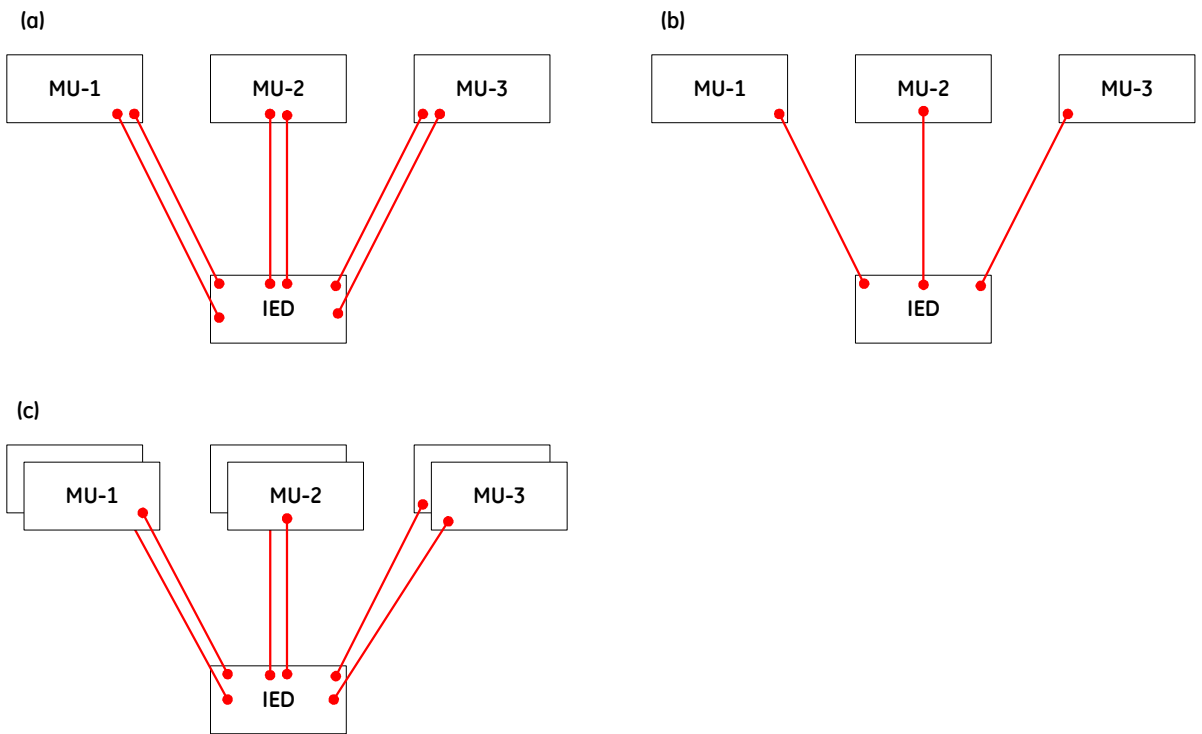


Fig. B-3.
Alternative solutions
using simplification
or added
redundancy.



built as subsystems (see Figure B-4). These subsystems are CPU with communications, power supply, binary input modules, ac input modules, contact output modules, etc. For the system (IED as known today) to have a 100 years of MTTF, the subsystems must be much more reliable. Assuming equal reliability of the 5 major subsystems of the IED in Figure B-4, each subsystem has an MTTF of about 500 years.

Assume now those existing subsystems are relocated to

compose a distributed protection system with I/Os moved to the switchyard (merging units), and input-less IED left in the control house. Assume the arbitrary reliability of 500 years for each subsystems is improved by the factor of 2. Assuming 500 years of MTTF for the direct connections, such system would reach the level of 71 years of MTTF as depicted in Figure B-5.

If the merging units and their connections are redundant, the system of Figure B-5 would reach exactly 100 years of MTTF.

This surprising number results from a simple fact: The system of Figure B-5 is very similar to today's IEDs. The complexity and part count are similar yielding approximately the same overall MTTF level. The added components (connections and power supply modules in the merging units) are compensated by redundancy of those elements, and assumed two-fold increase in reliability of the subsystems.

It is intuitively obvious that a process bus protection system set up with today's off-the-shelf components (complex merging units fed for non-conventional instrument transformers and explicitly synchronized via their IRIG-B inputs and communicating via Ethernet network) would have reliability numbers similar to the example of Figure B-1a. This is because of substantial increase in the total part count of the system as compared with today's microprocessor-based relays. A successful system for replacing copper wires with fiber optics would have to keep the total part count and complexity at the level of today's relays.

There are challenges in designing such a system primarily time synchronization, and sharing data from merging units to multiple IEDs without an explicit network, while keeping the total count of merging units at a reasonable level.

It is justified to assume relay vendors have / are working on solutions. It is quite obvious that the interoperability protocols of the IEC 61850 in the areas of process bus and peer-to-peer communication are of little help in solving this architectural/reliability puzzle.

Fig. B-4.
Today's IED as a system.

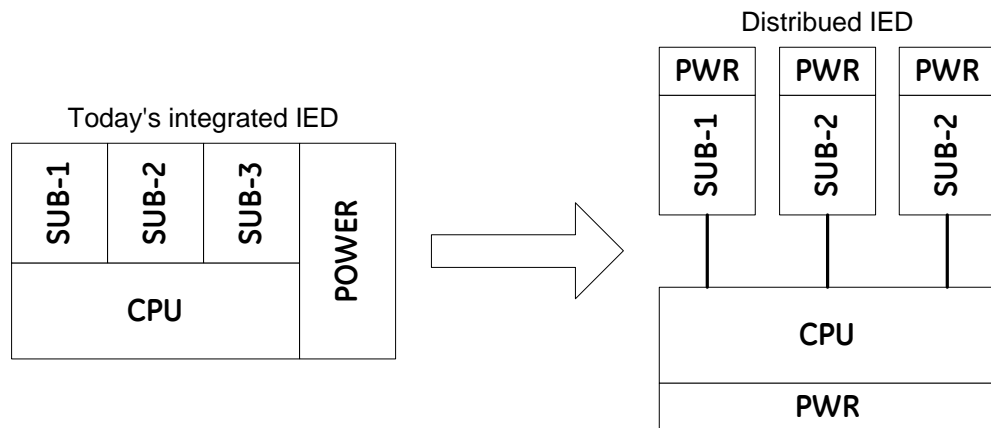
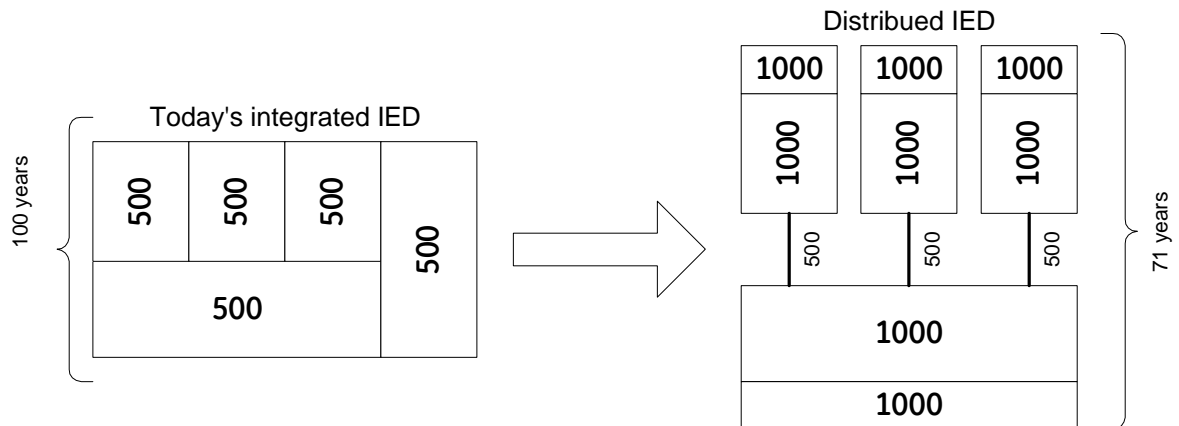


Fig. B-5.
Today's IED as a distributed system.



**Georgia
Tech**



Distance Learning and
Professional Education

POWER SYSTEM CONFERENCES

9th Annual Fault & Disturbance Analysis Conference

May 1-2, 2006 • Atlanta, Georgia • \$220

60th Annual Protective Relaying Conference

May 3-5, 2006 • Atlanta, Georgia • \$250

Discount available for attending both conferences!

Register Now! Call (404) 385-3500 or register online at:
www.emarket.gatech.edu/power

Come visit GE Multilin at the 2006 Georgia Tech Protective Relay Conference:

The following papers will be presented:

- Rebirth of the Phase Comparison Line Protection Principle
- Perfecting Performance of Distance Protective Relays and Associated Pilot Protection Schemes in Extra High Voltage (EHV) Transmission Line Applications
- IEC61850 - A Practical Application Primer for Protection Engineers
- The Application of IEC61850 to Replace Auxiliary Devices Including Lockout Relays
- Evaluation of High-Impedance Fault Detection Relays in Widespread Field Trials
- Commissioning and Testing Complex Busbar Protection Schemes - Experience at Pacific Gas & Electric
- Self-Adaptive Generator Protection Methods
- Fundamentals of Adaptive Protection of Large Capacitor Banks
- Distribution Feeder Protection and Control Scheme Utilizing Innovative Capabilities of Microprocessor Relays
- Impact of Transformer Inrush Currents on Sensitive Protection Functions - How to Configure Adjacent Relays to Avoid Nuisance Tripping

Please join us at our hospitality suite at the 2006 Georgia Tech Protective Relay Conference
May 2-4 from 5-10pm - Atlanta Ballroom B - Renaissance Atlanta Hotel Downtown -
590 West Peachtree Street