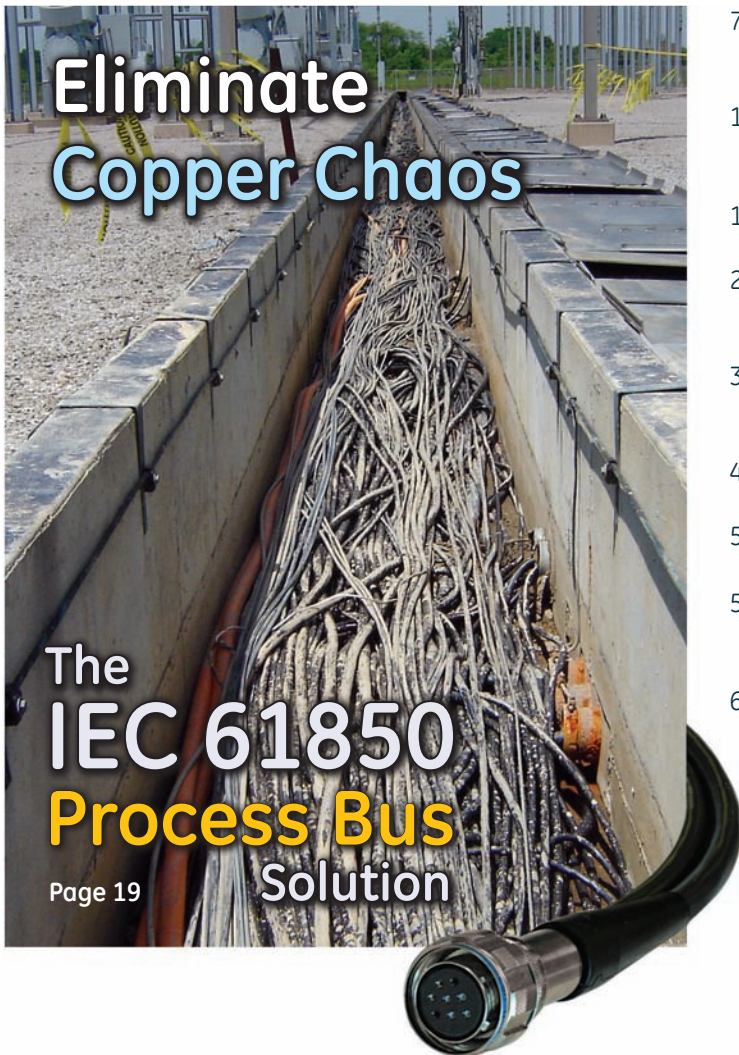


# Protection & Control Journal

October 2008



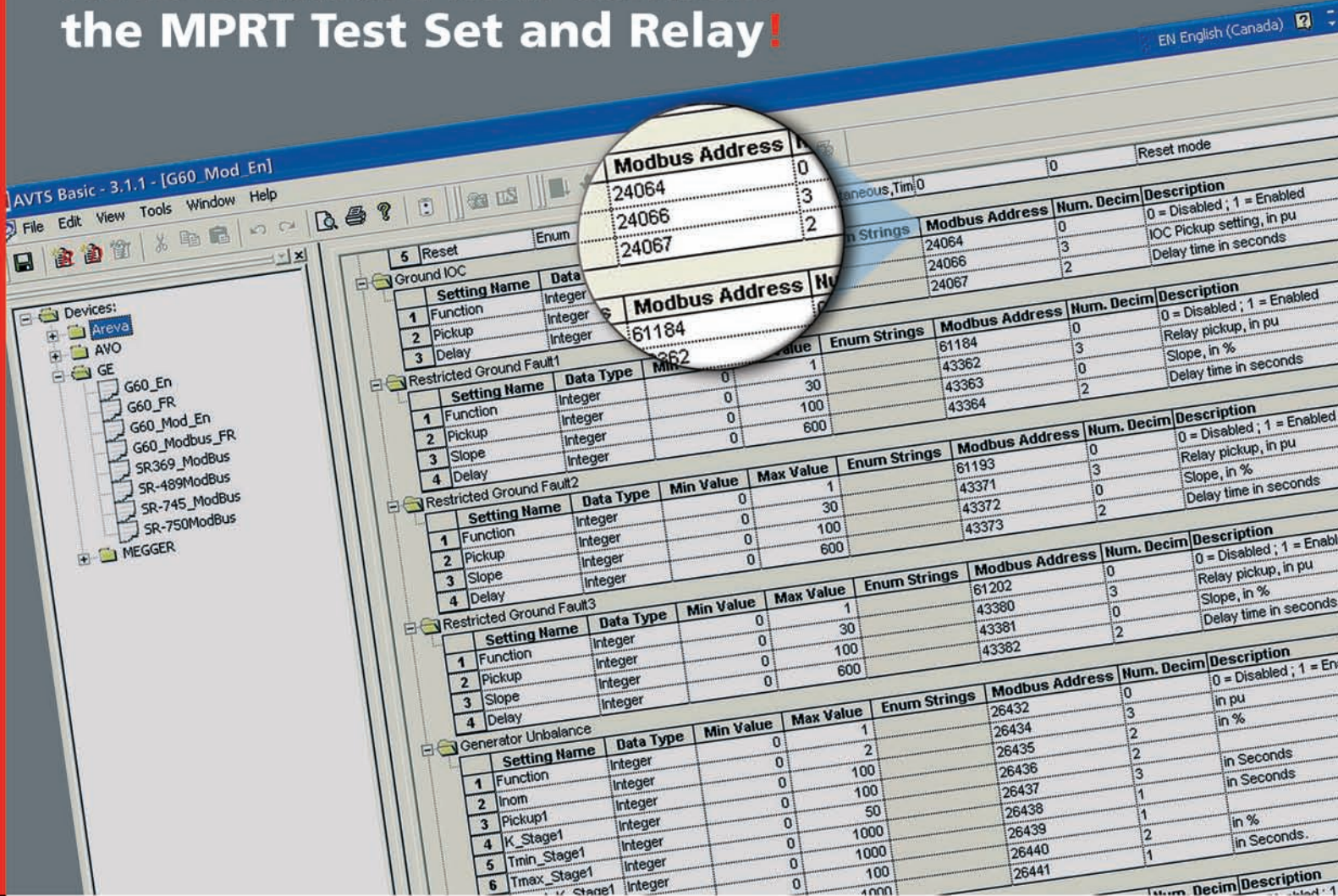
- 7 Design & Implementation of an Industrial Facility  
Islanding and Load Shed System
- 15 Business Considerations in the Design of Next  
Generation Protection and Control Systems
- 19 An Architecture and System for IEC 61850 Process Bus
- 29 The Advantages of IEC 61850 Process Bus Over Copper-  
Based Protection and Control Installations
- 35 Detection of Incipient Faults in Underground Medium  
Voltage Cables
- 45 Using 6-Sigma Methodology to Review System Security
- 51 Security Architecture for IEC 61850-9-2
- 59 Testing and Commissioning Protection & Control  
Systems Based On IEC 61850 Process Bus
- 67 Scalability of IEC 61850 Process Bus Solutions



Digital Energy  
Multilin

[www.GEMultilin.com](http://www.GEMultilin.com)  
\$19.95 USD

# AVTS Software now controls the MPRT Test Set and Relay!



## Megger AVTS Relay Test Software

Now available, Version 3.1.1

Megger AVTS Relay Test Software comes with communication capability to any Modbus equipped relay. This saves time and allows more efficient and accurate relay testing. Why? Because the relay settings can be automatically read by AVTS, as well as changed as required during testing.



In addition, there is no more need to manually input relay setting or change settings via the relay test software.

And, there are more innovative capabilities which have been added to both AVTS 3.1.1 Software and the MPRT Relay Test Set.

Learn even more about AVTS by attending one of our Relay Testing Seminars. Go to [www.megger.com/rc](http://www.megger.com/rc) for more seminar information.

# Megger

WWW.MEGGER.COM

Phone: 1-800-723-2861 U.S.  
1-800-287-9688 Canada  
Email: [sales@megger.com](mailto:sales@megger.com)  
Website: [www.megger.com](http://www.megger.com)

# Protection & Control Journal

---



## Stay Current

---

### Get your FREE subscription today

To receive future publications of the Protection & Control Journal, sign up at:  
[www.GEMultilin.com/journal](http://www.GEMultilin.com/journal)


### Advertising Opportunities

Learn more about how to reach today's protection and control professionals.  
[www.GEMultilin.com/journal](http://www.GEMultilin.com/journal)

### Submit Articles

To submit articles to be considered for inclusion in a future issue of this journal email:  
[gemultilin@ge.com](mailto:gemultilin@ge.com)

The Protection and Control Journal is a unique publication that presents power system protection and control engineers with a compilation of relevant and valuable documents. GE Digital Energy grants permission to educators and academic libraries to photocopy articles from this journal for classroom purposes. There is no charge to educators and academic libraries provided that they give credit to the Protection & Control Journal and GE Digital Energy. Others must request reprint permission from GE Digital Energy.

The Protection & Control Journal is published by GE Digital Energy, 215 Anderson Avenue, Markham, Ontario, Canada, L6E 1B3. All rights reserved. GE and  are trademarks of the General Electric Company. Copyright © 2008 GE Digital Energy. All rights reserved.

Cover photo courtesy of Ryan Barnt, American Electric Power

ISSN 1718-3189

## Contents

### IEC 61850 Process Bus



7	<b>Design and Implementation of an Industrial Facility Islanding and Load Shed System</b>
	M. Adamiak, B. Cable
15	<b>Business Considerations in the Design of Next Generation P&amp;C Systems</b>
	B. Kasztenny, J. Mazereeuw, S. Hodder, R. Hunt
19	<b>An Architecture and System for IEC 61850 Process Bus</b>
	B. Kasztenny, D. McGinn, W. Wang, R. Mao, D. Baigent, N. Nazir, S. Hodder, J. Mazereeuw
29	<b>The Advantages of IEC 61850 Process Bus Over Copper-Based P&amp;C Installations</b>
	S. Hodder, R. Hunt, D. McGinn, B. Kasztenny, M. Adamiak
35	<b>Detection of Incipient Faults in Underground Medium Voltage Cables</b>
	B. Kasztenny, I. Voloh, C. G. Jones, G. Baroudi
45	<b>Using 6-Sigma Methodology to Review System Security</b>
	B. Barnett
51	<b>Security Architecture for IEC 61850-9-2</b>
	D. Thanos, B. Kasztenny
59	<b>Testing and Commissioning P&amp;C Systems Based On IEC 61850 Process Bus</b>
	D. McGinn, S. Hodder, B. Kasztenny, R. Hunt
67	<b>Scalability of IEC 61850 Process Bus Solutions</b>
	D. Finney, B. Kasztenny



**Engineering Quicktip**

78



**Industry Innovations**

82

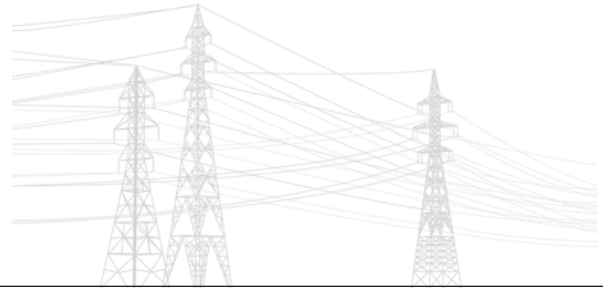


**Upcoming Events**

85



**Richard Hunt**  
Application Engineer



## The dream of process bus realized.

Picture yourself 10 years from now and imagine you've just become the Manager of System Protection at your utility. In your first weeks on the job, you realize the magnitude of the challenges you face. **70% of the transformers are over 35 years old, 60% of the circuit breakers are over 30 years old, and all are reaching the end of their life.**

Your utility has been experiencing 2%-5% load growth over the last 10 years, requiring the construction of new transmission substations every year. And with no increase in the capital budget, you can't add people to your team to spread the workload. Your most knowledgeable and experienced engineers have already retired, with more set to retire in the next few years. Open positions are left unfilled, as talented young engineers pick more lucrative industries like communications, software, or computers. And in talking to the manager of operations to commiserate, you find they are in exactly the same situation with relay and substation technicians.

This is the coming reality of the electric utility industry. Every part of the world is facing significant load growth, requiring expansion of the utility infrastructure. Developed nations also have the challenge of replacing aging infrastructure, much of which was built in the 1970s or earlier. And all of this is occurring in the midst of a worldwide shortage of engineers and technical employees.

Being a good manager (or engineer), when you look at protection and control systems, the problem to address is readily apparent. Even with the use of digital relays, these intelligent electronic devices are still connected to primary equipment in the switchyard using hundreds of copper wires and thousands of wiring terminations. Each one of these copper wires and terminations must be designed, documented

through drawings, made and installed by hand on-site, and tested in place for each substation. This workshop mode of production is reminiscent of manufacturing in the 1800s, requiring skilled labor every step of the way. When crunching the numbers, you find that labor costs are 75%-90% of the total installed cost of a protection and control system.

So the problem really is: how can I design out copper wiring in a substation? And the answer you want is a system that results in a standard substation design, with standard interface equipment, using commercial, off-the-shelf solutions. This standard interface and design must reduce engineering and documentation time, and must provide for solutions that require a relaxed skill set for installation, testing, and commissioning.

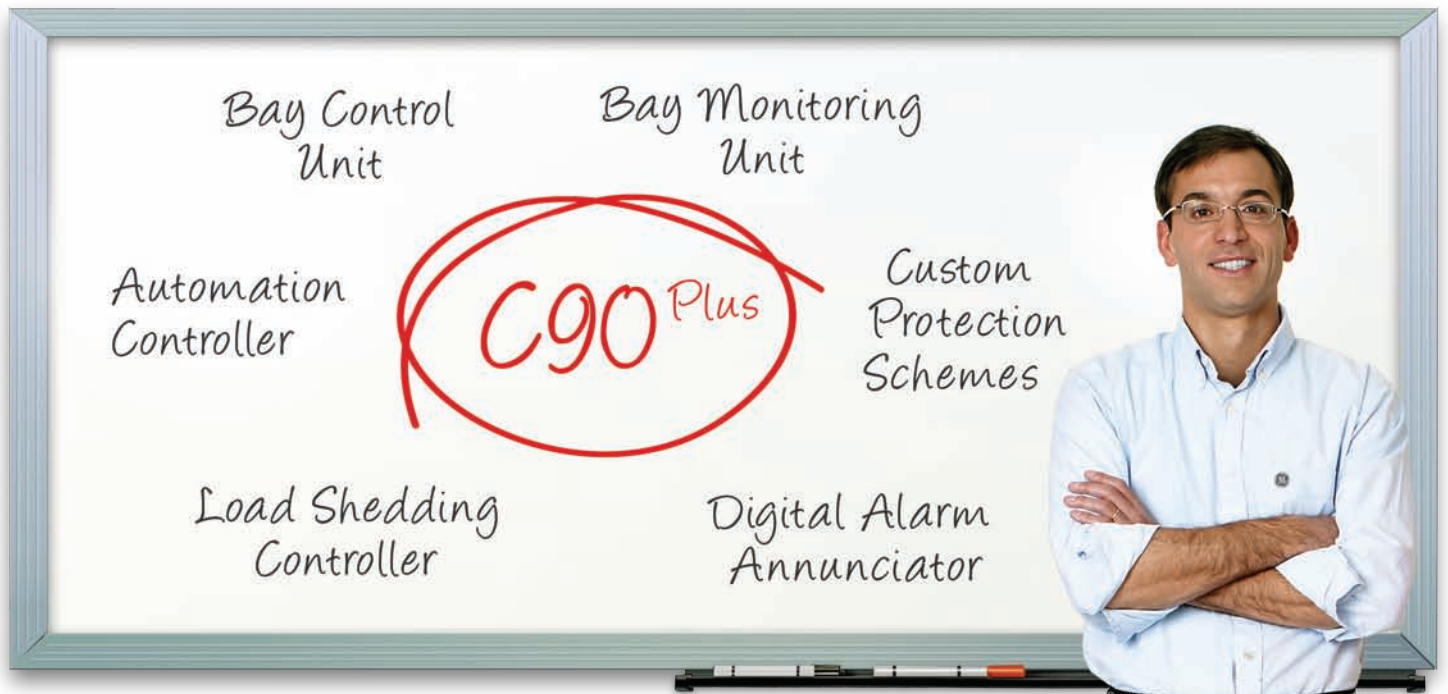
Luckily, the utility industry has recognized this need, and developed the concept of "process bus". Process bus, as suggested by the IEC 61850 global standard for communications networks and systems in substations, is a fiber optic communications network connecting protective relays in the control house, with analog signals in the switchyard. To achieve this, an interface device, or merging unit, is located in the switchyard at every current transformer or voltage transformer location. The merging unit converts these analog measurements to digital sample values sent over a fiber optic communications network. Protective relays in the control house connect to the same network to read these sampled values.

It is simple to imagine a "plug and play" system where new circuit breakers are shipped with merging units already installed, ready to connect to the process bus network. A logical extension to the merging unit is to add contact inputs and contact outputs for status and control of equipment. But so far, process bus has been just an idea, with implied solutions facing challenges concerning reliability, performance, time synchronization, testing, inter-operability, and cyber-security.

Until now. This issue of the Protection and Control Journal describes a complete, open, simple, scalable, robust, and practical process bus system for all zones of protection. Picture yourself as the Manager of System Protection who has chosen to use process bus for their next project.

Design and termination of all the copper wiring would be done by your circuit breaker manufacturers as they install merging units while building the breakers. Construction labor would pull the fiber optic cables, and makes the connections between the fiber cable and the switchyard devices, and then documents these connections via a points list after installation. Substation technicians would only be needed to test relay settings, and do final commissioning checkout after all construction is complete.

The time to design and install the protection and control system would drop by 50%. With a process bus, your capital costs are under control, your projects are on schedule, and your engineers are back to focusing on relay scheme design and protection settings. A dream come true.



# Unparalleled Control

Whether your application requires advanced substation automation, complete bay protection and control or multi-stage load shedding capabilities, the Multilin C90Plus Controller is simply the most powerful solution available for your utility substation or industrial power system applications. As a single-platform custom engineering tool set, the Multilin C90Plus Controller features true convergence of functions, including advanced automation and control, digital fault recording, comprehensive communications and extensive local HMI capabilities, delivering unparalleled flexibility for the design of your custom applications.

To Learn more visit us at: [www.gemultilin.com/C90P.htm](http://www.gemultilin.com/C90P.htm)



C90<sup>Plus</sup> Controller



Digital Energy  
Multilin

# Design & Implementation of an Industrial Facility Islanding and Load Shed System

Mark Adamiak  
GE Digital Energy

Bernard Cable  
GE Energy

## 1. Abstract

The availability of electricity supply in all areas of life has become a critical need. In the industrial arena, costs due to the loss of electrical power and resulting process interruption can usually be quantified into hard dollars. Many larger industrials, however, contain significant co-generation capability that produce both electricity and waste heat for steam production utilized in the plant processes. At any instant in time, the available generation may be able to supply the needs of the plant if islanded; at other times and conditions, a sizable portion of the plant load must be shed in order for the load to match the available generation. In all cases, the goal is to maintain as much of the plant process as possible during an external disturbance or island condition in order to minimize environmental impact, production loss, and potential equipment damage.

This paper presents the design and implementation details of a control system that detects an island condition in an industrial facility, creates the island if needed, and executes a multi-tier load shed based on the load-generation balance that existed prior to the creation of the island. System operation in island mode and performance metrics obtained from dynamic tests are presented.

## 2. Business Case

As with all major industrial installations, reliability was a major consideration in the plant's design. With few exceptions, most components of the electrical system were designed to withstand one failure (N-1 contingency). Dual transmission lines from the Utility Grid were backed up by two 37.5 MW generators to provide power to the plant. This design allowed for the loss of any one source without impact to normal operation. All sources feed a 34.5 kV distribution bus in the main incoming substation. The distribution bus then feeds several of the plant's double-ended substations. Even at the utilization level most motors have installed spares. With this design, it was believed that the plants power system was secure and was capable of providing continuity of service under most failure scenarios.

Commercial operation began in December 2001. In May 2002 the security of the power system design was tested during its first major event. An insulator flashover in the plant's 230 kV substation ring resulted in a complete separation from the local utility. The site's cogeneration units were able to successfully operate in "Island Mode" for a period of approximately 12 hours. Eventually, the substation issues were corrected, and the Site



power system was re-synchronized to the utility grid without event or loss of power to the site.

One week later, the system experienced its second event due to an electrical equipment failure - again initiating "Island Mode" operation as before without any impact to the plant. However, with the cogeneration units operating at reduced load, this resulted in a reduction in steam generation and steam became a critical issue for the site. In order to generate more steam to meet the sites demand, one of the two cogeneration units was ramped up in load in order to achieve the minimum megawatt permissible for auxiliary firing of a Heat Recovery Steam Generator (HRSG). However, before this could be accomplished, the HRSG tripped on excessive superheated steam outlet temperature, which cross-tripped the gas turbine resulting in loss of the generator. With only one cogeneration system remaining on line and with no way to balance the site demand to internal generation, the demand exceeded the generation capacity resulting in a trip of the second unit. This dynamic event lead to a site wide power outage lasting approximately 30 minutes, resulting in a loss of production, equipment damage, and an environmental impact.

It was recognized, after the second event, that if the power system could be dynamically monitored such that the internal generation and load could be balanced and, if required, pre-determined loads shed, then a stabilized island could be created and the plant electrical system could remain intact. Though the cost of installing an islanding and load shed system can be considerable, it was determined that the initial monetary capital cost of such a system would be eclipsed if a total loss of site power could be avoided.

### 3. Design Criteria

As mentioned earlier, the primary goal of the scheme is to detect an island condition and, if necessary, shed the amount of load required to create a load-generation balanced island. Step one is the detection of an island condition. From the diagram in Figure 1, it can be seen that the “primary” island detection is accomplished by determining the Open/Close status of breakers MA and MB – the 34.5kV feeds into the plant. If both MA and MB breakers are open, then the plant is islanded from the main grid. A “secondary” island condition can be created if all four breakers in the plant’s 230kV ring bus are opened.

In addition to a “detected” island, the scheme was designed to “force” an island. Specifically, if an underfrequency or undervoltage condition is detected, the scheme trips both 34.5 Main breakers - MA and MB - to forcibly separate from the main grid due to an apparent unstable condition on the utility system.

### 4. Load Shed Decision Criteria

The decision as to whether to shed load and how much load to shed is based on the measurement of the dynamic load-generation balance. The internal plant load is calculated by summing the power flows on the 4 primary feeds into the plant, specifically:

$$Total\_Internal\_Load = P_{GA} + P_{MA} + P_{MB} + P_{GB}$$

Note that if there is excess generation from the internal generators, the power flow through breakers MA and MB becomes negative and the Total Internal Load is still calculated correctly.

The Total Internal Generation is then calculated as:

$$Total\_Internal\_Generation = P_{G1} + P_{G2}$$

The final calculation is the Load-Generation balance, which is:

$$Load\_Generation\_Balance = Total\_Internal\_Load - Total\_Internal\_Generation$$

A positive value for the Load-Generation balance indicates that the load is greater than the available generation and that, upon detection of an island condition, a load shed may be required in order to maintain plants electrical system stability.

The loads to be shed were identified by plant personnel and broken down into 3 load groups or “tiers”. For the specific design, the Load-Generation difference levels at which each tier was invoked were set at:

$$1.5 MW < (Load - Generation) \leq 19.8 MW; \text{ Shed TIER 1 Load}$$

$$19.8 MW < (Load - Generation) \leq 27.3 MW; \text{ Shed TIER 1 and TIER 2 Load}$$

$$27.3 MW < (Load - Generation); \text{ Shed TIER 1 and TIER 2 and TIER 3 Load}$$

Note that the gas turbines were capable of picking up at least a 1.5MW Load-Generation difference and were quite fast at slowing down under the over-generation scenario.

Once islanded, there was still a chance that events in the plant could start to take down the local island. To address the “sinking island” scenario, and given that there was additional load to shed, two of the relays were programmed to address additional stability criteria, specifically:

If:

$$Frequency < 58.8 \text{ Hz for } 1.0 \text{ Second or Voltage} < .85 \text{ pu for } 1.5 \text{ seconds}$$

Note that it was necessary to coordinate the Underfrequency element on the generator protection relays with the islanded underfrequency load shed values.

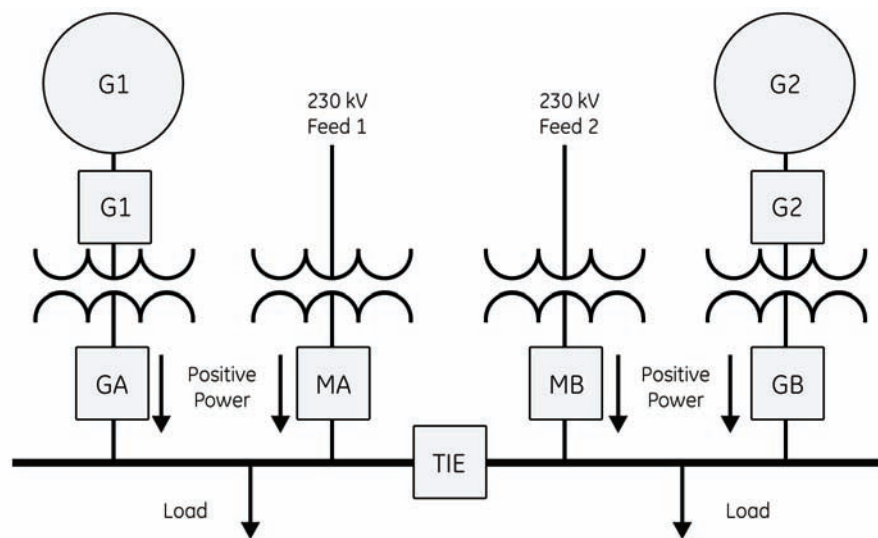


Figure 1.  
34.5 kV bus sources



## Shed Conditions

- MA & MB Open
- 230 kV Bkrs Open
- Under Frequency
- Under Voltage

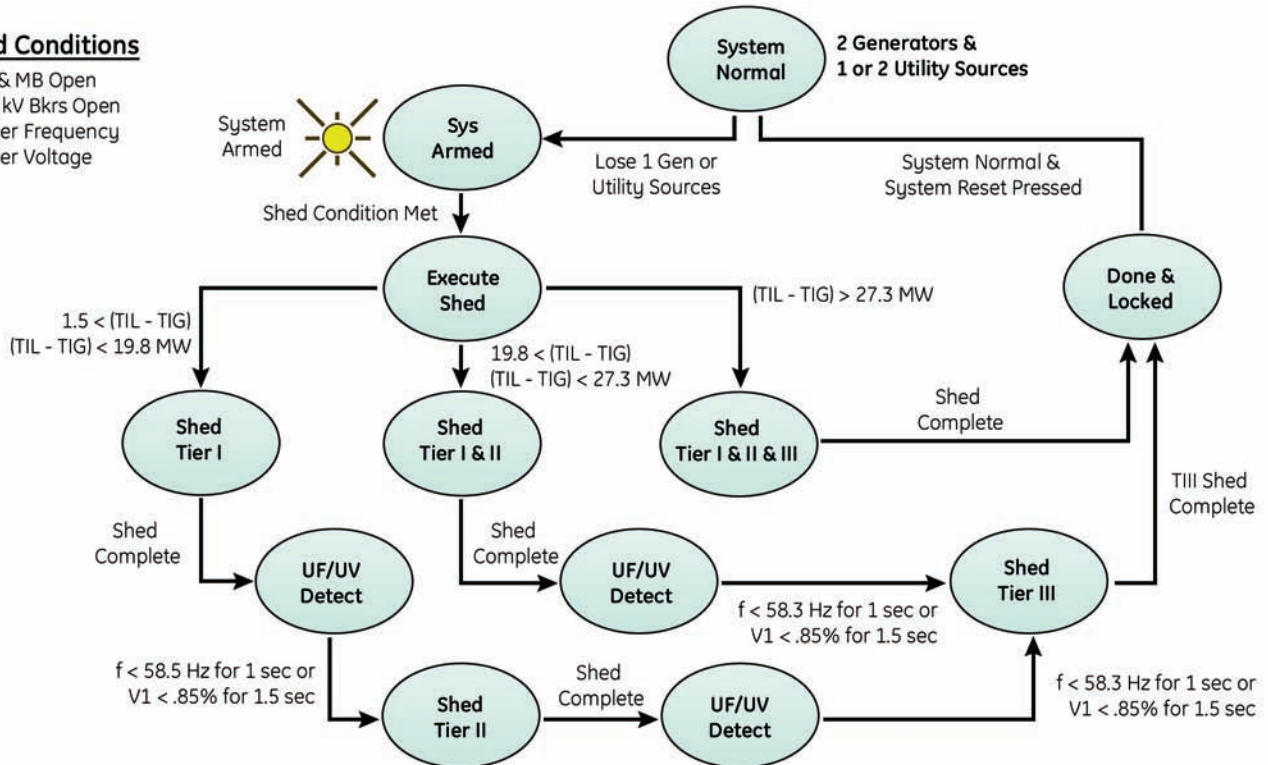


Figure 2.  
Load Shed Scheme State Transition Diagram

Depending on how many tiers of load were available to shed, different shed criteria were defined. To visualize the different states of the load shed system, a State Transition diagram was developed (Figure 2) and used in the system design and as a system operating map and training tool.

As the distances between the controller and the sheddable loads were substantial (1000m), it was not practical to have direct copper paths to perform the load shed trips. The decision was made to perform the trips via remotely located controllers. The signals to trip would be sent via a communication channel that would connect the various venues. As communications was crucial to the proper execution of the shed command, the decision was made to provide redundant communication channels. In addition, all communications were to be carried via fiber optic cable.

## 5. Implementation

The first part of the implementation was the calculation of the Load-Generation balance. To implement this calculation, programmable relays were located in the breaker cubicles of MA, MB, GA, and GB. These relays were connected to measure “positive” power flow as being into the plant. In addition, breaker status was monitored via digital inputs into these relays. As both “a” and “b” contacts were available from the breakers, double-point breaker status was implemented. In order for a breaker to be declared “open”, the “a” contact had to be opened and the “b” contact had to be closed. If both the “a” and “b” contacts reported the same value, a “Breaker a/b Mismatch” alarm was issued. For reliability, a given breaker status was measured by two different relays. For example, the status of breaker MA was sensed by both

the MA relay and also by the MB relay. The logic was designed such that a breaker was determined as “open” only if a valid open state was declared by either relay. Sharing of this information was accomplished through the use of both GOOSE (defined below) and a vendor specific Direct I/O communication scheme.

## 6. Load-Generation Balance

In order to perform the Load-Generation balance calculations noted above, all the analog data had to be communicated to a central location in the plant and then summed or differenced appropriately. The relays chosen for this application had a summator function available in the device. In this scheme, the MA relay was chosen as the calculation engine so all the analog values had to be communicated to the MA relay. The mechanism that was used to transport the analog values was the IEC 61850 Generic Object Oriented Substation Event or GOOSE. The GOOSE is a “user-defined” dataset that can be a combination of analog, digital, and quality data values. The GOOSE is launched on change of state of a status value, on a percent change in an analog value (user settable), or periodically as an integrity test. In this particular application, the analog value changes were tested once a second and re-transmitted as appropriate.

Once received and summed into the Load – Generation quantity, the resultant value was evaluated in comparators per the ranges noted in the Design section above. The output of the comparators was then mapped into “Tier” data values. Specifically, the Tier 1 Armed flag was set first, followed by the Tier 2 Armed flag, and finally followed by the Tier 3 Armed flag.

## 7. Load Shed Activation

By having the Tiers pre-armed, when an island condition is detected, the appropriate Tiers can be shed with no appreciable time delay. In the implemented scheme, the time delays come from 4 primary sources: Breaker Status indication, Logic Processing, Output Contact operation, and breaker operation. On the breaker status indication, all breaker status inputs are denounced for 8ms before becoming "valid" to use in the logic. Once validated, the breaker status values are fed into a logic engine that operated every 2ms. Any decisions to shed load were then communicated via GOOSE to the appropriate remotely located controllers. Note that the communication time is not noted as a primary source of delay as the time on the wire of the communication message is less than 300msec. In the receiving relay, there is a 0 to 2ms delay for logic processing, there is a 3ms time delay in the operation of the output contact and finally, there is a 37ms breaker operate time. In as much as these times are "worst case" timings, an average time of 13ms was measured from initiation of the island condition to energization of the trip coils on the load shed breakers or lockouts. Note that lockouts were needed on some loads to prevent automatic or operator re-starts.

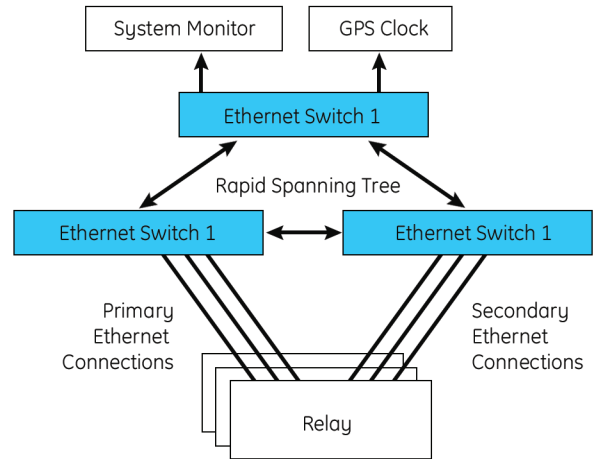
## 8. Time Synchronization

The plant load shedding scheme also included a GPS Satellite clock, used to time-synchronize each of the installed relays and controllers via different mechanisms and to varying degrees of accuracy. The relays used have synchrophasor recording capability, which is used as a long-time trend recorder in the operation of the plant electrical system. Recording is initiated via a number of different triggers. Time-synchronization of each of these synchrophasor relays required 1msec absolute time accuracy. This level of accuracy was achieved through the use of the IRIG-B time synchronization protocol via direct wiring from the GPS clock to each relay. As the load controllers were located a significant distance from the GPS clock and as they did not need the same level of accuracy, time synchronization was achieved over the communication channel using the Simple Network Time Protocol – SNTP. Time synchronization via SNTP is typically able to achieve 1ms time accuracy. Given that all the devices are time synchronized, an integrated Sequence of Events report can be created that interleaves all the events from all the devices into one common report.

## 9. Device-to-Device Communications

Primary communications to all devices was achieved via Ethernet. As the operation of the system is based on reliable/available communications, a redundant Ethernet network was implemented. All the relays had redundant Ethernet ports on them and each port was connected through redundant Ethernet switches (see Figure 3). The switches themselves were connected in a Ring configuration. In as much as Ethernet abhors a ring, an Ethernet protocol, known as Rapid Spanning Tree, was configured which automatically detects any ring conditions, dynamically breaks the ring, and automatically heals the ring upon detection of failure of another part of the ring.

In addition to the redundant Ethernet communications, a secondary communication path was established using a 64kbps synchronous communication channel connected in a ring amongst all the relays in the system. The secondary communication channel provides additional back-up communication of status and control information. As it operates in a ring configuration, there is a 3ms delay at each node as a received packet is received and then forwarded. This secondary channel was also used to communicate additional information that wouldn't fit in the available GOOSE packets.



**Figure 3.**  
*Redundant Ethernet Communications*

## 10. User Interface

Monitoring and control of the system was achieved through LEDs and Pushbuttons located on the front of the relays. Specifically, one relay was chosen as a central controller that could arm/disarm all the devices in the system, RESET all targets and alarms, and control what breakers tripped in a given load shed scenario.

Status, operational information, and alarms of the system were visually reported through an assignment of the various pieces of information to user-programmable LEDs. Specifically, breaker status, arming levels, relay targets, device alarms, and other equipment alarms (e.g. – Ethernet switch status) were all mapped to individual LEDs on the front of the various relays.



**Figure 4.**  
*Advanced User Interface of Multilin C90<sup>plus</sup> Controller IED*

## 11. Operational Information

In addition to the User Interface information, each of the relays provides additional operational information in the form of Sequence of Events (SOE), High-speed Oscillography, Synchrophasors, and Demand data. All digital inputs, internal logic status, and internal alarm information is captured in the SOE log. The contact inputs are sampled with a  $\Delta t$  of 500msec and the internal logic and alarms are sampled with a  $\Delta t$  of 2ms. Each relay can hold up to 1024 events, however, an external system automatically retrieves the SOE logs from each device, integrates them into a common database, and provides standard database queries to sort and process the SOE information.

For events such as faults, high-speed oscillography is provided with a sample rate of 3840 samples per second. Long-term oscillography is provided by the synchrophasor function. Triggered by functions such as over or under frequency, over or under voltage, and rate of change of frequency, a single synchrophasor record can span over 20 minutes in length. Finally, 15 minute phase current, MW and MVar demand information is logged and can be retrieved for load analysis.

## 12. Testing

Testing of the system took place on two fronts, namely: a Factory Acceptance Test (FAT) and a Site Acceptance Test (SAT). For the FAT, the system was racked (all 8 relays), wired, and connected for communication (fiber cables to redundant Ethernet switches and Direct I/O) in the factory almost exactly as it would be installed in the field. The test included injection of voltages and currents into the measuring relays, simulation of all the contact inputs (representing the various breaker and lock-out states), and monitoring of the output contact performance. The GPS clock was connected and time synchronization was verified in all devices.

The voltage/current injection was wired such that the different tier arming scenarios could be simulated by opening, closing, and reversing the injected currents. As the design of the system was based on a state diagram, there was a clear test matrix that was derived based on tracing through all possible state transitions. Timing of the scheme was accomplished by examining the sequence of events logs from the relays involved in a particular Tier operation.



**Figure 5.**  
*Retrieving and analyzing event record data*

### 12.1. Site acceptance test

The SAT for the project consisted of two pieces: a commissioning test and a live islanding test.

The commissioning tests included:

- Verification of all contact inputs – as driven by the respective breaker or lockout relay. Note that this was greatly facilitated through the use of the relay front panel LEDs to which all breaker and lock-out status indications were mapped
- Verification of operation of each connected breaker or lock-out relay
- Verification of the various communication networks – including redundancy testing
- Verification of the time synchronization functionality
- Verification of power flow measurements and directions
- Verification of the various system alarms

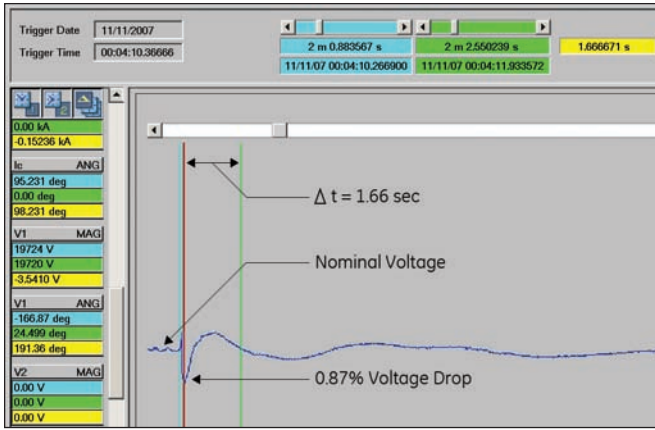
Several minor issues were found during commissioning, however, the diagnostics designed into the system quickly identified the source of the issues and allowed for rapid remediation.

Of note in commissioning was the desire by the customer to change two of the breakers that were to be tripped during a load shed operation. Due to the system design of tripping via GOOSE messaging, the changes involved writing some new logic and wiring the new breakers into one of the existing controllers – a relatively minor implementation task.

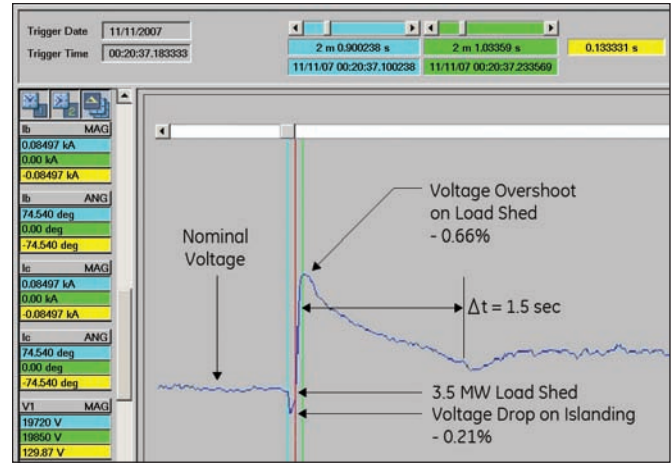
### 12.2 Live islanding tests

Once the system had been commissioned, the load shed system was tested in two actual island situations – scenario 1 where a load shed was not required and scenario 2 where a load shed was required. As the plant was not operating at full load and as the available sheddable load was only 3.5MW, the load shed levels in the controller were temporality modified for a smaller shed range. The island was created by manually tripping the primary and secondary external feeds into the plant. As a precaution in both scenarios, the trip signals were removed from all but the available sheddable load (a backup 3.5MW pump motor).

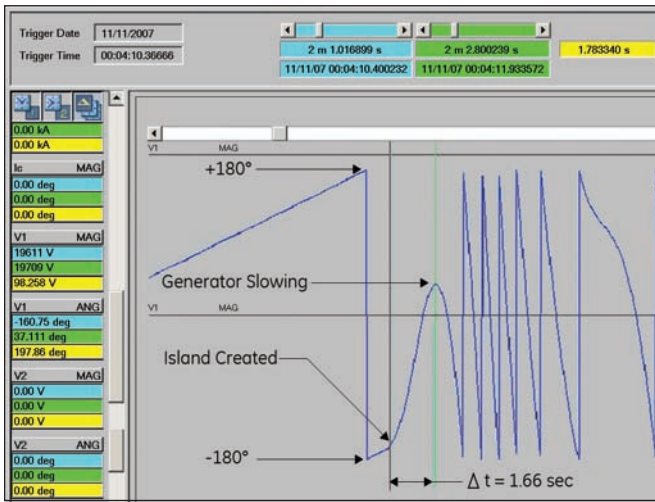
In scenario 1, the gas turbines were set to deliver the entire internal plant load plus an additional 9.4 MW, which was effectively exported to the local utility. Prior to the island, it was noted (as expected) that none of the load shed Tiers were “armed”. Upon creation of the island, as expected, there was an immediate but small voltage increase (0.27%), however, within 16ms, the voltage regulator initiated a 0.87% drop in voltage (see Figure 8). The turbines did start to accelerate until 1.78 seconds after islanding, the turbine controls had started the slow-down process of the turbine. The resulting positive sequence Synchrophasor voltage angle for the island is shown in Figure 7.



**Figure 6.**  
*V1 Magnitude Synchrophasor Response to Over-powered Island Creation*



**Figure 8.**  
*V1 Synchrophasor Magnitude Response to Underpower Island Creation*



**Figure 7.**  
*V1 Synchrophasor Angle Response to Over-powered Island Creation*

In scenario 2, the turbines were programmed to output 4.55 MW less than the internal plant load. This scenario was designed to execute the “shed” commands. As mentioned earlier, the arming levels were temporarily lowered to force the arming of the respective load shed tiers. Prior to islanding, it was noted that all 3 Tiers were “armed” and ready to operate upon detection of the island condition. The recovery from the 4.55 MW deficit was to be made up of two sources, namely, a 3.5 MW motor shed and dynamic power up-take by the gas turbines.

Again, opening the main breakers created the island. The island was detected in 8ms (the debounce time on the breaker contacts) and a 3-Tier Load Shed command was immediately issued. The 3.5 MW motor was off-line (including breaker operation time) in 50ms from the detection of the island. Figure 8 shows the response of the positive sequence voltage – V1. Upon creation of the island, the voltage immediately drops only 0.21% and then starts to recover. When the motor load is shed, the voltage overshoots 0.66% - a very nominal amount.

### 13. Conclusions

Today’s manufacturing facilities require a higher degree of availability of electrical energy than in the past. Although load shed as a reliability mechanism is not a new concept, the design of a distributed system based on IEC 61850 GOOSE and an Ethernet communication network provides many advantages in terms of performance and flexibility as demonstrated through the inclusion of actual test results.

## From Concept to Commissioning

*Virelec has delivered systems for many utilities and industrials across Canada and in the USA. Let our team of knowledgeable professionals help you with your P&C or SCADA project.*



### Protection, Control and SCADA Systems

Virelec is an experienced supplier to the industry, offering engineering design, procurement, panel manufacture, system integration, testing and site commissioning.

### System Engineering

In addition to detailed protection design, Virelec offers power system load flow, short circuit and relay co-ordination studies.

### Drop-in Control Houses

Virelec offers this new method of delivering P&C systems. The complete building envelope containing panels, AC/DC distribution, batteries and auxiliaries is cabled, tested and pre-commissioned at Virelec's factory ready for field equipment cabling.

### IED Engineering and Support

Virelec's experienced team has expertise in integrating IEDs into substation automation systems, including the IEC 61850 standard. Virelec also provides relay settings and programming, as well as site commissioning.



Call us at 905-569-8030  
E-mail: [info@virelec.com](mailto:info@virelec.com)  
Website: [www.virelec.com](http://www.virelec.com)  
Virelec Ltd., Mississauga, Ontario

# Labor Bound By Copper?

## Let HardFiber™ IEC 61850 Process Bus Remove the Shackles

Utilities have their hands tied with expensive and time consuming copper-reliant switchyard communications requiring tedious individual cable splicing, terminating, and testing.

The Multilin HardFiber System was specifically designed to break the bonds of copper cabling by reducing capital costs, and freeing highly skilled utility workers from performing labor-intensive activities.

The HardFiber System is a complete IEC 61850 system available for a wide variety of protection applications, including generator, transformer, transmission line, bus, feeder, capacitor bank, and motor protection.

By eliminating the need to install and maintain thousands of copper wires, utilities can save up to 50% of protection and control installation and maintenance costs, while at the same time increasing worker safety and power system reliability.



**HardFiber™ Brick**  
Hardened Switchyard Interface



Digital Energy  
Multilin

# Business Considerations in the Design of Next Generation Protection and Control Systems

Bogdan Kasztenny, Jeff Mazereeuw, Steven Hodder, Rich Hunt  
GE Digital Energy

---

## 1. Introduction

The technology of protection and control systems (or station automation and protection systems) has been continuously evolving and integrating increasing numbers of functions over the last several decades, delivering significant improvements in dependability, security, sensitivity, accuracy and greater reduction in equipment footprint. The strategic-thinking manager has taken advantage of these improvements to produce many tangible business benefits such as project cost reduction, faster facility restoration through access to operational information and lower maintenance costs.

In the past, Protection and Control (P&C) systems consisted of numerous electromechanical relays. A line protection system would typically contain ten or so primary relays, many priced the same as an automobile. Later, solid-state relay technology emerged whereby two measuring units (phase and ground), each in the same price range, replaced the ten primary relays. Now, a single microprocessor based relay costing a fraction of the price of a solid-state measuring unit, performs all the measuring functions, incorporates auxiliary relay functions, and provides fault and event recording. In addition, microprocessor based relays support serial communication technologies originally developed for business applications and industrial automation. Pioneer efforts used vendor specific protocols each with functionality limited to one application. For example, dial-in modem access of fault records reduced the labor required and response time for fault analysis and direct relay-to-relay serial I/O decreased the cost of short-haul protection signaling. The last 10 years has seen a rapid pace of adoption of Ethernet for SCADA access to relays and relay to relay signaling.

This evolution in technology has helped control capital costs for the materials required for protection and control expansion projects. However, the electric utility industry is facing some significant challenges in the next few years. Incremental improvements in the capabilities of digital devices and cost reduction in these devices will not be enough to supply the desired cost savings, as material costs are less than 25% of the total installed cost of protection and control systems. It will be necessary to significantly reduce the installed cost of new facilities as they are built, and the subsequent cost to operate and maintain these facilities.

## 2. Industry Challenges

The primary challenge relates to the age and capacity of the transmission system. The existing system is essentially operating at full capacity, with significant growth expected in most regions of the world. In addition, much of the equipment that makes up the existing system is aging. In North America, for example, 70% of the transmission lines and power transformers are more than 25 years old, and 60% of the circuit breakers are more than 30 years old [1]. Obviously, the electric utility industry must invest in a major construction effort to maintain the performance of the existing transmission system and provide new facilities to serve growing energy demand.

A second challenge is the technical workforce needed to refurbish existing facilities and construct new facilities. The expectation is that the size of the technical workforce will stay essentially the same, even with the foreseen increase in construction projects. Therefore, the technical workforce will need to achieve significant productivity gains. These challenges require a new technical solution that addresses the entire protection and control system, not only the protection and control devices. A successful technical solution must realize a significant cost savings based on actual business considerations.

## 3. Primary Enterprise Objectives

### 3.1 Cost reduction

In the modern electricity marketplace, in particular those areas with investor-owned electric generation, transmission and distribution companies, there is an ever-increasing demand to reduce costs in all aspects of the production and transmission of electric power. These cost savings historically have been realized in protection and control systems by integrating multiple separate functions into a single, multi-function Intelligent Electronic Device (IED). This integration realized a considerable degree of cost savings by reducing the number of individual devices needed to implement required protection, control and monitoring functions. The amount of cost savings that can be achieved through integration asymptotically approaches a finite limit, as the IED hardware itself becomes responsible for a vanishingly small fraction of the total installed cost of the system.

Clearly, this trend for cost reductions must be realized through other means beyond simple material cost savings or further integration and focus more on a holistic, system-level strategy. For any new approach to be viable from a business standpoint, it must be able to realize significant cost savings beyond material costs, and address application engineering, drafting and commissioning labor costs and the costs of copper wiring and its associated labor and infrastructure.

### 3.2 Reduced Project Duration

There is a pressing business requirement to reduce the time needed for the design, documentation, installation, and commissioning of protection and automation systems. The drivers are limited availability of skilled workforce and the recent, extensive escalation in investment into the electricity infrastructure both in developed and developing nations. This trend is expected to continue far into the future due to the necessity to quickly catch-up with demand. This investment will replace aging infrastructure and strengthen and expand the power system.

### 3.3 Changing workforce

Many electrical utilities have to address the issue of a rapidly aging workforce and the strategic replacement of staff while retaining key domain knowledge and skills [2]. In general, very little effort and consideration has been given to succession planning for technical staff and skilled trades-people, thereby raising concerns over the availability of staff to perform basic utility work. There are two key considerations:

- Focus on the transfer of key skills and knowledge from the current workforce to incoming staff. This transfer must take place while also performing usual business activities.
- The need for a relaxed, not expanded, workforce skill set required to design, install and configure the system. This necessitates a technical solution for protection, control and automation that is easy to grasp and deploy, is transportable across geographic and generational borders and offers an opportunity to relax the skill set requirements for certain workforce segments including engineering, drafting, construction and maintenance.

A sound protection and control system of the future should have an intuitive architecture, thereby minimizing the training requirements and shortening the learning curve necessary to reach a suitable level of productivity with the design, construction and commissioning of process bus systems.

A successful solution will have to trade the on-site labor with pre-fabricated material, particularly for some disappearing, non-sustainable professions. Material manufactured in a controlled environment using automated processes and single purpose tooling is not only of lower cost and higher quality, but also readily available, as compared with on-site assembly using the shrinking journeyman workforce.

### 3.4 External procurement of subsystems

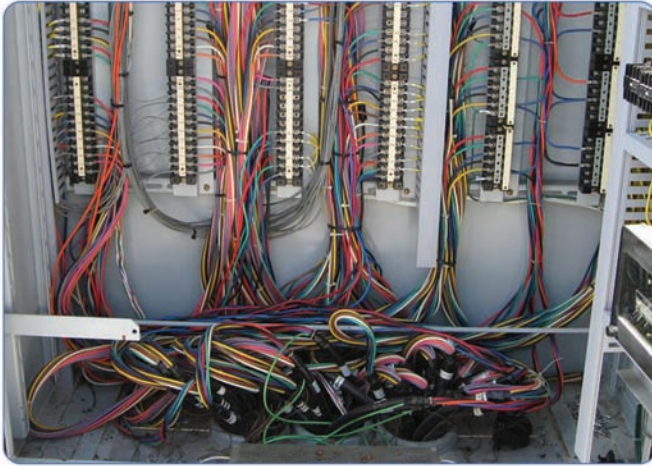
Along with the changing workforce, there is an increasing trend for utilities to externally procure major subcomponents of a substation, delivered to site as a pre-configured and tested entity. This transfers the maximum amount of design and construction to a controlled environment rather than on-site, and as much testing as possible is shifted from Site Acceptance Testing (SAT) to Factory Acceptance Testing (FAT). A viable protection and control system should support these trends, and by doing so potentially result in higher quality of work delivered and improved long-term reliability.

### 3.5 Discussion of costs for protection and automation systems

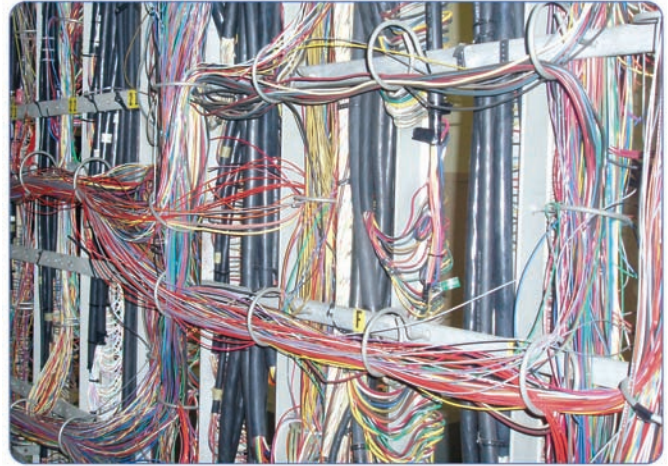
The Total Lifecycle Costs associated with protection and automation systems can be broken down into two general categories: Total Installed Cost, and Operation and Maintenance Cost. Total Installed Cost (TIC) relates to the initial design, installation and commissioning of protection and automation systems (commonly referred to as Capital work). Ongoing activities with the continued operation, maintenance and sustainment of these systems are commonly referred to as Operating and Maintenance, or O&M, work. Total Lifecycle Cost (TLC) is the sum of TIC, O&M and any retirement costs associated with the system. An action to reduce the material component of TIC may actually increase the engineering design, commissioning components of TIC and TLC through added complexity. Alternatively, a decision that reduces the engineering and installation components of TIC may result in higher cost for material, but may offer reduced TIC and TLC.

Copper wiring is used to transmit information or control actions within substations. It uses primitive, low signal density signals and hence, the volume of copper wiring is large and labor intensive to design, document, install and commission. Copper wire starts with terminations located at primary equipment in the switchyard. Each piece of equipment has terminations for multiple wires (Figure 1) for signaling and control. Numerous copper cables are pulled across the switchyard in conduits or trenches (Figure 2). Thousands of individual copper wires are terminated in racks located in the control house (Figure 3). Copper wires are then distributed through the control house from the termination rack, ending in numerous terminations at relay panels (Figure 4). The flexibility of discrete wiring enables the interconnection of different primary equipment types, vendors and provide for variations in physical switchyard topology. This is achieved through labor-intensive activities that limit the use of mass production methods and off-site manufacturing. Each copper wire and termination must be designed for the specific project and documented through a custom wiring diagram. Terminations are made on-site by skilled labor, one termination at a time. Each wire and termination must then be individually tested during commissioning. Wiring diagrams must be updated and corrected to match the final field installation.





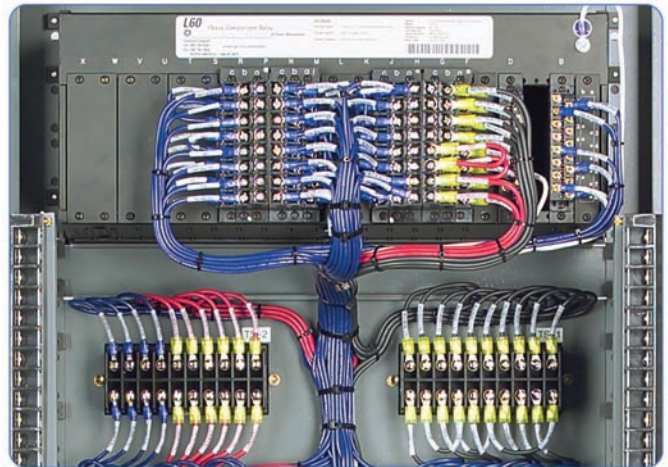
**Figure 1.**  
*Primary apparatus terminations*



**Figure 3.**  
*Termination racks for copper wiring and cables*



**Figure 2.**  
*Traditional cable trenches*



**Figure 4.**  
*Labor-intensive copper wiring on relay panels*

Copper wiring has many technical disadvantages as it requires engineered designs to provide overvoltage withstand capability, interference immunity and safety for the workforce. Additionally, copper wiring is susceptible to environmental effects (e.g. oxidation/verdigris) and latent/hidden failures (e.g. a broken connection).

It can be shown that the volume and variability of copper wiring has a dominating cost impact on all aspects of protection and automation TIC and TLC. Designing out copper connectivity is therefore a clear way to reduce the cost in many interrelated areas.

## 4. Basis for a New Protection and Control Solution

With present technology, fiber optics is the clear choice to replace copper wire. Fiber optics can transmit immense volumes of information or control actions within substations without the disadvantages of copper wiring. It has equivalent flexibility where information or control actions can be processed or distributed in the logic domain of networked equipment. This flexibility translates into less costly installation and provides for easier modification versus that of physical copper wiring. The implementation of fiber optic communications also empowers databases and software design and testing tools. It enables off-site manufacturing and testing of cables, is not open to many of the environmental, overvoltage or interference effects as copper wire and it can provide detection and diagnostics of the integrity of the communication path. A next generation protection and control secondary system must meet certain objectives of the utility company.

## 5. Technical Objectives

In addition to meeting the stated business objectives, a new protection and control system originates from the following technical objectives.

### 5.1 System performance

The next generation system needs to meet or exceed the performance of today's hard-wired solutions. With increased oversight from the regulatory bodies, the new P&C systems need to perform equally or better than today's systems or else the risk of impacting today's stretched power systems would outweigh the expected benefits – forcing the decision makers to take a conservative stand. Reliability is not the only factor to consider. Simplicity and security are other important factors that impact the overall performance by avoiding human errors and interference.

### 5.2 Safety

A key concern of utilities is safety, especially at a time of increasing intake of new staff to replace experienced workers leaving through attrition. A key benefit of any new system based on fiber optics is greatly enhanced safety through the elimination of CT and VT circuits from within the control house. Testing and maintenance procedures of such a system will largely be software based, thus significantly limiting the need to interact with physical electrical test points and circuitry associated with the primary equipment.

### 5.3 Interchangeable system conforming to an open standard

The system needs to be as interchangeable as today's copper based P&C schemes. An existing copper-based scheme may be easily replaced by the new architecture, and the new architecture can be replaced by a different version of a fiber-based system. Conformance to an open standard is a must to ensure that multiple vendors can provide compatible solutions. Engagement of multiple vendors ensures long-term viability of the next generation P&C architecture. The open standard that supports the next generation P&C architecture is the international IEC 61850 standard, using the definition of "process bus" contained in IEC 61850-9-2. Process bus is a generic technical term that in protection and control systems refers to a digital communications architecture that carries information between the switchyard and protection and control devices in the control building.

### 5.4 Cyber security

A growing concern in utilities is the threat of computer-based ("cyber") attacks on electric generation, transmission and distribution infrastructures due to the proliferation of protection, control and automation systems using switched Ethernet communications between devices and substations. In order to be truly acceptable within the utility sector, any proposed system should itself be secure from cyber-attacks, as well as not introducing any new attack vectors into existing protection, control and automation systems that would require additional security and add complexity to the system.

A successful architecture for a new protection and control system must take into account the key enterprise objectives discussed above, both business and technical.

## 6. Conclusions

In this paper, trends and expectations of the electric power industry for the next generation protection, control and automation system have been presented. It is clear that the successful system of the future needs to address these trends: cost pressures, retrofit schedules, labor shortage and shifting skill set in particular.

Copper-based signaling should be the central question in designing the protection and control system. Copper wiring is a source of physical variability that not only generates the majority of the labor cost, but also prevents transition of the industry from a "workshop" mode of production to a factory mode: with less assembly done in-situ by hand and more physical elements manufactured in a controlled environment, pre-tested and shipped with a manufacturer's warranty.

Being a part of a critical infrastructure, the new solution needs to be as reliable as today's proven systems. It also needs to be a simple and robust architecture that could be understood and dealt with by existing and future workforces.

A successful architecture will have to prove significant reduction in the total costs of installation and ownership. This should account not only for the initial engineering, construction and material cost of a solution meeting all other requirements, availability in particular; but also the costs of maintaining the extra electronic equipment and for cost benefits from reduced project durations, better workforce utilization and improved safety.

It is the real and measurable benefits that separate what is technically possible from what is eventually manufactured, given a chance to mature, and be deployed in the field. This is a lesson extrapolated from adoption of microprocessor-based multi-function relays.

## 7. References

- [1] "Frayed Wires: U.S. Transmission System Shows Its Age", Fitch Ratings report, October 25, 2006, [www.fitchratings.com](http://www.fitchratings.com)
- [2] W.K.Reeder, "The Technical Talent Challenge and Implications of Our Maturing Workforce" (IEEE Power and Energy Magazine, January/February 2006, pp.32-39).
- [3] IEC International Standard "Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3", (IEC Reference number IEC/TR 61850-9-2:2004(E), IEC, Geneva, Switzerland).

# An Architecture and System for IEC 61850 Process Bus

Bogdan Kasztenny, David McGinn, Wei Wang, Roy Mao, Drew Baigent, Nadejda Nazir, Steven Hodder, Jeff Mazereeuw

GE Digital Energy

## 1. Introduction

The IEC 61850-9-2 standard [1] focuses on transparency and standardization of data communications. Implementation issues such as suitable architectures, reliability, time synchronization, data sharing, maintainability, testability, and scalability remain outside the scope of the standard.

Process bus architecture is a missing element on the road to implementing the next generation of Protection and Control (P&C) systems. In this paper, architecture refers to the definition and structure of the process interface points, partitioning and allocation of functions to the devices, the underlying structure of time synchronization, settings and firmware management, failure-tolerant communication framework, required data throughputs and latency considerations, data traffic patterns, and other related aspects.

Careful analysis of the rules and symmetries occurring in topologies of high voltage substations allow for identification of process bus data traffic patterns, origins, destinations, and throughput required to accomplish a simple, robust, scalable and flexible IEC 61850 process bus architecture. The primary equipment itself drives a logical and natural architecture for a communication-based protection and control scheme.

This paper presents a practical process bus architecture conforming to IEC 61850-9-2 that fits the task of protection and control of substations by drawing from the universal topology rules of substations.

## 2. Technical Attributes of A Robust Process Bus Architecture

Successful technical solutions, including a process bus P&C system, are those that address important and well-defined real world problems. Therefore, development of a process bus protection and control system should be approached from the utility enterprise perspective that recognizes and addresses real and present needs of today's utilities – cost reduction and speed of deployment being the chief ones. The proposed process bus system originates from the following enterprise objectives:

- Achieving cost savings
- Reducing project duration and outage windows
- Shifting cost from labour to pre-fabricated material



- Recognizing copper wiring as a main driver for cost of labour
- Limiting skill set requirements
- Supporting optimum work execution
- Improving system performance and safety
- Using an Interchangeable system conforming to an open standard

With cost, labour and time requirements predominantly associated with copper wiring, the next generation P&C system should replace copper wiring by placing electronic modules throughout the switchyard and using fiber communications for bi-directional exchange of data. On the surface this is yet another remote I/O strategy, practiced for decades in the factory automation field. When applied to protection and control, however, the remote I/O approach faces a level of difficulty far beyond what has been worked out and proven in the realm of factory floor automation.

The following requirements must be factored into the design of a successful architecture. These must not be afterthoughts following an organic development of the concept. Instead, these requirements must be addressed as a part of high-level design before a single printed circuit board is laid out, line of code written, or dataset defined.

### **Comprehensible and complete architecture**

Any component of the system, including field (merging) units, Intelligent Electronic Devices (IEDs), communication infrastructure, datasets, time synchronization, and so on can be designed only after a complete architecture is created demonstrating the ultimate shape of the system. The architecture needs to be simple and intuitive for all affected disciplines in the user's organization. It needs to follow today's proven protection fundamentals and be fit for purpose – addressing the right problem with the right solution. The primary goal is to deliver switchyard data to the P&C devices and to return commands from the latter to the switchyard devices. Not all the process data is needed by all IEDs. The limited data requirements of each IED are clearly and unambiguously dictated by the virtually fixed power equipment arrangement. The process bus network need not be designed to accommodate arbitrary or evolving IED data requirements.

### **Reliability**

When increasing the number of electronic devices and connections in a system, the system's reliability decreases with the increasing device count. This can be easily demonstrated by using typical Mean Time To Failure (MTTF) data and running calculations on hypothetical process bus architectures [2,3]. Each additional element in the system will increase the failure frequency. In a properly designed architecture compensating measures, which often increase system complexity and cost, should not be required to make up for artificially reduced reliability.

### **Minimal co-dependencies**

Today, a single zone of protection can be taken out of service for upgrades, troubleshooting, periodic testing or maintenance without impacting the rest of the secondary system and without an outage in the primary system (for applications where there is a redundant protection system). A zone of protection can be engineered and deployed with minimal interactions with respect to other secondary systems. This separation has proved an indispensable foundation of practical protection engineering, and needs to be retained in the next generation solutions. Without proper consideration, a firmware upgrade for a single digital component of the system may result in unexpected system behaviour and ultimately may trigger a firmware upgrade to adjacent devices. Such domino effects created by co-dependencies are undesirable, may introduce latent failure modes and ultimately would become obstacles in acceptance of the system.

### **Scalability**

A successful system needs to be scalable. One should be able to deploy the system at any initial size (single zone up to an entire substation), and continue expanding one zone at a time as required. An expansion or modification should not raise any network congestion concerns, or other problems. The system must be both feasible and economically attractive in both retrofit and green-field situations.

### **Testability and maintainability**

The system needs to be provisioned to facilitate testing and maintenance. Testing is defined here as verification and re-verification of a complete protection and control system after it has been deployed – initial commissioning, repair, periodically or after a major work such as protection system expansion, firmware

upgrade or component replacement. Maintainability is defined as the existence of simple, safe and trusted means of performing firmware and setting changes and replacing faulty elements of the system. Addressing testability and maintainability is possible only by fundamentally engineering these facilities into the system at the beginning, not as afterthoughts in an organically developed solution.

### **Cyber security**

The system needs to be naturally secure from the cyber security point of view. The high data rates of the process bus traffic and the requirement of very high availability of this data create challenges for known cyber security solutions such as intrusion detection or encryption. Cyber security issues, if left unattended, may either slow down adoption of the solution by creating the need to augment it later for compliance, and/or may create extra cost and effort for the user when deploying and running the system. The best solution is to develop an architecture which does not introduce issues related to cyber security in the first place.

This section summarized the key technical requirements for the next generation P&C architecture. It is clear that these requirements need to be factored in early into the architecture development. The next section introduces the rules of substation topologies and explains how these rules lead into a process bus architecture that meets the stated requirements.

## **3. Observations on Substation Topologies**

Power substations are structured following strict rules.

The primary structure of any substation is divided into zones of protection. In order to minimize the size of an outage upon a protection trip, these zones typically span a single network element. Any protection zone is bounded by Current Transformers (CTs) that allow location of a fault, and Circuit Breakers (CBs) that allow isolation of the fault. These measuring and isolation boundaries are close to each other for better selectivity, and overlap in a certain way (the measuring zone is generally slightly larger than the isolating zone).

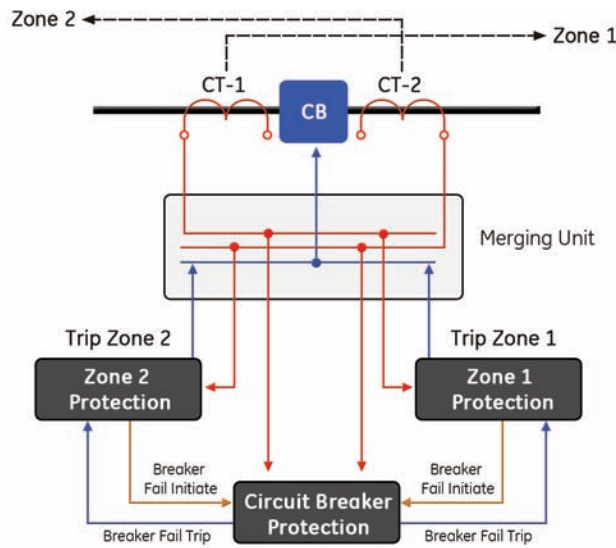
Traditionally, a single multi-function relay is used to provide protection for any given zone. Such a device needs access to all CTs surrounding the zone for a given principle of protection, and needs to control all CBs around such zone. Any given relay therefore, has well-defined data origins – there is no need to make all possible signals available to all possible relays. By the same logic, any given relay has well-defined signal destinations. These destinations (CBs) are generally coincident with the origins (CTs) as the measuring and isolation boundaries of protection zones are physically close to each other.

From the perspective of a relay there is a need for a bi-directional data exchange with points that bound its zone of protection. This creates a consistent one-to-many data traffic pattern. With the exception of a bus relay that may have a considerable number of CT/CB points surrounding its zone, all other known types of protection require access to just few points – typically all local three-phase conductors to the protected network element (CT/CB combination), and voltage from within the zone as needed.

Zones of protection are normally engineered to overlap in order to eliminate blind spots. Ideally this overlap should occur at the breakers, or at least within close proximity of the breakers. Engineering a precise fault measurement scheme without a corresponding means for fault isolation does not make economic sense (with a few exceptions such as transformer leads), therefore the situation depicted in Figure 1 is typical. In this arrangement zone 1 protection measures CT-1 (among others) and trips the breaker, while zone 2 protection measures CT-2 and trips the same breaker. Breaker Failure (BF) protection may be integrated with either or both of the protection relays, or implemented as a stand-alone device. In any case, the BF device will measure the same currents as the two protection zones.

A field (merging) unit is defined as a device interfacing with both CTs and the CB at the intersection of the two zones of protection in Figure 1. From that point of view such a unit needs to communicate with only 2 or 3 relays: the zone 1 and 2 relays, and potentially a stand-alone BF relay. This creates a universal one-to-many pattern for the bi-directional data traffic between the merging unit and its relays.

Detailed analysis of typical substation arrangements proves that the ability to feed four relays from a single merging unit covers all typical applications. For the few exceptions where more relays need to be fed from the same point, a second merging unit can be added and wired to the same signals.



**Figure 1.**  
*Intersecting zones of protection map into a process bus architecture.*

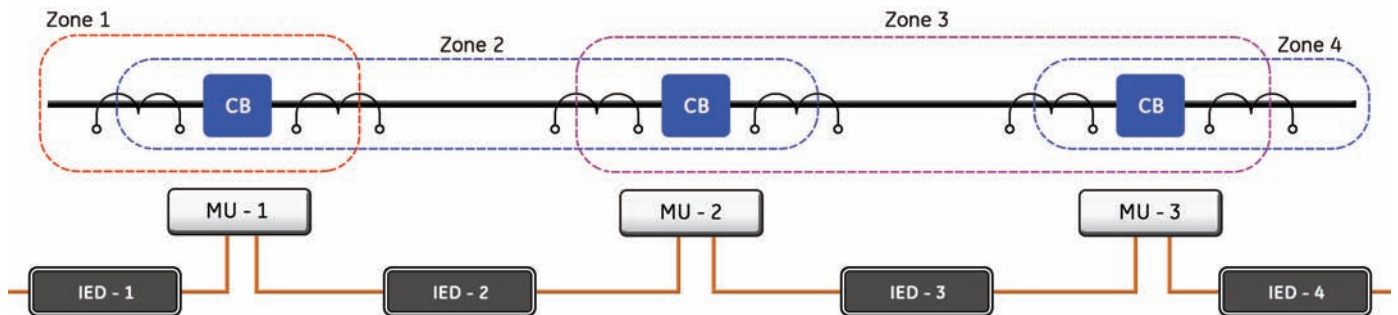
Zones of protection span and overlap breakers and network elements throughout the entire substation. This means that if a single merging unit is used for a given point of interest in the switchyard, the following domino effect takes place (Figure 2): IED-1 may need data from merging unit MU-1; MU-1 may feed IED-2; which in turn will connect to MU-2 to perform its function; etc. This means that the one-to-many data patterns of IEDs intersect with the one-to-many data patterns of merging units, seemingly putting all IEDs and merging units in the same communication network, and leading to a LAN spanning the entire substation. This would introduce maintenance and reliability problems, but can be avoided by observing that only four logical connections from a merging unit are required, which can easily be provided on a dedicated point-to-point basis.

Consider further a Breaker Failure application. With reference to Figure 1, when initiated from zone 1, the BF function should use CT-1 or CT-2 for the measurement, and upon breaker failure, it should issue a trip to all breakers surrounding zone 2, initiating their BF functions at the same time. Symmetrically, when initiated from zone 2, the BF function trips and initiates BF for all breakers of zone 1. This is a universal rule that holds true for all standard substation topologies.

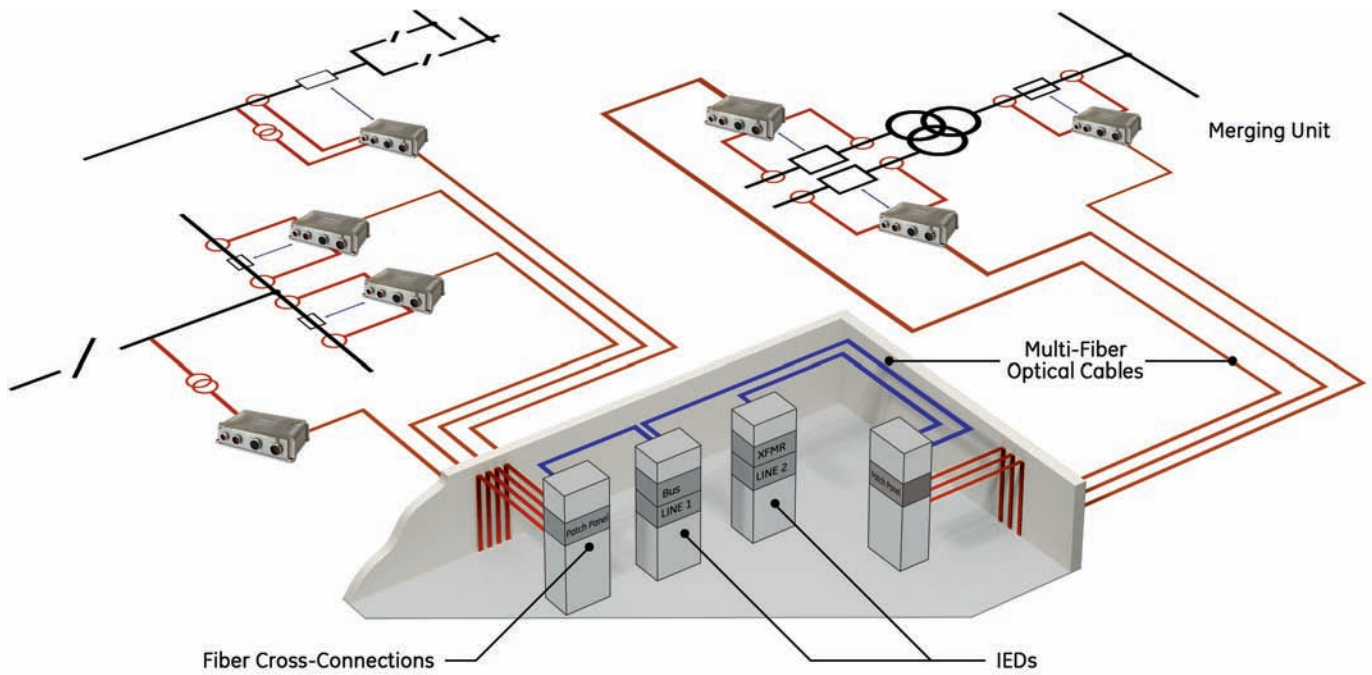
Note that from this perspective, a merging unit that monitors CT-1 and CT-2 while controlling the breaker in between, is a suitable data exchange point (a “mailbox”) for all involved IEDs. In order to function and issue a zone 1 trip, IED-1 needs to communicate with this merging unit, so it can also send a Breaker Fail Initiate (BFI) signal to the merging unit. In order to measure breaker current / position to perform its BF function, BF IED needs to communicate with the said merging unit, thus it can also receive a BFI from this merging unit. By the same logic, the BF IED can send the BF trip command to the said merging unit. This signal can be then forwarded by the merging unit to IED-2 and there executed as a trip and BFI for all breakers of zone 2.

The above observation shows how one could take advantage of the constraints imposed by switchyard topology to avoid challenges associated with passing BFI signals over station bus (isolation, testing, determinism) by building a fit for purpose architecture. From this perspective Figure 2 does not illustrate a problem anymore, but an opportunity. Station topology requires that any pair of IEDs that need to exchange protection signals typically both communicate with a common merging unit that may be used as a mailbox to forward the signals.

This section explained some of the rules and symmetries used to arrange primary equipment in a typical substation. When understood, these rules allow structuring a robust and simple process bus architecture as detailed out in the following section.



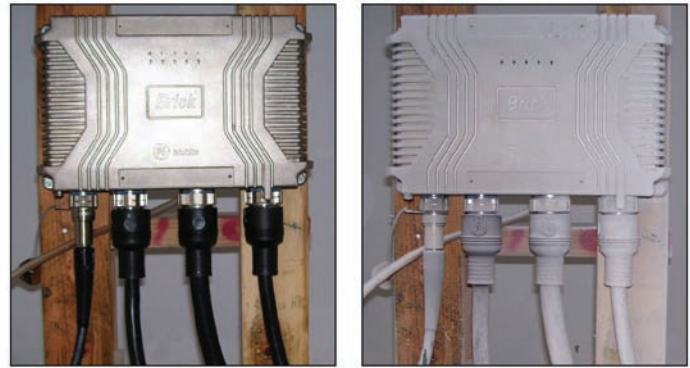
**Figure 2.**  
*One-to-many data traffic patterns.*



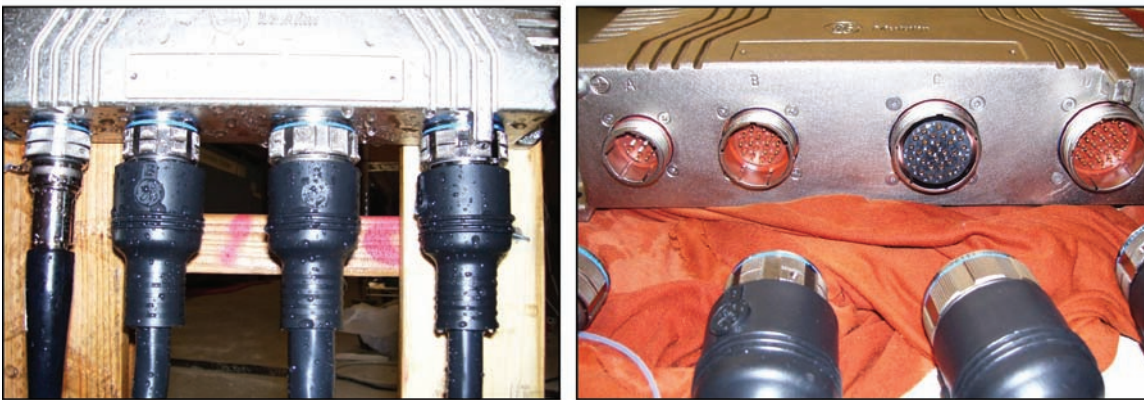
**Figure 3.**  
Proposed Process Bus architecture



**Figure 4.**  
Rugged outdoor merging unit



**Figure 5.**  
HardFiber Brick merging units tested for dust: pre-dust inspection (left) and post-dust inspection (right)



**Figure 6.**  
HardFiber Brick merging units tested for water ingress (pressure washing): post water inspection

## 4. Proposed Architecture For A Distributed IEC 61850 P&C System

The proposed architecture incorporates all the stated utility driven requirements in performance, maintainability, expandability and reliability through using merging units to collect CT/VT signals and CB/process control and status signals. The IEC 61850-9-2 output of each merging unit is connected via pre-terminated fiber cable to a patch panel that directs the appropriate signals to each relay.

In reference to Figure 3 the system includes merging units mounted at the primary apparatus, relay, pre-terminated cables, and fiber patch panels for cross-connecting the merging units and relays [4].

The merging units are designed to interface with all signals typically used for substation automation and protection as close to their respective origins as practical, including AC currents and voltages from instrument transformers, breaker status and alarms, breaker control, disconnect switch status and control, temperature and pressure readings, etc (Figure 4). The merging units are designed for harsh environments including temperature extremes, shock and vibration, electromagnetic compatibility, sun load effect, pressure washing and exposure to salt and other harsh chemicals (Figures 5 and 6).

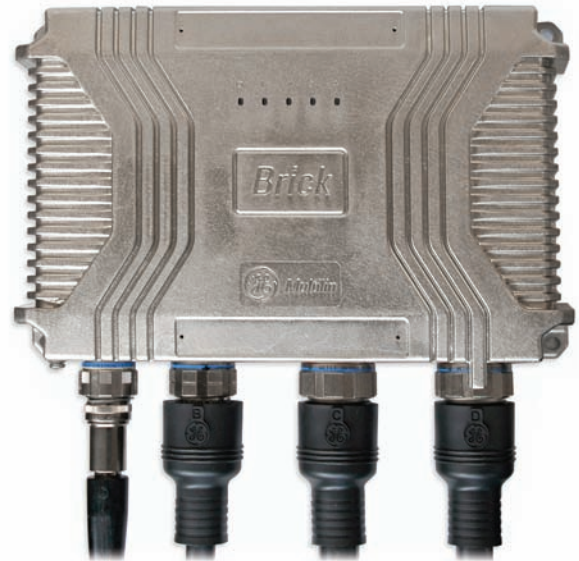
Each merging unit contains four independent digital cores each composed of a microcontroller with individual bi-directional (bi-di) fiber links providing dedicated point-to-point communications with a single relay. Sampled value communications used conform to IEC 61850-9-2, and GOOSE communications to IEC 61850-8-1. These cores share common input/output hardware, implementing a fail-safe design strategy that ensures total isolation and independence of the digital cores.

Enhanced security and availability of protection is optionally supported via duplicated merging units. No protection or control algorithms are implemented within the merging units; instead their sole function is to be a high-speed robust IEC 61850 interface to the switchyard.

All cables are connectorized and pre-terminated for ease of deployment and replacement (Figure 7), using standard military/avionic grade components. The outdoor fiber cables contain a pair of DC supply wires to provide control power to the merging units including the internal wetting voltage for field contact sensing (e.g. auxiliary switches, gas alarms, etc.) within the switchgear associated with each merging unit, independent from the control power in the field.

Patch panels (Figure 8) are used to land and organize the outdoor cables, and to distribute and individually fuse the DC power to the merging units. Standard patch cords are used to accomplish "hard-fibering", making all the necessary IEC 61850 connections between the relays and the merging units as dictated by the station configuration on a one-to-one basis, without the use of switched network communications as detailed in Figure 8.

Each relay has eight optical fiber ports, and thus can access directly up to eight merging units (Figure 9). These maximum connectivity numbers have been selected upon careful analysis of substation topologies and required data traffic patterns as explained in the previous section. As such the 8/4 connectivity covers almost all typical applications. Each relay provides protection for one basic zone, conforming to established protection philosophies.



**Figure 7.**  
*GE Brick merging units is fully pre-connectorized.*

It receives the signals to perform its function over a secure and dedicated network consisting of direct hard-fibered links to each of the associated IEC 61850 merging units. Due to the completely deterministic data traffic on these dedicated links, a simple and robust method is used for synchronization whereby each relay controls the sample timing of the connected merging unit cores over the link without relying on an external clock for process bus data synchronisation.

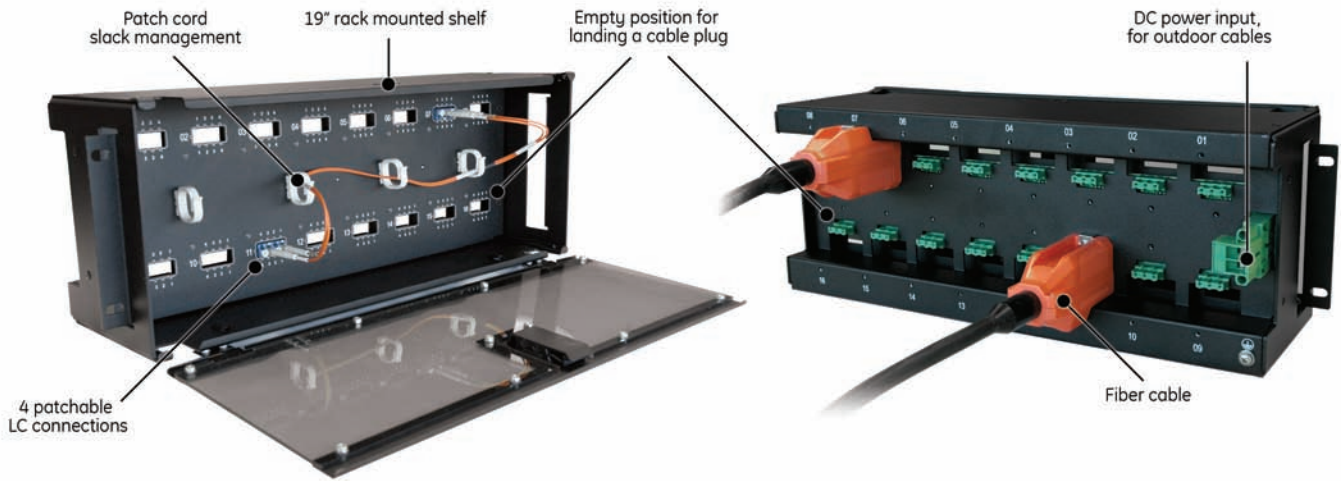
All architectural decisions have been made based on recognizing present technology and its current momentum as well as making practical tradeoffs. For example, the cost of implementing four independent cores in a merging unit is negligible compared with the gain of simplicity and independency of relays in the system. Similarly, the cost of point-to-point connectivity is comparable to implementing redundant switched networks with the added advantages of avoiding active network devices and supporting the ability to perform system maintenance and isolation.

All system components conform to the best industry standards:

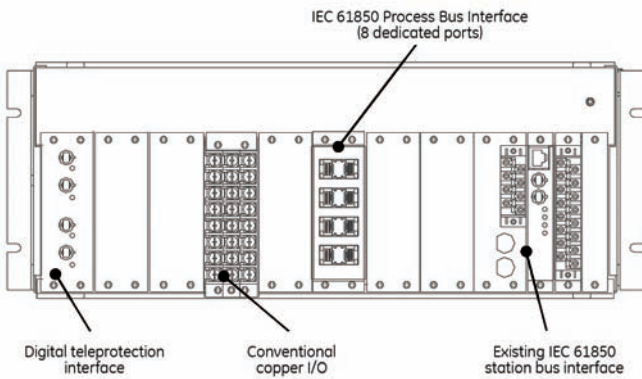
- Communications between merging units and IEDs conforms to IEC 61850-9-2 and IEC 61850-8-1
- Bi-directional Ethernet conforms to IEEE 802.3 100Base-BX
- Merging unit connectors conform to MIL-DTL-38999
- Patchable fiber connectors are standard LC type [per TIA/EIA-568-B.1].

The system can be implemented on existing relay platforms supporting all typically required applications. Owing to the built-in supervision and optional redundancy of inputs and outputs, the new system is more reliable when compared with today's solutions.

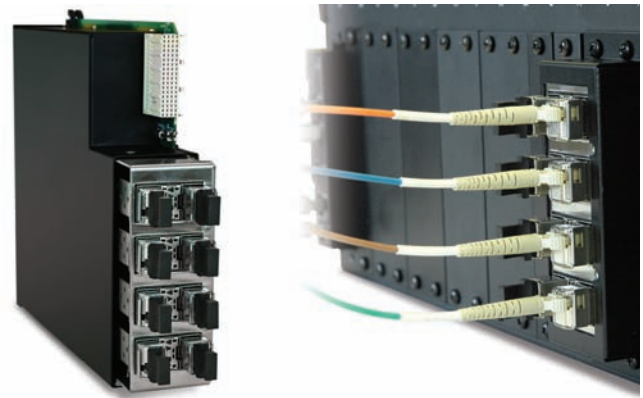
The following sections provide examples of system topologies, and elaborate more on key technical challenges and solutions.



**Figure 8.**  
HardFiber Cross-Connect patch panel



**Figure 9a.**  
IED's means of connectivity



**Figure 9b.**  
Rear view of the GE Universal Relay (right) incorporating 61850 Process Card (left).

## 5. Example 1

In reference [3] a benchmark substation topology has been proposed for the purpose of illustrating applications for IEC 61850 process bus architectures.

This station is a 10-breaker, arbitrary combination of a ring bus and breaker-and-a-half arrangements with two transformer banks that will be used to illustrate the proposed solution. Only one system is shown (main 1 or main 2), the merging units are deployed non-redundantly, and auto-reclose control is integrated within the line relays. Breaker Failure protection may be done in a number of ways in this architecture, and is not addressed in this example for simplicity.

Figure 10 presents the station topology, while Table 1 lists the IEDs and explains their associations.

Note that the count of IEDs is identical to a traditional solution. The second transformer bank is protected via bushing CTs, and two extra relays are used to provide differential protection for the HV and LV leads. Alternatively a single two-zone differential relay can be used to protect the HV and LV leads, reducing the number of IEDs to 10.

The IEDs do not carry the overhead of physical I/O. Instead the I/O interface is provided via a total of 16 merging units, marked B1 through B16. These units make available a total of 128 single-phase AC inputs. Almost 80% of them are utilized in this benchmark case. A total of more than 250 digital inputs are available on the 16 merging units allowing to interface breaker and disconnect positions and alarms. On average each merging unit feeds 2.625 IEDs. Two 16-position patch panels are required, 16 outdoor fiber cables, 14 indoor fiber cables, and 42 patch cords are needed to cross-connect IEDs and merging units.



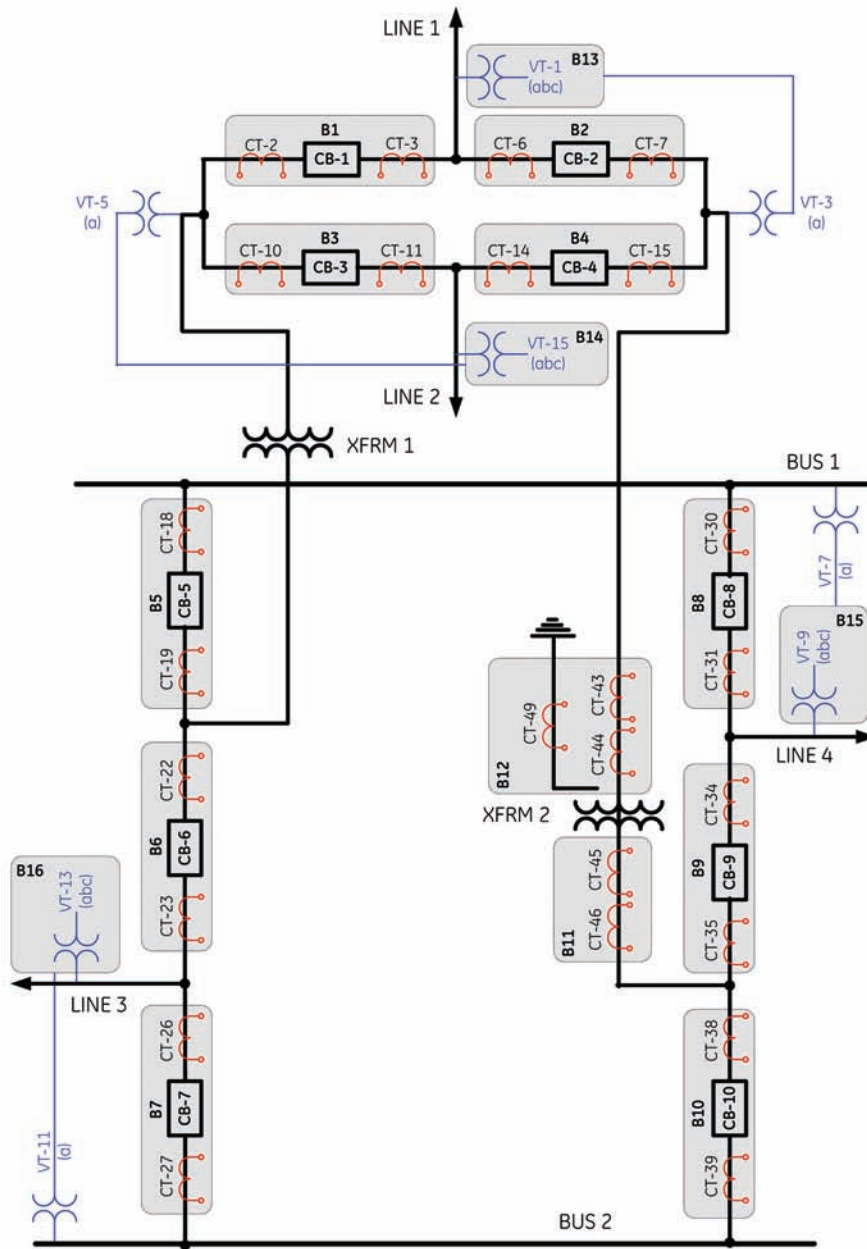


Figure 10.  
Sample benchmark case [3].

## 6. Example 2

Figure 11 presents another application example of the system. In this sample breaker-and-half diameter all merging units are deployed in a fully redundant configuration. CB-2 is a live-tank breaker with free-standing CTs (CT-3/4); there are no CTs on the L-1 line side of the breaker. CT column ground fault protection will use CT-5. The merging units interface with key signals as shown in the Figure. In addition, disconnect position/control can be interfaced via nearby merging units as well (not shown).

Table 2 associates the IEDs and their function with the merging units and their I/Os.

## 7. Key Technical Challenges

The two top technical challenges for the next generation P&C architecture are data sharing and sampling synchronization for AC inputs. A number of other technical issues such as firmware management simplify themselves once these two fundamental problems are solved. Note that neither of the two challenges is encountered in today's hard-wired protection applications: analogue signals are delivered via wires to each individual relay.

Zone (IED)	Merging Units																Comments
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
Line 1	x	x											x	x			CT-2, CT-7, VT-1 for protection and metering, Tripping CB-1 and CB-2, VT-3 and VT-5 for synchrocheck
Line 2			x	x									x	x			CT-10, CT-15, VT-15 for protection and metering, Tripping CB-3 and CB-4, VT-3 and VT-5 for synchrocheck
Line 3						x	x							x		x	CT-22, CT-27, VT-13 for protection and metering, Tripping CB-6 and CB-7, VT-5 and VT-11 for synchrocheck
Line 4								x	x				x		x		CT-30, CT-35, VT-9 for protection and metering, Tripping CB-8 and CB-9, VT-3 and VT-7 for synchrocheck
XFRM 1	x		x		x	x								x			CT-3, CT-11, CT-18, CT-23 for protection, CT-2, CT-11 and VT-5 for metering, Tripping CB-1, CB-3, CB-5, CB-6
XFRM 2		x		x					x	x	x	x	x				CT-43, CT-46, CT-49 for protection, CT 43 and VT-3 for metering, Tripping CB-2, CB-4, CB-9, CB-10
XFRM 2 HV leads		x		x					x	x		x					CT-6, CT-14, CT-44 for protection, Tripping CB-2, CB-4, CB-9, CB-10
XFRM 2 LV leads		x		x					x	x	x						CT-45, CT-34, CT-39 for protection, Tripping CB-2, CB-4, CB-9, CB-10
Bus 1					x			x									CT-19, CT-31 for protection, Tripping CB-5, CB-8
Bus 2							x			x							CT-26, CT-38 for protection, Tripping CB-7, CB-10
Total	2	4	2	4	2	2	2	2	4	4	2	2	4	4	1	1	On average each merging unit feeds 2.625 IEDs; 42 patch cords required

**Table 1.**  
List of IEDs and association of functions for the case of Figure 10

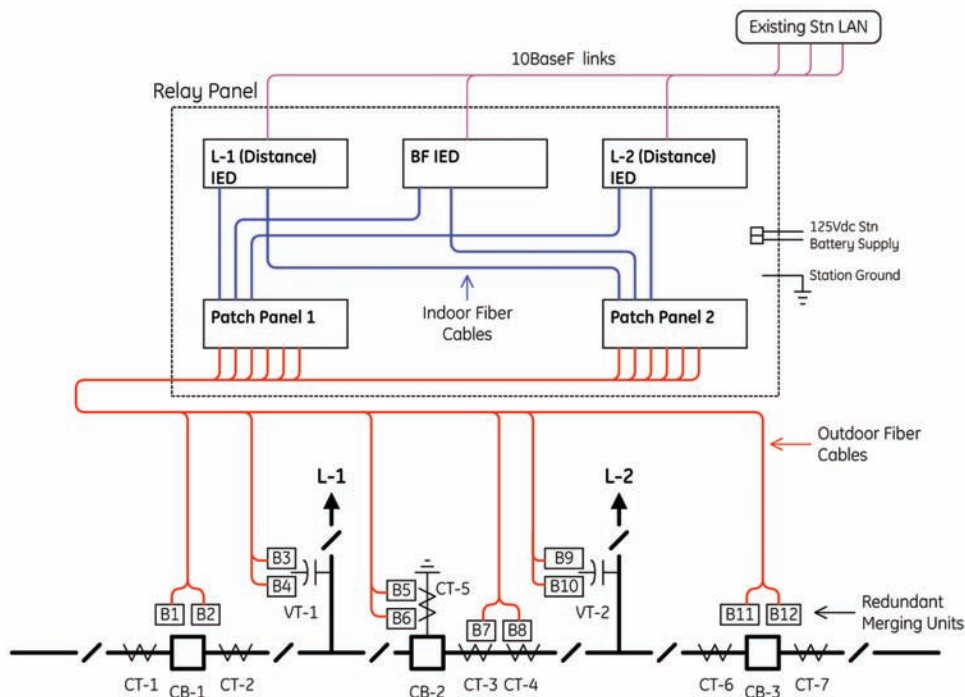
The proposed approach is best understood with reference to Figure 12. In this system each merging unit contains a common I/O structure and four digital cores. The I/O structure is controlled independently of the relays and digital cores by low-level hardware. The control circuitry is exceptionally basic and future-proof. The concept of a common I/O structure allows for a single compact field device and its associated wiring. That I/O structure is isolated from the digital cores using appropriately deployed hardware buffering. In this way it is impossible under reasonable failure conditions for the digital cores to interfere with the common I/O hardware or one another.

The cores are totally isolated on the hardware level and are comprised of independent microcontrollers running independent firmware instances, and communicating with IEDs via independent

fiber transceivers. The interface to the common I/O structure and the power supply circuitry is engineered to ensure total independence of the digital cores. Each digital core is associated with a specific IED, and each core runs as if it were the only core in the merging unit. For example, core number 1 may be working with a line current differential relay model A running firmware rev.5.61, while core number 2 may be in the process of upgrading its firmware to rev. 5.80, while core number 3 may be running firmware rev. 2.22 of a bus differential relay model B.

The independent cores combined with the concept of point-to-point connectivity allow solving the two key technical challenges.

Each relay operates in its own "time zone", developing its own explicit sample and hold signal (S&H) internally to match the needs



**Figure 11.**  
Example of application to a breaker-and-a-half diameter

Zone (IED)	Merging Units												Comments	
	1	2	3	4	5	6	7	8	9	10	11	12		
Line 1	x	x	x	x	x	x	x	x						CT-1, CT-4, VT-1 for protection, Tripping CB-1 and CB-2
Line 2					x	x	x	x	x	x	x	x		CT-3, CT-7, VT-2 for protection, Tripping CB-2 and CB-3
BF	x	x			x	x	x	x				x	x	CT-3/4 for BF protection, CT-5 for CT column ground protection, Tripping CB-1 and CB-3
Total	2	2	1	1	3	3	3	3	1	1	2	2		On average each merging unit feeds 2 IEDs; 24 patch cords required

**Table 2.**  
List of IEDs and association of functions for the case of Figure 11

of its specific application algorithms. This S&H signal is sent using IEC 61850 GOOSE messages to all merging units connected to the relay (up to 8 in the proposed architecture). Owing to the point-to-point connectivity, any foreign data traffic is prevented, and the GOOSE messages are delivered to the merging units in a short and very consistent time. In this implementation the S&H jitter is kept below 1 microsecond, with no need to run phase locked loops to average out random jitter. The payload of the GOOSE messages is a dataset controlling the local sampling and the outputs of the merging units (trip, close, interlock).

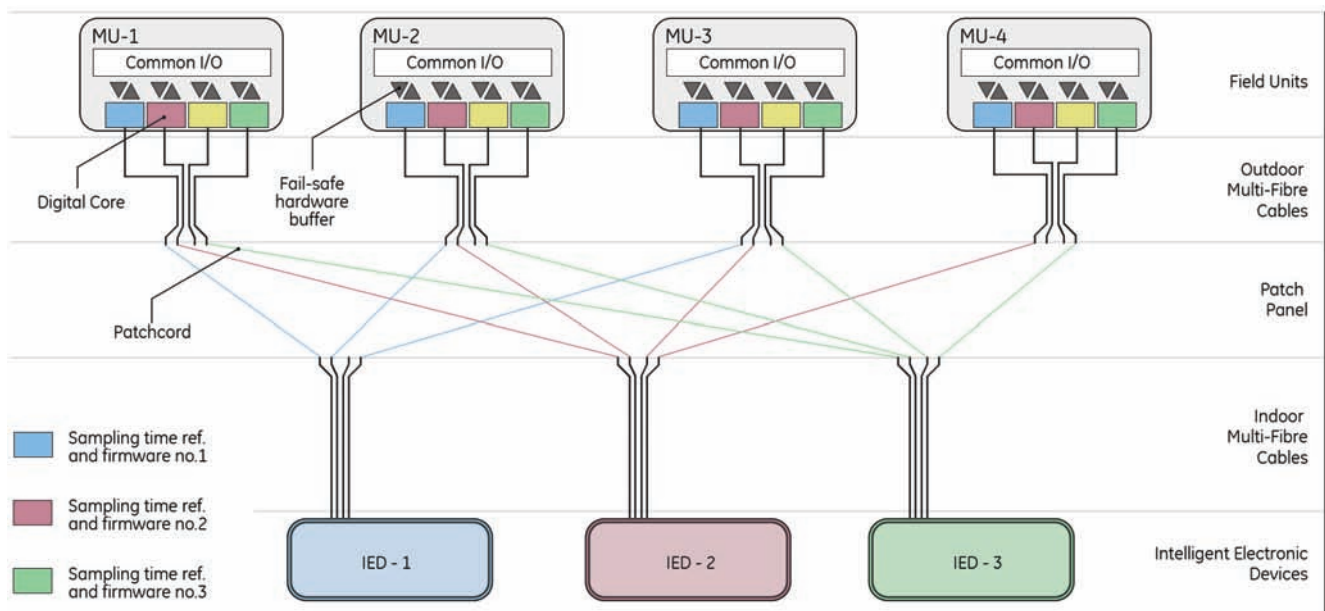
The common I/O structure of the merging unit collects AC samples based on its own free-running S&H clock at a relatively high rate. Individual copies of such physical samples are presented via independent digital links inside the merging units to each of the four digital cores. These cores, upon receiving their virtual S&H signals in the form of GOOSE messages, re-sample their own stream of physical samples to obtain and return virtual samples in precise synch with the requesting IEDs. In this way each merging unit supports 5 time references: one local and one for each of the 4 relays, all running asynchronously to each other.

Each relay receives its samples synchronized with its own S&H clock. The high physical sampling rate allows high accuracy of re-sampling required for metering and sensitive protection functions.

In this IEC 61850 architecture each relay can sample following its own frequency tracking scheme and different relays can apply different sampling rates. None of the sampling or protection functions are dependant on a central clock or on a large number of complicated distributed phase lock loops either within an open standard or proprietary that need to synchronize before the system can start producing and consuming data.

The concept of independent digital cores in the merging units facilitates not only independent timing zones, but also independent “firmware zones”. Upon start up each relay checks the firmware revision on all connected merging unit cores. If the revision does not match the firmware on the relay, the relay automatically loads the appropriate firmware to the connected core, while the other cores continue normal operations unaffected and unaware of the changes occurring in their neighbour. This operation lasts only milliseconds and is entirely transparent to both the user and the system.

The merging units do not have inherent firmware or settings – all is controlled from each connected relay. In this way the user is not exposed to the problem of permutations of firmware and settings among the relays and merging units (the domino effect). No software tools are required to deal with the merging units. A traditional relay setup program – as understood today – is sufficient to setup the system.



**Figure 12.**  
Independence of sampling clocks and firmware between devices in the system

The second issue of data sharing is solved via point-to-point connections. This is a very simple and robust solution, eliminating a whole array of problems associated with switched networks. On the surface this point-to-point scheme might seem to carry a cost overhead and reliability degradation associated with the number of transceiver ports and fiber terminations. This is not actually the case.

In a switched network architecture, two ports are required to integrate each merging unit (one in a switch and one in the merging unit). The same applies to each of the main 1 and main 2 relays to switch links. This makes the total number of ports in a system equal to the number of merging units times two plus the number of relays times four. Assume each relay works with 6 merging units on average (two CB/CT points and one voltage point, each with redundant merging units). Also, assume each merging unit feeds 3 relays on average (zone 1, zone 2, stand-alone BF). This implies there are two merging units for each relay. Thus the number of ports in such a system is on average 8 per relay. In practice some extra ports are used up to build a LAN out of switches with a finite port count. Assume an overhead of 1 extra port per relay, bringing the total in this example to 9 ports per relay.

In the point-to-point architecture presented in this paper, a total of 12 ports are required per relay to connect 3 merging units and 3 redundant merging units (6 in the relay and 6 in the merging units). However due to the fixed port count in relays and merging units of 8 and 4 respectively, the actual total is 16 ports per relay in this example. The 9:12 proportion for reliability considerations, and 9:16 proportion for hardware considerations are acceptable given the gain of simplicity, maintainability and reliability of the proposed architecture.

Moreover, this architecture uses bi-directional fiber (using wavelength division multiplexing per IEEE 802.3 100Base-BX), cutting the number of fiber terminations by half, improving both cost and reliability.

This architecture has an additional advantage in that signal routing is completely defined in hardware at the patch panel. No software configuration or active components are required.

This section explained how the proposed architecture solves the key technical challenges for the IEC 61850-9-2 P&C system: time synchronization and data sharing.

## 8. Summary

The paper presents a robust IEC 61850-9-2 process bus architecture for distributed protection, metering and control. In particular the solution:

- Targets copper wiring as a major cost, labour and time factor, and replaces copper wiring for protection and control purposes in the switchyard and the control room with fiber-based communication.
- Introduces rugged merging units that solve practical problems such as outdoor fiber cabling and connectivity in harsh conditions, weatherproofing, commissioning, maintenance, and expandability.
- Uses merging units designed to interface all process interface

measuring and control points at a given switchyard location using a common device conforming to IEC 61850 and working with a standard I/O structure: status inputs, binary output commands, transducers and sensors, and instrument transformers.

- Uses an optimized communication framework that mirrors the topology of the primary equipment and recognizes the exact data flow patterns, origins and destinations required to accomplish a practical zone-based approach to protection.
- Solves the data synchronization problem without reliance on external clocks, and their associated communication-based or hard-wired distribution.
- Solves the data-sharing bottleneck for substations of any size without relying on impractical throughputs, in a simple, robust, scalable and maintainable communication framework.
- Increases reliability by a novel concept of redundancy and optimized communication architecture.
- Eliminates cyber security concerns by using a non-routed communication scheme.
- Eliminates the need for extra software tools for setting up the process bus data.
- Preserves all major protection principles successfully practiced for decades:
  - separation of protection zones,
  - determinism,
  - independence of devices,
  - simplicity,
  - ability to augment a single protection zone without the danger of affecting adjacent zones, and other potentially problematic aspects.

The work presented in this paper reflects the actual development of a complete system encompassing all major protection application types [4].

## 9. References

- [1] IEC International Standard "Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3", (IEC Reference number IEC/TR 61850-9-2:2004(E), IEC, Geneva, Switzerland).
- [2] M.Adamiak, B.Kasztenny, J. Mazereeuw, D. McGinn, S. Hodder "Considerations for Process Bus deployment in real-world protection and control systems: a business analysis" (42 CIGRE Session, Paris, August 24-29, 2008, paper B5-102).
- [3] B.Kasztenny, D.Finney, M.Adamiak, E.Udren, J.Whatley, J.Burger, "Unanswered Questions about IEC 61850 - What needs to happen to realize the vision?" (Proceedings of the 31st Annual Western Protective Relay Conference, Spokane, WA, 2005).
- [4] HardFiber System Instruction Manual, GE Publication GEK-113500.

# The Advantages of IEC 61850 Process Bus Over Copper-Based Protection and Control Installations

Steven Hodder, Rich Hunt, Dave McGinn, Bogdan Kasztenny, Mark Adamiak  
GE Digital Energy

---

## 1. Introduction

This paper reviews key aspects of the process of implementing traditional hard-wired solutions utilizing integrated multi-function relays and compares them with implementing the equivalent system using an IEC 61850-9-2 [1] process bus solution [2]. The various benefits as they relate to the engineering, construction, commissioning, and routine maintenance from transitioning from traditional Protection and Control (P&C) systems to a process bus solution are reviewed.

Typically benefits are translated into specific cost savings on a project. Recognizing differences in absolute cost and relative costs of materials and labour, as well as other factors such as accounting for constraints resulting from labour regulations, relative currency differences and so on, specific financial costs savings are difficult to predict in a general case. However, by deploying practical IEC 61850 process bus-based P&C systems, it is estimated that total labour savings approaching 50% or more are realizable over the life of the system, particularly in green-field installations.

Not all benefits can directly be translated into specific monetary savings. A number of benefits relate to the ability to better optimize the utilization and deployment of resources, improving the overall efficiency in using both capital and operating & maintenance budgets. This paper presents evidence as to these assertions.

## 2. The Traditional Protection & Control System

The traditional P&C system uses individual copper wires to transmit signals from the switchyard to protective relays in the control house. Each copper wire for an individual signal is terminated at the primary apparatus in the switchyard, pulled through cable trenches to a termination block in the control house, then is terminated numerous times within the control house through terminal blocks, test switches and various relay terminals. The signal is then returned from the relay to the primary apparatus through even more terminations. One complete copper signal path typically requires 8 or 10 terminations.

During the design phase, these numerous copper connections result in large amounts of variability in engineering design. Each design and application will be unique, based on the individual site location, designer and design requirements. Design changes require significant manual labour to implement the changes in the copper connectivity. Each change usually requires a skilled draftsman revising a large number of drawings manually. Materials are procured and installed as individual components in the system, and the number and type of materials vary between zones, again due to all of the variability introduced by the copper wiring.

On-site construction, commissioning and maintenance also expend a great deal of effort, and consequently carry a high cost, dealing with copper wiring. Each wire and termination is made by hand in the field, one wire at a time, using expensive, skilled labour. The integrity of each copper signal path needs to be verified during commissioning, and errors require troubleshooting and rework to correct. High-energy signals from primary equipment are brought to the control house and therefore test switches are required during maintenance procedures to isolate these signals for both personnel and equipment safety. Isolating and restoration of individual signals using test switches during maintenance carry a risk of human error and misoperation of protection, as all of the correct test switches must be opened to start maintenance safely, and then correctly restored for proper system operation after restoration.

Project management is difficult, as there are large requirements for skilled labour, and many handoffs between engineering, drafting, construction, and maintenance groups in the utility. All of these handoffs must be accounted for in the project schedule, and a delay in one group handing their output to the next group can have significant impact to the project in terms of both delays and cost overruns.

### 3. A Practical Process Bus System

One example of a practical IEC 61850 process bus system is the HardFiber system from GE shown in Figure 1. This system is made up of a small number of standardized components, almost completely connectorized for fast installations and easy replacement. The system itself is naturally scalable, supporting the addition of new zones and modifications to existing zone in a straightforward and low-risk manner.

### 4. The Benefits of IEC 61850 Process Bus

Benefits of a particular process bus system, the HardFiber System [3], can be found at every step of the design, installation, and maintenance of P&C systems. Standardized components, copper terminations that end at merging units installed at primary apparatus in the switchyard, and purpose-driven, straightforward architecture simplify procurement, engineering, drafting, construction, commissioning, maintenance, and operations.

#### 4.1 Materials

With the HardFiber system, materials become a finite set of standard components, with a small number of each type, across all zones and stations. Regardless of the physical construction or vintage of the associated primary apparatus and the nature of the project (new construction versus retrofit), the interface to the primary power system is always exactly the same. Even the order code for the associated protective relay is reduced to a relay with a single IEC 61850 Process Card for virtually every application.

Control buildings and cable trenches can be greatly reduced in size due to elimination of most of the bulky copper cables, terminal racks and AC and DC test switches on relay panels.

#### 4.2 Engineering

The interface between the protection and control system and the power system is always presented exactly the same, regardless of the actual physicals of the substation – the interface is always a Brick located in the switchyard at the end of a fiber optic communications channel. There is only minor physical variability in mapping Bricks to specific relays, based on the topology of the switchyard as mirrored in the provisioning of specific protection & control zones. All of the variability with respect to the mapping of specific power system signals is transferred completely into the specific configuration of each relay involved in protection and control, as opposed to the mapping and connection of specific physical signals via copper wiring.

The HardFiber system is based on the well-proven Universal Relay (UR) family of protection and control relays, covering a wide range of protection applications and zones. The use of a known relay product line, coupled with the fact that the fundamental operation of the relay algorithms remains unchanged, greatly reduces the risk and amount of type testing necessary to adopt, adapt and deploy the HardFiber system.

#### 4.3 Drafting

The only documentation required for copper connections in the switchyard is in the interface wiring between the primary apparatus and the corresponding Brick I/O. These documents can be standardized to each primary equipment vendor and type. The documentation for the installation of the Bricks in the primary apparatus may be specified as deliverable as part of purchase of apparatus.

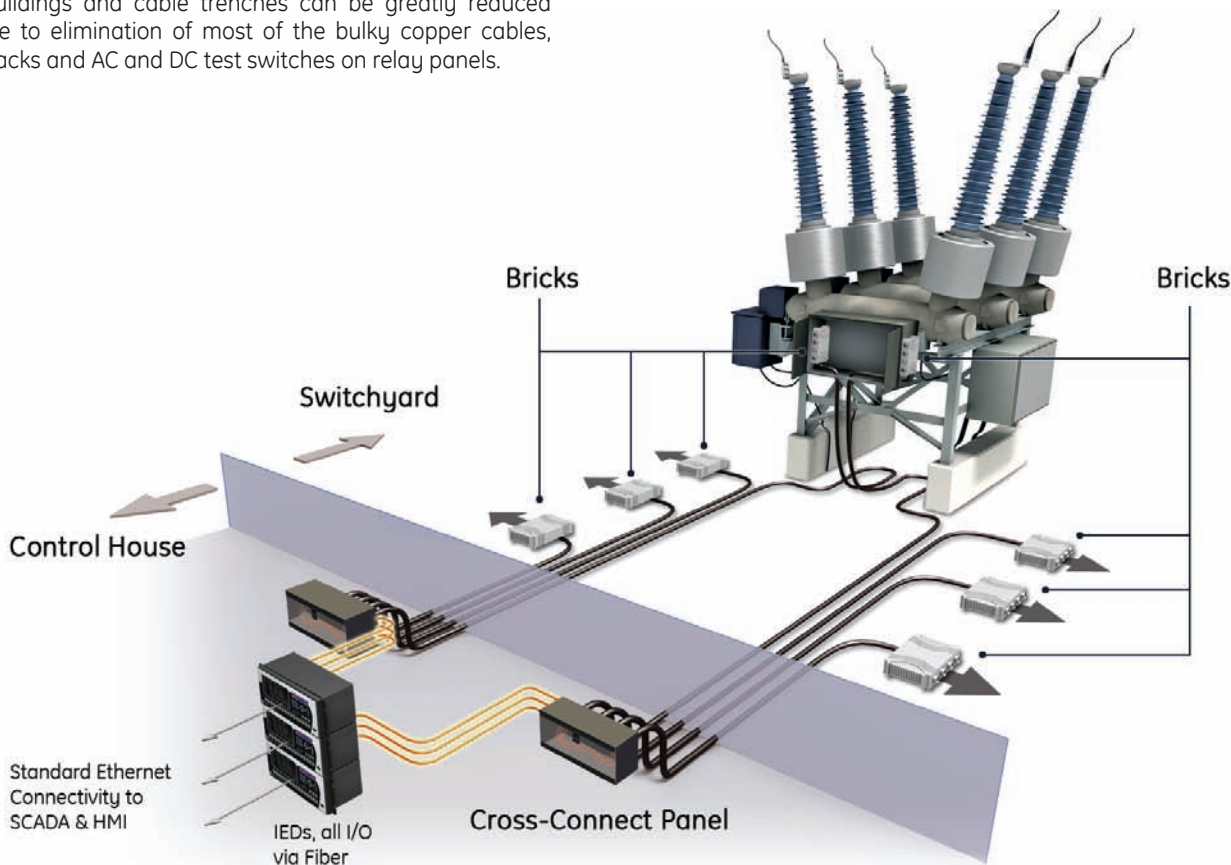


Figure 1.  
HardFiber process bus architecture

Within the control house, the amount of documentation for the connectivity is vastly reduced and simplified to single point-to-point fiber connections. These connections can be summarized in tabular form as opposed to drawings, and may even be automatically generated by software to create system and connection documentation.

#### 4.4 Construction

The construction effort needed to make on-site copper connections, and is virtually eliminated when the apparatus manufacturer installs Bricks in the primary apparatus prior to delivery to site. The chance for errors is vastly reduced by eliminating the majority of copper terminations and by standardising the physical connectivity between the primary apparatus and the Bricks.

The simplified interface point to the switchyard offered by the Cross Connect Panel provides faster on-site installation for P&C systems, particularly where turn-key control buildings are used with primary apparatus pre-wired with Bricks.

#### 4.5 Commissioning and Maintenance

Continuous monitoring of the architecture and equipment reduces protection misoperations from incorrect isolation or restoration during protection testing [4]. Construction errors are limited to provisioning of communication between origin and destination of information. No high-energy signals (AC or DC) are present in the control building for greater personnel safety when working on protection and control systems.

By providing the opportunity to use fully duplicated field measurement hardware (Bricks), along with continuous self-monitoring of all hardware and communications allows maintenance to be condition-based (event-driven, e.g. run-to-fail) as opposed to calendar-based periodic maintenance. This reduces the costs associated with maintenance over the entire life of the P&C system, and reduces the opportunity for power system interruptions to occur due to human error during isolation and restoration of a P&C system during routine maintenance.

#### 4.6 System Modifications & Switchyard Additions

The HardFiber system's point-to-point architecture allows for the same degree of scalability that traditional hardwired P&C systems provide. Each zone can be conveniently engineered, installed and commissioned individually without impacting adjacent zones. For retrofit applications, the HardFiber system can be deployed for a single zone only, for example the addition of a new capacitor bank on an existing station, without disturbing the existing in-service protection nor requiring the entire station protection be converted to a process bus-based solution.

Similarly, existing process bus-based protection zones may be expanded to incorporate new power system elements by tapping to the newly added Brick. The dedicated point-to-point architecture of the HardFiber system allows new zones and new equipment to be added and integrated without concerns regarding isolation for existing protection and control applications or adverse system performance from increased network traffic.

#### 4.7 Project Management

Procurement, engineering, and construction are greatly standardized, and fewer handoffs with less labour effort required at each stage increase productivity and helps control and reduce project cycle times. Up-front decisions regarding material planning are simplified, so engineers and draftpersons can be engaged earlier on detailed design work, without needing the complete physical details of the installation.

Another advantage is the execution of work on-site is almost completely decoupled from the presence of large components like breakers and a control at the substation. Outdoor fiber optic cables for the Bricks can be run at convenient time when labour is available, even if the Bricks have not been installed yet. Turn-key control houses can be assembled in a controlled environment and completely tested to the demarcation point (Cross Connect Panel) prior to delivery to the substation site. Bricks can be installed in the primary apparatus, and even tested in-situ to ensure the correctness of the copper interface wiring. Ideally, new breakers or refurbished breakers will have the Bricks installed and tested in the controlled environment of the breaker shop. The on-site installation then becomes the simple task of making fiber optic connections between the pre-tested relays in the control house and pre-tested Bricks in the switchyard – a truly “plug-in” substation project.

#### 4.8 Operations

The high degree continuous self-monitoring and optional duplicated measurement hardware allows the hardware implementing protection and control to detect spontaneous failures and go into a fail-safe state, thereby preventing certain protection maloperations and the corresponding unexpected outage of the primary power system. The Brick, with its connectorized cabling and no internal settings or firmware facilitate fast replacement of hardware without requiring long outages to re-commission protection and control systems in the event of a hardware failure.

#### 4.9 Cyber Security

The dedicated, point-to-point architecture of the HardFiber system does not contain any active network switching or routing hardware, and therefore does not require any external access for monitoring or configuration purposes. Due to its completely isolated nature, the HardFiber system as designed is implicitly secure from external cyber security threats and by design complies with cyber security requirements.

## 5. Conclusions

In this paper, some of the advantages have been presented that are realized by deploying an IEC 61850 process bus solution like the HardFiber System to implement power system protection & control systems.

Copper-based signalling is the central question in the IEC 61850-9-2 process bus discussion. Copper wiring is a source of physical variability that not only generates the majority of the labour cost, but also prevents transition of the industry from a “workshop” mode of production to a factory mode: with less assembly done in-situ by hand and more physical elements pre-tested and shipped with a manufacturer’s warranty. This optimization of labour is going to become a key consideration in the electricity sector for many years to come [5].

Utilities should strategically look at the adoption of a low-risk process bus solution like the one presented in this paper and take advantage of all of the tangible business benefits such as project cost reduction, faster facility construction, lower maintenance costs and improved reliability that this exciting new technology offers.

## 6. References

- [1] IEC International Standard “Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3”, (IEC Reference number IEC/TR 61850-9-2:2004(E), IEC, Geneva, Switzerland).
- [2] HardFiber System Instruction Manual, GE Publication GEK-113500.
- [3] B.Kasztenny, D.McGinn, S.Hodder, D.Ma, J.Mazereeuw, M.Goraj, “A Practical IEC61850-9-2 Process Bus Architecture Driven by Topology of the Primary Equipment” (42 CIGRE Session, Paris, August 24-29, 2008, paper B5-105).
- [4] D.McGinn, S.Hodder, B.Kasztenny, D.Ma, “Constraints and Solutions in Testing IEC 61850 Process Bus Protection and Control Systems” (42 CIGRE Session, Paris, August 24-29, 2008, paper B5-206).
- [5] W.K.Redder, “The Technical Talent Challenge and Implications of Our Maturing Workforce” (IEEE Power and Energy Magazine, January/February 2006, pp.32-39).

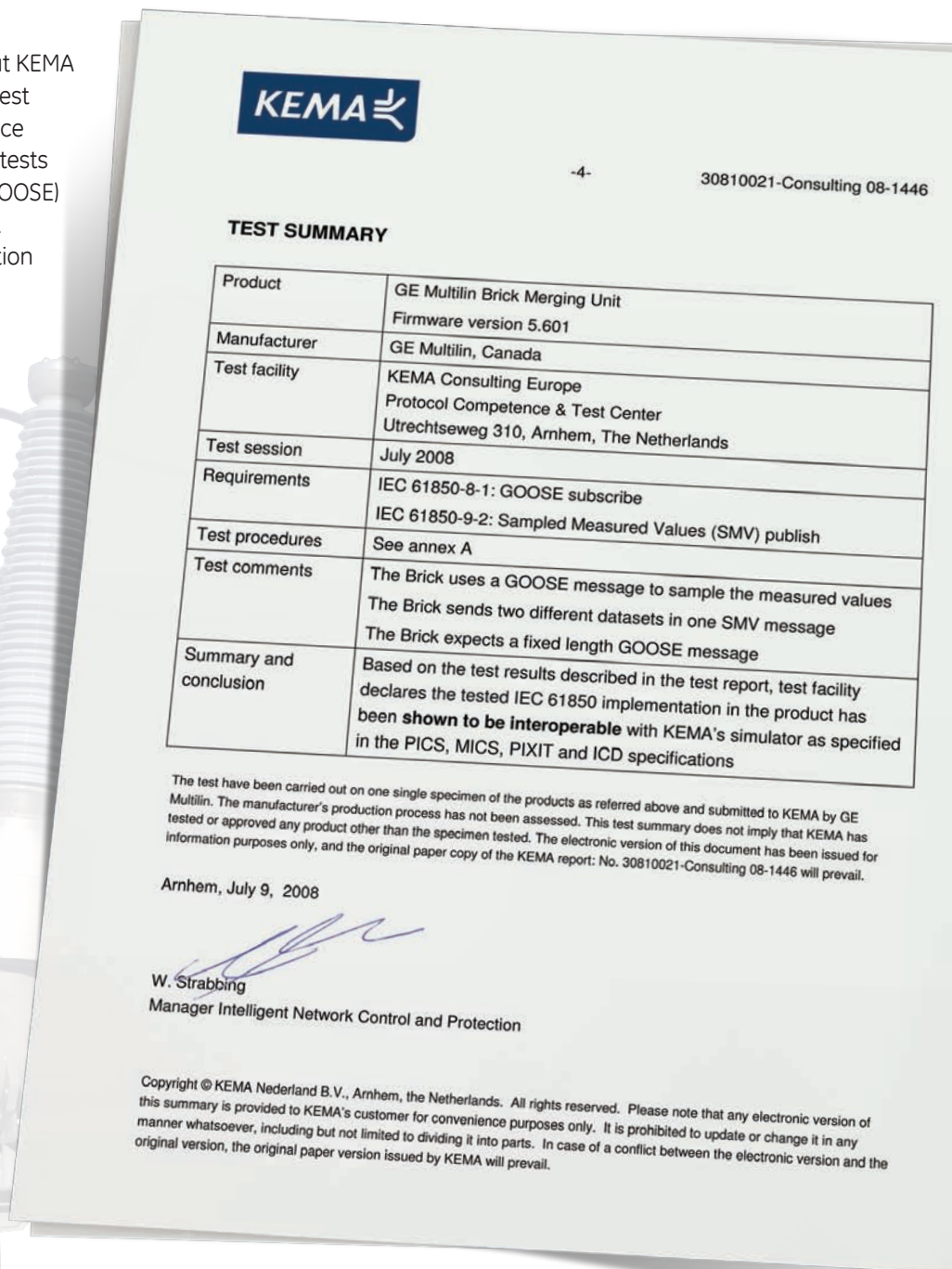


# GE Digital Energy's Multilin HardFiber™ System Tested for IEC 61850

GE Digital Energy is pleased to announce that KEMA Consulting Europe, Protocol Competence & Test Center has successfully performed compliance testing of the Multilin HardFiber System. The tests covered communication to (IEC 61850-8-1 GOOSE) and from (IEC 61850-9-2) the HardFiber Brick merging unit. The tests have shown the solution to be interoperable as per KEMA's testing methodology.



**HardFiber™ Brick**  
Hardened Switchyard Interface





# MPHUSKY

CABLE TRAY & CABLE BUS



MPHusky Cable Bus systems are designed and manufactured to utilize less conductive material, providing significant savings versus non-segregated phase bus duct, conduit and wire, and other electrical feeders. As copper prices have continued to remain at historically high levels, the savings clients realize are even greater and more important.

*Cost savings of 40% or more!*



## It's Just Plain Better!

No matter how you look at it, MPHusky Cable Bus outperforms other electrical busways in reliability, cost, and flexibility. See for yourself why more engineers, owners and buyers choose MPHusky Cable Bus Systems over the competition. Call today for more information at

**864-234-4800**  
or visit our new website.

**m p h u s k y . c o m**



# Detection of Incipient Faults in Underground Medium Voltage Cables

Bogdan Kasztenny, Ilia Voloh  
GE Digital Energy

Christopher G. Jones, George Baroudi  
Consolidated Edison Company  
of New York, Inc.

## 1. Introduction

Medium voltage underground cables may exhibit incipient, self-clearing arcing faults prior to failing permanently. These events typically last one half-cycle and extinguish at the first natural zero crossing of the current. The magnitude of the half-cycle event is primarily dependent on the location of the fault on the feeder, but is also dependent on the point on the voltage waveform that the fault starts.

Operational experience, at least in urban areas, suggests that it is beneficial to trip a feeder suspected of incipient cable faults automatically very early after detecting first symptoms of an incipient fault. Because it limits the overall energy at the point of fault, it also limits the often-repeated voltage transient seen by the system. However, the relatively short duration of an incipient fault and the inability to achieve selectivity via time coordination, make the design of an incipient fault protection function challenging. A simple instantaneous overcurrent element is not sufficient.

Along with presenting operational experience of these half-cycle events at a large urban utility, this paper details a simple and robust method for detecting incipient faults in cable and combined overhead and cable feeders. A number of security measures are implemented to make the method fast, secure and selective.

The method is based on current signals only (no voltage signal required) and, therefore, can be applied in simple feeder overcurrent relays. The logic is simple enough to be programmed via user-programmable math and logic available on some modern microprocessor-based relays.

Test results are presented and explained, including playback of field events and transient simulation using a digital power system simulator.

## 2. Operational Experience with Underground Cables

With the increased installation of system power quality monitoring devices at the substation level, it was noticed that prior to approximately 10 to 15% of feeder trips the feeder exhibited earlier signs of breakdown in the form of the half-cycle events described above.



Because the monitoring devices were at the substation level, typically installed on one of the supplying transformers, it was not known on which of the 8 to 30 feeders the disturbance was occurring. What was known was that anywhere from two cycles to two weeks later, these half-cycle events could manifest into a permanent multi-cycle fault, on the same phase, which would operate traditional overcurrent relay elements. The number of half-cycle events that occur before the “true” fault could be anywhere from one to more than 100.

Very rarely has a half-cycle event occurred in the medium voltage underground network system that has not resulted in a subsequent fault that could be linked to the earlier event by phase and also by magnitude of the neutral current.

The operating implications of these half-cycle faults are as follows:

### 2.1 Fault energy and safety

The resulting arc flash energy from these half-cycle events is typically 10 to 20% of a full 3- to 5-cycle fault. Limiting the energy released in a fault obviously has safety benefits for a crew that may be working in the vicinity of the feeder, and also limits the damage to other feeders or equipment. It also has benefits for transformer faults, in that it limits the possibility of a violent failure.

At one extreme, if the relay is enabled to trip after one half-cycle event, with no intentional delay, this would limit the energy of the full fault for almost all cases, except those where the half-cycle event precedes the eventual full fault by less than 3 to 5 cycles.

The other option is to have the relay alarm for these events, if the microprocessor relay is connected to an alarming scheme. This helps identify which feeder the fault is on, and the feeder may be taken out of service, or work in close proximity to the feeder restricted. Of course, this has limited value, because the full fault may occur before operational people can react to the alarm.

The decision as to whether to trip or alarm has the following considerations

- will it eventually fail permanently
- what are the system conditions at the time of the fault
- can the fault be located

Ability to locate the fault is a major consideration in making the decision to allow tripping or just alarming.

## 2.2 Network reliability

Every time there is a fault on the system, whether it is a full fault or a half-cycle fault, there can be some elevated voltage transients, particularly at the interruption of the fault. This is even more prevalent for ground faults on a large network system supplying delta-connected transformers from a station that is effectively ungrounded (typical source impedances for a Con Edison Area Station are  $Z1=0+0.2j$  ohms,  $Z0=0+0.95j$  ohms).

The problem that half-cycle faults present that are not present in "true" faults, where the feeder breaker opens, is that the half-cycle faults can occur numerous times in quick succession. On a number of occasions they have been seen to occur multiple times at periods of less than 2 or 3 seconds apart. If, on occasion, a half-cycle fault occurred in a cable joint on a feeder about 40 to 50 times over 90-second period. At the end of the 90-second period, the fault manifested into a true fault, and tripped the breaker, but in the intervening 90 seconds, 2 other faults occurred on separate feeders, almost certainly caused by the voltage transients that occurred on the clearing of each half-cycle event. Within a 90-second period, the network went from all feeders in-service to a 3rd contingency, which was beyond the level designed for.

## 2.3 Fault location

There is another consideration regarding opening or tripping the feeder that has had these half-cycle faults: whether the fault can now be located using the fault locating techniques presently employed. The thinking being that because the fault self-healed at the first current zero, it will be less likely to break down again under elevated test voltage. This is certainly a consideration and to date there is very little data on this issue, as almost no feeders have ever been taken out of service for a half-cycle event.

However, there have been a few occasions where the fault has been a full-cycle self-clearing event, which operated the traditional relaying protection. Under these circumstances no particular difficulty was observed in locating the fault.

Although rare, another issue that has occurred is where the flash from a half-cycle event is observed by the public or by a crew. The knowledge that it is a primary half-cycle event, and not a low voltage secondary event, is garnered from a corresponding half-cycle disturbance recorded by the substation Power Quality

(PQ) device. In this case, where the manhole structure contains only one primary feeder, the issue is simple. Take the feeder out, confirm the location of the fault, and repair. However, when there are multiple primary feeders in the hole, the issue is more complicated because, although the fault is localized to the structure, we may not know which feeder is having the problem, and entry to the manhole for a full inspection of the feeders is not possible for safety reasons. In these cases, having a feeder relay that trips or alarm for such events would be beneficial. In cases such as this that have occurred to date, the feeder with the half-cycle event has failed before any other actions were required. The eventual fault is correlated with the half-cycle fault by phase, approximate magnitude of neutral current, and the fact the half-cycle events cease.

## 3. Fundamentals of Incipient Faults in Cables

Incipient faults are leading indicators of deteriorating insulation. The aging process of the cable insulating material can be caused by a number of factors, including thermal, electrical, mechanical, and environmental/chemical factors. These mechanisms are relatively well understood. Reference [1] provides good background information. In [1] the aging factors for cables are classified as summarized in Table 1.

Most commonly, electrical stress is the predominant factor in causing cable failures. A typical failure mechanism is a partial discharge and treeing. The former mechanism takes place in organic dielectrics such as in the cross-linked polyethylene (XLPE) cables. The latter mechanism is typical in oil/paper-insulated cables and is aggravated by the presence of moisture.

Aging Factor		Aging Mechanism
Thermal	High temperature and temperature cycling	<ul style="list-style-type: none"> <li>• Chemical reaction</li> <li>• Thermal expansion</li> <li>• Diffusion</li> <li>• Insulation melting</li> <li>• Anneal locked-in mechanical stresses</li> </ul>
	Low temperature	<ul style="list-style-type: none"> <li>• Cracking</li> <li>• Thermal contraction</li> </ul>
Electrical	Voltage	<ul style="list-style-type: none"> <li>• Partial discharges</li> <li>• Electrical trees</li> <li>• Water trees</li> <li>• Charge injection</li> <li>• Intrinsic breakdown</li> <li>• Dielectric losses and capacitance</li> </ul>
	Current	<ul style="list-style-type: none"> <li>• Overheating</li> </ul>
Mechanical	Cyclic bending, vibration, fatigue, tensile, compressive and shear stress	<ul style="list-style-type: none"> <li>• Yielding of materials</li> <li>• Cracking</li> <li>• Rupture</li> </ul>
Environmental	Water, humidity, contamination, liquids, gases	<ul style="list-style-type: none"> <li>• Electrical tracking</li> <li>• Water treeing</li> <li>• Corrosion</li> <li>• Dielectric losses and capacitance</li> </ul>
	Radiation	<ul style="list-style-type: none"> <li>• Accelerated chemical reactions</li> </ul>

**Table 1.**  
Cable aging [1]

This pre-breakdown phenomenon takes place in the form of either electrical trees or water trees [1]. The cause of treeing in dry dielectrics is partial discharges due to high electric stresses (Figure 1), and moisture at lower electric stresses (Figure 2).

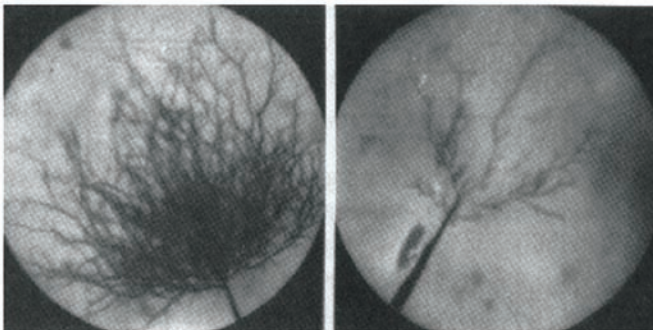
### 3.1 Electrical trees

The presence of high and divergent electric stresses is the primary contributing factor to initiate and propagate electrical trees [1]. An electrical tree may consist of many discharge paths including a “trunk” and “branches.”

Electrical trees initiate at about 150kV/mm field strength. When initiated, an electrical tree will propagate through the insulation as a series of random bursts, and when the branches of the tree span the entire insulator layer, a breakdown occurs.

### 3.2 Water trees

Water trees are caused in the presence of moisture typically at the semiconductor-insulation interface of a cable. Water trees typically start at lower electric fields and propagate slower compared with electric trees [1].



**Figure 1.**  
Sample electrical trees [1]



**Figure 2.**  
Sample water trees [1]

Water trees convert to electrical trees and result in a catastrophic failure. Typically the conversion is associated with a sustained discharge activity in cavities that are created in the water tree

channels. Large water trees can convert at normal operating voltages, and small water trees convert at higher voltage levels during over-voltages caused by switching transients or lightning. As the discharge takes place in the water cavities, only water trees are not associated with detectable partial discharge patterns before converting to the electrical trees.

Water trees convert to electrical trees and result in a catastrophic failure. Typically the conversion is associated with a sustained discharge activity in cavities that are created in the water tree channels. Large water trees can convert at normal operating voltages, and small water trees convert at higher voltage levels during over-voltages caused by switching transients or lightning. As the discharge takes place in the water cavities, only water trees are not associated with detectable partial discharge patterns before converting to the electrical trees.

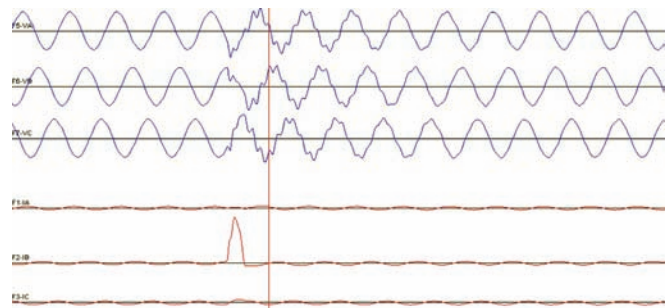
### 3.3 Incipient faults

The process of converting a water tree into an electrical tree through a localized partial discharge is relatively complicated and can occur at various rates, including temporary regression of the degradation process due to evaporation of the moisture.

During such period of partial discharge high frequency components are present in the currents. The frequency spectrum spans into few or few tens of kHz, and the nature of such current spikes is random. This situation can last days or months or even years. This paper is not concerned with detecting incipient faults at this stage.

Eventually when the insulating layer is broken, a high fault current of a fundamental frequency is created. However, at this stage considerable damage is done to the cable, and the phenomenon will repeat at an accelerated rate leading very quickly to a permanent fault.

Figure 3 shows an example of an incipient fault. The phase B current is affected showing a typical half-cycle fault pattern. When the current is self-extinguished considerable transients are created in voltages due to interactions between the cables inductances and capacitance.



**Figure 3.**  
Sample incipient fault: voltages (top) and currents (bottom).

## 4. Tripping of Incipient Faults in Cables

### 4.1 Fundamentals

This section describes a method for detecting incipient cable faults based on signals available to a feeder protective relay.

The algorithm is a heuristic pattern recognition function defining an incipient cable fault as the following event (compare with Figure 3):

- no load change occurs during an incipient fault; pre- and post-event currents are virtually identical, otherwise the event might be an external fault cleared very fast by a fuse
- an incipient fault occurs in one phase only; the superimposed fault current in one of the phases matches, therefore, the neutral current
- an incipient fault lasts for few multiples of a half cycle; a limit of 3 half-cycles is applied (vast majority of incipient faults are half-cycle events, and if lasting more than three half-cycle the incipient faults are detectable by traditional protection functions)

The above pattern is analyzed independently in each phase.

The algorithm described in this section processes samples of currents and half-cycle measurements to detect an incipient fault. This fine temporal resolution is necessary because of the short-lived nature of the incipient fault current. Processing filtered currents and their magnitudes estimated with full-cycle windows or longer would not be appropriate.

The basic algorithm detects a single incipient fault pattern based on the current. This is complemented by the following supplementary functionality:

- An overcurrent pickup setting is provided
- A pickup operand is provided to flag a single occurrence of an incipient fault and can be used with counters and logic in customized user applications
- Two hard-coded operating (tripping) modes are provided: trip on  $N$ -th count of the event ( $N$  is a setting) and, trip on the  $N$ -th count occurring in a time window  $T$  (both  $N$  and  $T$  are settings)

In theory more security can be brought into the algorithm by monitoring the voltage signal and specific patterns in it. This algorithm does not use voltages in order to expand its applicability to relays with no voltage measurements. The required security is ensured by monitoring certain features in the current signals.

Also, the algorithm is non-directional and will respond to a fault in either direction. This needs to be considered by operating the network in a loop configuration.

### 4.2 Algorithm

#### Signals and constants

$i_A, i_B, i_C$	instantaneous values of the current in phases A, B and C; in per unit of CT nominal; raw samples;
$i_N$	instantaneous values of the neutral current calculated from raw samples of currents in phases A, B and C;
$i_{FA}, i_{FB}, i_{FC}$	fault components of the current in phases A, B and C calculated from raw samples of currents in phases A, B and C;
$S_A, S_B, S_C$	measures of match between the fault currents in phases A, B and C, and the neutral current;
$I_{FA\_MAG}$	magnitude of the superimposed current in phase A (similar for B and C); estimated with the half-cycle Fourier;
$I_{1MAG}$	magnitude of the positive-sequence current;
$\Delta_{OC}$	pickup level of the overcurrent detector in per unit of CT nominal (user setting);
$N_1$	number of samples per power cycle ( $64s/c$ );
$N_M$	length of the memory operation separating the fault and load components;
$C_1 - C_4$	factory constants;

**Figure 2.**  
Substation Network Boundaries

### Calculations

The neutral current is calculated first as:

$$i_{N(k)} = i_{A(k)} + i_{B(k)} + i_{C(k)} \quad (1)$$

In equation (1) and below,  $k$  stands for a sample index and means a present sample, while  $k - 1$  means the previous sample, and so on.

Incremental (superimposed) current components are calculated next in order to separate the load and fault currents. This is done on samples using a 2-cycle memory:

$$i_{FA(k)} = i_{A(k)} - i_{A(k-N_M)} \quad (2a)$$

$$i_{FB(k)} = i_{B(k)} - i_{B(k-N_M)} \quad (2b)$$

$$i_{FC(k)} = i_{C(k)} - i_{C(k-N_M)} \quad (2c)$$

Under steady state conditions, even with distorted waveforms, the fault components are very small, ideally zero. During faults and other switching events, the above signals will reflect the fault component in the first two cycles of the fault.

During incipient faults the neutral current and the fault component in the affected phase match. Therefore a measure of that match is calculated as follows:

$$S_{A(k)} = \frac{2}{N_1} \cdot \sum_{j=0}^{\frac{N_1-1}{2}} |i_{FA(k-j)} - i_{N(k-j)}| \quad (3a)$$

$$S_{B(k)} = \frac{2}{N_1} \cdot \sum_{j=0}^{\frac{N_1-1}{2}} |i_{FB(k-j)} - i_{N(k-j)}| \quad (3b)$$

$$S_{C(k)} = \frac{2}{N_1} \cdot \sum_{j=0}^{\frac{N_1-1}{2}} |i_{FC(k-j)} - i_{N(k-j)}| \quad (3c)$$

Next, a half-cycle Fourier algorithm is run on the fault current samples:

$$i_{FA(k)} \rightarrow I_{FA\_MAG(p)} \quad (4a)$$

$$i_{FB(k)} \rightarrow I_{FB\_MAG(p)} \quad (4b)$$

$$i_{FC(k)} \rightarrow I_{FC\_MAG(p)} \quad (4c)$$

In equations (4) and below,  $p$  stands for a protection processing instant, while  $p - 1$  means the previous processing instant, and so on.

It is assumed that the magnitude is scaled as the peak value.

Overcurrent conditions are declared based on the following flags:

$$OC_{A(p)} = (I_{FA\_MAG(p)} > \sqrt{2} \cdot \Delta_{OC}) \quad (5a)$$

$$OC_{B(p)} = (I_{FB\_MAG(p)} > \sqrt{2} \cdot \Delta_{OC}) \quad (5b)$$

$$OC_{C(p)} = (I_{FC\_MAG(p)} > \sqrt{2} \cdot \Delta_{OC}) \quad (5c)$$

A match between phase fault currents and the neutral current is established via the following flags:

$$R_{A(p)} = (S_{A(p)} < \max(C_1 \cdot I_{FA(p)}, C_2)) \quad (6a)$$

$$R_{B(p)} = (S_{B(p)} < \max(C_1 \cdot I_{FB(p)}, C_2)) \quad (6b)$$

$$R_{C(p)} = (S_{C(p)} < \max(C_1 \cdot I_{FC(p)}, C_2)) \quad (6c)$$

Next, the following flags are established:

$$E_{A(p)} = OC_{A(p)} \& R_{A(p)} \& \text{not}(OC_{B(p)} \text{ or } OC_{C(p)} \text{ or } R_{B(p)} \text{ or } R_{C(p)}) \quad (7a)$$

$$E_{B(p)} = OC_{B(p)} \& R_{B(p)} \& \text{not}(OC_{A(p)} \text{ or } OC_{C(p)} \text{ or } R_{A(p)} \text{ or } R_{C(p)}) \quad (7b)$$

$$E_{C(p)} = OC_{C(p)} \& R_{C(p)} \& \text{not}(OC_{A(p)} \text{ or } OC_{B(p)} \text{ or } R_{A(p)} \text{ or } R_{B(p)}) \quad (7c)$$

During incipient faults one of the above flags will pickup for a short period of time, depending on the magnitude of the current and duration of the fault.

The last step is to check the lack of loss of load in order to distinguish incipient faults from load changes or external faults.

Upon a rising edge of the  $E$  flag defined as:

$$E_{(p)} = E_{A(p)} \text{ or } E_{B(p)} \text{ or } E_{C(p)} \quad (8)$$

the following operations are performed:

- Magnitude of a pre-fault positive-sequence current is captured: . This value is a 2-cycle old value preceding the rising edge of the  $E$  flag.
- Magnitude of the post-fault positive-sequence current is captured: . This value is a value that occurs 4 cycles after the rising edge of the  $E$  flag.

Consistent load is declared if the two values differ less than certain portion of the pre-fault current and the CT nominal current:

$$L = (|I_{1PRE} - I_{1POST}| < \max(C_3 \cdot \max(I_{1PRE}, I_{1POST}), C_4)) \quad (9)$$

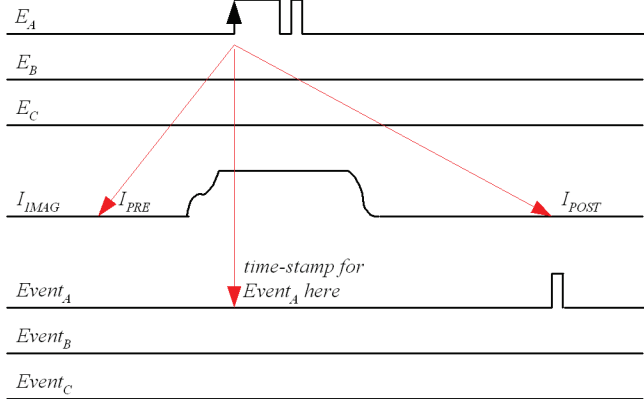
The final event flags are supervised with the consistent load condition as follows:

$$Event_A = E_A \& L \& \text{not}(OC_{A(at\ post-fault)}) \quad (10a)$$

$$Event_B = E_B \& L \& \text{not}(OC_{B(at\ post-fault)}) \quad (10b)$$

$$Event_C = E_C \& L \& \text{not}(OC_{C(at\ post-fault)}) \quad (10c)$$

Figure 4 explains the timing relationship between the event flags and the pre- and post-fault currents.



**Figure 4.**  
Explanation of capture and application of the pre- and post-fault load check

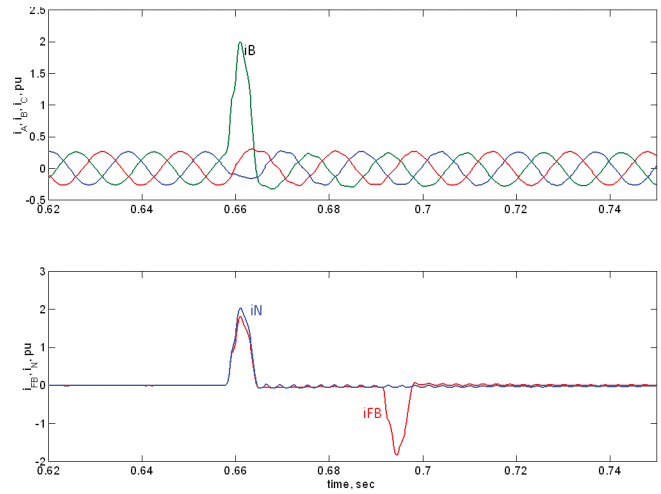
### 4.3 Illustration of the algorithm operation

Figure 5 shows a case of an incipient phase-B fault registered by a feeder relay (top Figure shows the raw A, B and C currents). The bottom portion shows the neutral current (blue) clearly revealing the fault period from under the load, and the superimposed phase B current (red). The superimposed current shows the fault current blip twice as the data slides through the 2-cycle memory window. During the actual fault, the neutral current and the superimposed phase B currents match very well, confirming the incipient fault hypothesis and identifying the affected phase.

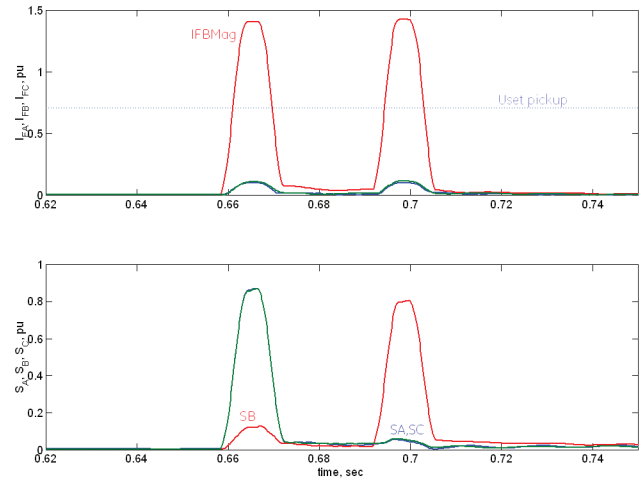
Figure 6 shows the magnitude of the superimposed currents. Due to half-cycle measurement, the fault current is estimated accurately (full cycle algorithm would see half of the current that last that short). The Figure shows a user pickup threshold set at 0.5pu RMS. The bottom portion of the Figure shows the S-values. During the actual fault the B-phase value is low indicating a good match between the neutral and phase B current. During the mirror spike in the B-phase, the neutral and B-currents do not match, which will prevent misidentification of this event as a fault.

Figure 7 shows key logic flags of the algorithm. The neutral current is shown to signify the time of actual event. The E-flag is asserted shortly afterwards and stays robustly picked up. The OC-flags behave as expected: only the B-phase seen and overcurrent condition. Two pulses are visible: one for the actual event and the other for the mirror image due to the windowing effect. The match flags (R) are picked up during steady state conditions and reset during transients if the neutral and incremental phase currents do not match.

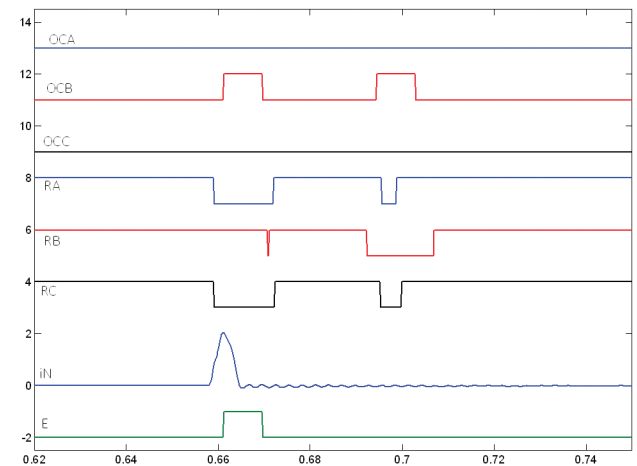
Figure 8 illustrates the measurement and capture of the positive-sequence current magnitude for the load consistency check.



**Figure 5.**  
Illustration of the algorithm: phase currents (top), calculated neutral and superimposed phase B current (bottom)

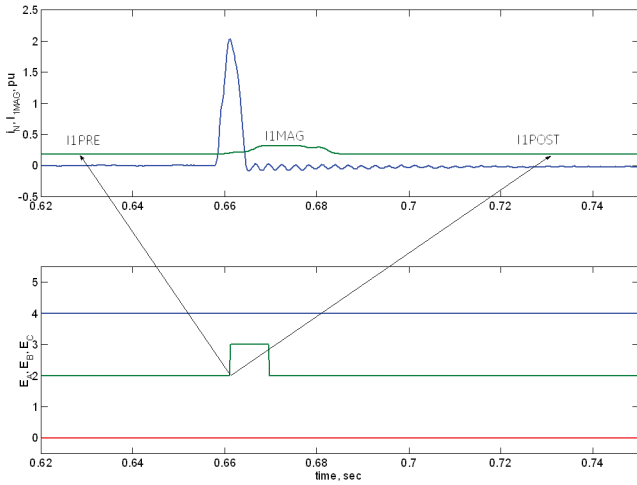


**Figure 6.**  
Illustration of the algorithm: fault magnitudes (top) and S-values (bottom)



**Figure 7.**  
Illustration of the algorithm: major logic flags





**Figure 8.**  
Illustration of the algorithm: positive-sequence magnitude and the pre- and post-fault current points

#### 4.4 Testing recommendations

Simplified test waveforms for positive testing can be created by superimposing a three-phase balanced load current and an incipient fault current ("blip"). The fault current should be combined as a series of 1, 2, or 3 half-cycle waveforms (cosine shapes). The magnitude of the fault component can be varied to test the overcurrent pickup. Figure 9 below illustrates the idea.

Simplified test waveforms for negative testing shall include regular faults (both inception and removal), and other cases that violate definition of the incipient fault as stated in clause 4.1. This includes load pickup and dropout, open phase conditions (down conductor), single-phase load and phase unbalance, etc.

#### 4.5 Operation using transformer currents

The method can be used with the total current supplied from the transformer toward the distribution bus. By subtracting the load current the method retains its sensitivity even though the load current may be significant as compared with the fault current. Of course, when supplied with the total current, the method loses selectivity and may be used for alarming rather than tripping.

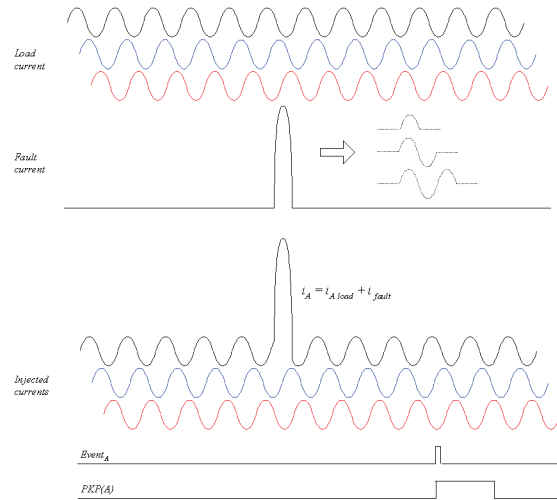
The method cannot be directly applied to the high-side transformer currents. For a wye/delta transformer, it is not possible to reconstruct the zero-sequence current on the low-side wye winding from the high-side delta winding currents. Therefore, measuring the high-side delta currents a relay is not able to calculate the true values of the low-side phase currents. However, both the positive- and negative-sequence components on the low-side can be reproduced from the high-side currents, and an expanded method is possible to detect the short lasting incipient faults in the low-side from the currents captured on the high-side of the transformer.

## 5. Field and Test Examples

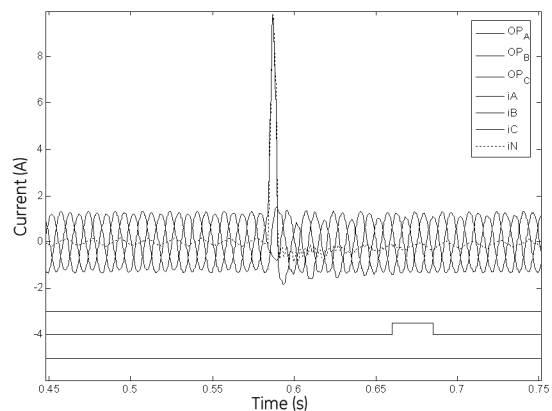
Figure 10 presents result of a playback of a sample incipient fault cases recorded by a feeder relay. The event is successfully detected after few cycles of delay in the algorithm provisioned for checking the load change.

Figure 11 presents a sample test case from a real time digital simulator. The incipient fault function was set to operate on the second occurrence of the fault within a pre-defined time window. The element picks up on both incipient faults and operates, as configured, on the second instance. This application can be used to ride through a single incipient fault but operate if the trouble is progressing. The PKP operand may be used for alarming, and the OP operand – for tripping.

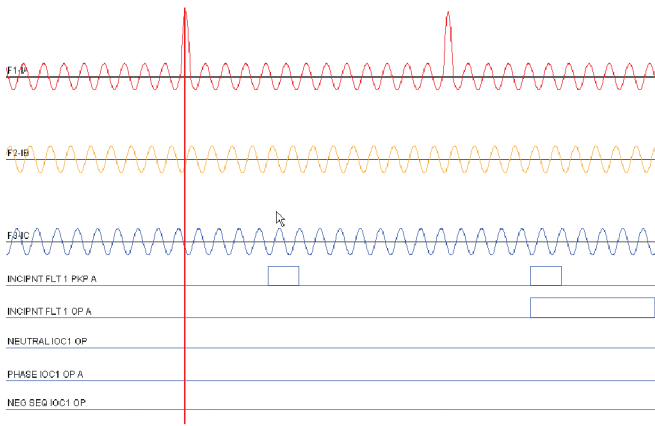
Figure 12 illustrates a case of an incipient fault with the magnitude of 3.1pu RMS and duration of one full cycle. The phase IOC function is set at 3.0pu, the neutral IOC function is set at 1.5pu, and the negative-sequence IOC is set at 0.5pu. All three elements are used as instantaneous. Depending on the magnitude of the incipient cable fault, it may or may not be detected by conventional protection elements. In this case, the neutral IOC function operates in addition to the dedicated incipient fault detection function.



**Figure 9.**  
Illustration of a simplified positive test of the algorithm

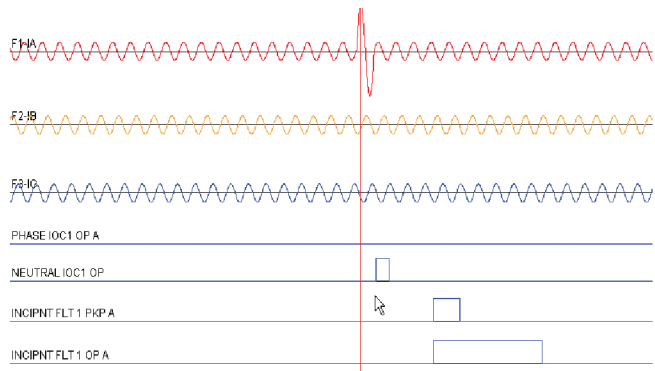


**Figure 10.**  
Illustration of a simplified positive test of the algorithm

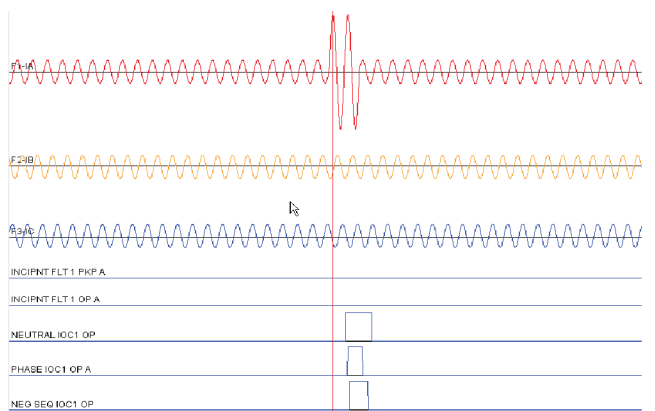


**Figure 11.**  
Operation example of the incipient fault element configured to trip in the second incipient fault

For comparison, Figure 13 shows a case of a fault lasting two cycles. This fault is seen by traditional protection but not by the dedicated incipient fault element. The latter does not respond by design as the event lasts longer than three half-cycles and is very unlikely to be an incipient fault.



**Figure 12.**  
Example of a one-cycle incipient fault detected by the incipient fault function and some traditional short circuit protection functions



**Figure 13.**  
Example of a two-cycle fault detected by the traditional short circuit protection functions, and not signaled (correctly) by the incipient fault detector

When testing the incipient fault function it is recommended to apply cases of traditional (permanent) faults, unequal pole closing/opening, external ground faults including very fast clearing via fuses, capacitor bank switching, transformer energization and similar events that may cause patterns of elevated current lasting between half a cycle and few cycles.

## 6. Application Guidelines for Tripping Incipient Cable Faults

The issues that come into the decision to deploy the logic in the first place is how often does the phenomena occur before each genuine fault. As discussed previously, it is estimated that approximately 10% to 15% of faults on the underground system that operate traditional relaying are preceded by at least one half-cycle event.

So, even with full deployment of this system, there will be no impact on the arc flash energy for 85 to 90% of all faults. That being said, there is some evidence to suggest that the number of half-cycle events is on the increase and this may be because they are more prevalent in the newer mechanical type joints that are making up an increasing percentage of the system.

Having decided to implement the logic, the decision really comes down to whether to alarm or to trip. If deciding to trip, the decision comes down to whether to trip after the detection of the first half-cycle event or whether to wait until two or three events occur (possibly even in a certain time period). What influences this decision is the number of events that are typically seen before the full fault and the time difference between the first event and the final fault.

The first issue to consider is that on a fully underground system, where there are no downstream HV switching devices (breakers, fuses) to co-ordinate with, if a half-cycle event has occurred, then the cable will almost certainly fail leading to a fault that will operate traditional overcurrent elements.

The problem faced by the relay engineer is really one caused by the fact he now has a choice as to whether to trip the breaker or wait until the full fault.

Ideally, if one has communication with the relay then one might be more inclined to trip at periods of low load or low system risk, and more inclined to see if the feeder will hold in during a summer heat wave. However, if the half-cycle event becomes more frequent with subsequent over-voltages produced by the events, the best thing for reliability purposes (to prevent damage to components on other feeders) may be to take the feeder out of service irrespective of loading and system conditions.

It needs to be recognized that the algorithm may trigger on an external fault on an unloaded or lightly loaded branch cleared fast by a fuse. Also, arrester operations may appear as half-cycle events and potentially trigger the algorithm. These must be taken into account when deploying the technology or troubleshooting field cases.

## 7. Summary

This paper presents an operational experience with incipient faults: it has been observed that 10 to 15% of cable faults are preceded by incipient faults. Practically, all incipient faults become permanent faults in the period between a few seconds to few weeks. Incipient faults occurring in fast successions create considerable over-voltages and induce faults on other feeders.

A method has been presented to detect incipient faults in a secure and reliable way. The method is secure by checking consistency of the load before and after the event, checking if the event is a single phase event, and checking for duration and consistency between the superimposed fault component and the ground current.

The presented method has been implemented [2] and tested using recorded field cases and on a digital simulator. Simplified variants of the method can be implemented by using programmability and flexibility of modern microprocessor based relays.

Recommendations are given as to the trip vs alarm applications of the incipient cable fault detection functions. In many cases tripping on the first incipient fault is a prudent application.

## 8. References

- [1] N.H.Malik, A.A.Al-Arainy, M.I.Qureshi, Electrical Insulation in Power Systems, Marcel Dekker, 1998.
- [2] F60 Feeder Management Relay, Instruction Manual, General Electric. Available at [www.multilin.com](http://www.multilin.com)

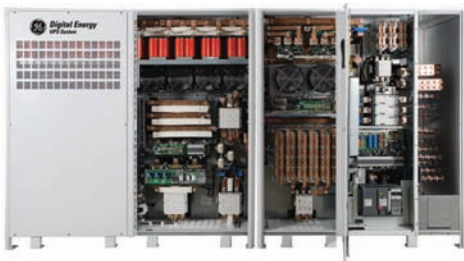
# Aim for Savings & Energy Efficiency

Do you know how much energy your mission critical facility loses each year?

Your current UPS may not be efficiently utilizing the power you are purchasing. GE Power Quality has solved this problem with the introduction of the Digital Energy™ SG Series 750kVA UPS for data center and mission critical facilities, an extension of our best in class SG Series UPS platform. One of the most efficient and reliable double conversion UPS systems available today, the 750kVA UPS builds upon GE's proven SG Series product technology to stop your energy investment from leaving the building.

The SG Series 750kVA UPS hits the target.

- > Energy Savings – maximum efficiency greater than 94%
- > Installed Savings – smaller footprint & lower weight
- > High Reliability – high MTBF and no single point of failure



Highly efficient 750kVA UPS



Digital Energy  
Power Quality



# Using 6-Sigma Methodology to Review System Security

Bruce Barnett  
GE Global Research

## 1. Summary

This paper discusses a methodology to apply 6-Sigma techniques as part of a security audit of a complete system for the purpose of threat assessment. A flow-down process is used to make sure all of the threats are considered. Then a modified FMEA is used to prioritize threats.

## 2. Introduction

Performing a security review/audit of a complex system is difficult. Several factors cause this. Some of these include:

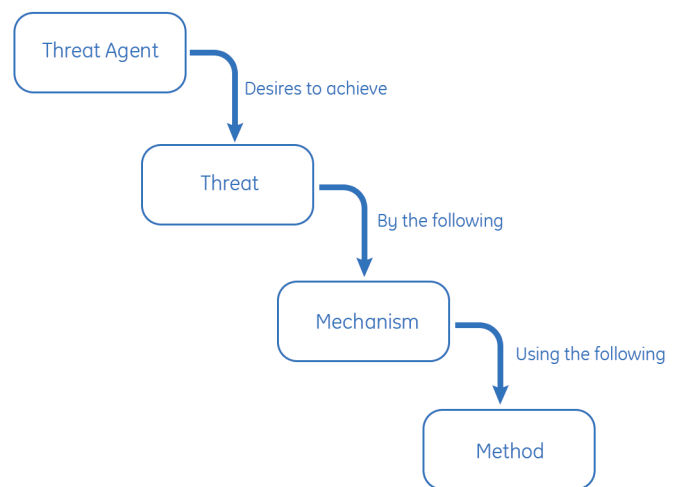
- Each system is different, and complex
- Each system has different requirements, different risks, and different priorities. What may be a major risk for one system may be insignificant in another system
- Security audit requires domain expertise, and no one person is an expert in all domain categories (encryption, protocols, system, physical, tamper protection, encryption, legal, and network interfaces)
- Audits are often performed using a checklist of items to examine. However, these checklists can never be comprehensive, because of the complexity of each system. Some items may generally be ranked "High Important" but the ranking may not reflect the true nature of the system. These checklists often encourage people to fix/buy solutions that may not address the real issues
- There is no way to determine the vulnerability of the total system

The last point is key. Without a measurement for overall threat protection, it becomes difficult to address the most severe threats. 6-Sigma methodology requires system architects to Design, Measure, Analyze, Improve, and Control (DMAIC) total system security. This paper describes one methodology that can be used to do this.

To accomplish this, we need a model than can be generalized for any threat.

## 3. Threat-based Unified Object Model

Our model is loosely based on the Common Criteria Object Model:<sup>[1]</sup>



Each of these categories refers to an object class, but in this case we use it as a step in the methodology. Individual examples in each class are called instances. The different classes are

- Threat Agents– The attacker or person or organization that wishes to accomplish a threat
- Threat – The desired goal of the attacker
- Mechanism – How the attacker will achieve the threat
- Method - The explicit sequence used to accomplish the threat

I will now describe each of these in more detail.

The first step was a QFD process modified for risk analysis. Instead of using a requirement process flow down, we used risk flow down model, as described below.

This is essentially an exercise in brainstorming, and as in all brainstorming sessions, suggestions made should be captured and considered. As the process is completed, the relative dangers will be determined. One of the goals of this exercise is to encourage the capture of unlikely events with catastrophic results.

### 3.1 Threat agent

We first generated a list of Threat Agents – which describes a class of attacker, along with the motivation and resources of the attacker. By considering these points, specific threats can be identified for each threat agent. The following categories were identified:

- Competitor
- Customer
- Countries motivated to develop competitive devices
- Terrorist organization
- Foreign Government
- Hacker interested in the challenge
- Activist (Environmental, political, social, etc.) motivated to expose activities that promote their agenda
- Disgruntled employee
- Publicity seeker

The goal is to have a comprehensive list of Threat Agents from which the system must defend itself.

Step 1: List all Threat Agents

### 3.2 Threat

Once a list of Threat Agents is obtained, each one can be considered, and all threats the agent wishes to accomplish can be listed next. It may be useful to use a grid layout, and place the Threat Agents on one axis, and the Threats on the other axis. Some threats may correspond to one or more Threat Agents.

The Threat Agents have different motivations, resources, and goals, and willingness to take risks. For instance, a competitor may wish to generate publicity that puts the system in a bad light using misinformation, while stealing the technology using an insider.

It is useful to consider threats or attacks of each security category. Stallings<sup>[2]</sup> suggests the different categories of attacks are:

- Interruption – The asset of a system becomes unavailable, destroyed or unusable. This is an attack on the asset's availability
- Interception – Unauthorized attack on the asset's confidentiality. The information isn't changed. Another variation is gathering information about the traffic, without knowing the contents of the data, by using traffic analysis
- Modification – The attacker is able to modify existing information, so this is an attack on the asset's integrity
- Fabrication – An unauthorized party is able to create counterfeit objects. This is an attack on the asset's authenticity

Attacks can be active or passive. Passive attacks do not change the behavior or contents of the system. Two categories include release of message contents and traffic analysis. Active attacks include masquerade, replay, message modification and Denial of Service.

Attacks affect the security services. These services are:

- Confidentiality – protecting the contents and characteristics of the data
- Authentication – Assuring the data is authentic
- Integrity – Assuring the data has not been modified
- Non-repudiation – Preventing someone from denying that a transmitted message occurs
- Access Control – Protecting access to the system
- Availability – Ensuring the availability of the system

To ensure that as complete a list of threats as possible is obtained, someone must consider the role of the Threat Agent, and consider what attacks can be made in each of these above categories. Other taxonomy classifications can be used, as long the classification system used covers all of the attack classes. Using multiple taxonomy systems may in fact uncover vulnerabilities that a single model missed.

Example threats that affect a business model include:

- Get options/upgrades/service/Intellectual Property without paying for it
- Allow others to obtain unauthorized services
- Damage company's reputation by exposing flaw with system
- Preventing customers from using company's service
- Distorting facts (repudiation, deleting log files), and placing liability on company
- Holding company liable for security failure, or privacy violation
- Cause company's system to interfere another system
- Terrorist Attack

This is often a useful exercise, because the focus is on ways for a complete system to fail. The more experts involved at this step, the more complete this list will be. Experts both in security and the business model are needed.

Step 2: For Each Threat Agent, List all Threats

### 3.3 Mechanism

By examining each of the threats, we then conceive of ways to accomplish these threats. Again, a grid layout may be useful. Some of the possible mechanisms include:

- Fabricate or modify data between company's system and customer's system
- Cause customer to lose money
- Bypassing security/protection mechanism
- Internal algorithms and all encryption keys are made public domain
- Develop copy of company's product, causing company to lose market share
- Allow competitor's product to integrate to company's product in unauthorized fashion
- Damage infrastructure of company

Step 3: For Each Threat, List all Mechanisms that allows threat to occur

### 3.4 Methods

For each of the mechanism, there is one or more methods that can be used to accomplish the mechanism. The grid layout may again be helpful here. Examples include:

- Brute Force attack on secret key(s)
- Insider reveals algorithm and keys from backup tape, discarded media, etc.
- Reverse engineer of system using physical attack
- Replay of data between two systems.
- Obtaining confidential information by bribery and/or extortion

In some cases, the Method and mechanism may be the same. What is important is that the method should be detailed enough that it can either be detected, or a countermeasure applied.

Step 4: For Each Mechanism list each possible Method

### 3.5 Scope

It is useful to have a complete list of possible threats methods. Realistically, some methods can be set aside temporarily, and addressed at a later date – if at all. As Bruce Schneier says, "Security is a process, not a product."<sup>[3]</sup> The motivations of Threat Agents are dynamic. Risks must be periodically re-evaluated.

Step 5: Prioritize Threat agents to address primary threats

### 3.6 Developing suitable scorecards

In order to rank risks, a scorecard must be developed for the Failure Mode Effects Analysis (FMEA) can be obtained. This paper uses three different measurements:

- Severity – how much damage can occur?
- Likelihood – how likely is it to happen?
- Detectability – If it does happen, can you detect it happened afterwards?

Likelihood indicates the theoretical chances of an attack, not the actual measured value of an attack.

One might say that a system with a response to an alarm reduces the likelihood. However, one should consider detectability and likelihood as independent values for the purposes of this methodology. Responses are covered later.

Each of these measurements has values that range from 1 to 10, with 10 being the worst. The appendix lists three tables that are a useful starting point reference.

The group should reach consensus on the values and meanings of each of these values. It is useful to be specific about the severity of a system failure, as different systems have different examples of "worst case." A medical system's worst case may be loss of a human life. A power system example of worst case is to allow a massive power grid failure during a terrorist attack. A business may consider worst case to be a major loss of market share.

It might seem that this process is difficult, but the scores are relative, so different responses and even systems can be compared, as long as the scales are compatible.

The likelihood score that was used originally was suited for process failure. We have adapted it to be suitable for security failures. Instead of the classic one failure per 6 million units, we use a logarithmic scale of failures based on time. Therefore a score of 1 is one failure every 1000 years, while a score of 10 is a failure of several times an hour (or perhaps minute if desired).

Appendixes A, B and C give sample values.

Step 6: Determine relative values for failure modes

### 3.7 Ranking of security risks of existing architecture

The threat method for the existing (or proposed) architecture is examined. Using this scale of 1 to 10, the security review team assigns a score to each of the three measurements. Because scores are relative, and subjective, the team doesn't have to assign absolute values to each of the cells in the table. Instead, the team has to make sure the relative value assigned to one threat is comparable to other threats. That is, it might be difficult to assign a fixed severity value for a single threat. It's easier to say one threat is relatively more severe than a second threat.

A Relative Prioritization Number (RPN) is determined for each threat method, by multiplying the three values together (Likelihood \* Detectability \* Severity.) Therefore, each risk can be assigned a RPM value.

Step 7: Calculate a RPN for each risk

### 3.8 Risk prioritization

The list of risks can be prioritized, sorted by RPN value. The largest RPN corresponds to the greatest risk. The resulting table may look like this:

		Straw-Man Values			
		Likelihood	Detectability (after the fact)	Severity	RPN
Methods	Insider reveals algorithm and keys	3	5	7	105
	Copy hardware configuration	2	6	5	60
	Brute force attack against encryption keys	1	5	7	35
	Obtain system, and Reverse Engineer the code	1	5	7	35
	<b>Total</b>				<b>235</b>

Step 8: Prioritize the possible risks

Note that a rough estimate of the total system security can be obtained by the following equation:

$OAR (Overall\ Average\ Risk) = \frac{Total\ RPN\ values}{(1000 * Number\ of\ Risks\ Listed)} * 100\%$ . A more mature system will have a lower Overall Average risk.

As systems evolve over time, new (or overlooked) vulnerabilities may be added. Therefore this number is not absolute. However, given the same set of risks, this number can indicate the maturity and ability of the system to handle those specific types of risks.

### 3.9 Determining the benefits of counter-measures

Next, a newer architecture can be considered. The security of the new system(s) can be compared with the security of the old system by re-calculating the value for each Threat Method. A copy of the above table can be made for each of the architectures considered. Notice that there are three different approaches that can be used to reduce risk:

- Decrease the severity of the attack (so it doesn't do as much damage)
- Decrease the likelihood of the attack (so that it theoretically occurs left often)
- Increase the detectability of the attack (allowing you to respond to attacks more quickly)

The new architectures may have higher or lower risks. Go through the complete list of risks, enter these values, and re-calculate the RPN values based on the system modifications. A second table can be used to evaluate the proposed architecture.

Step 9: Calculate the total RPN for an alternative architecture(s)

### 3.10 Comparison of architecture

At this point, the two (or more) systems can be compared. The difference between Overall Average Risk values can be compared. In addition, the total RPN values can be compared. For example, assume the following example which shows an existing system, and a proposed new architecture:

		Current Architecture			
		Likelihood	Detectability (after the fact)	Severity	RPN
Methods	Risk 1	3	5	7	105
	Risk 2	2	6	5	60
	Risk 3	1	5	7	35
	Risk 4	1	5	7	35
	Risk 5	0	5	7	0
	<b>Total</b>				<b>235</b>
	<b>Max</b>				5000
	<b>Overall</b>				4.70%

		Proposed Architecture				Relative Improvement
		Likelihood	Detectability (after the fact)	Severity	RPN	
Methods	Risk 1	1	5	7	35	
	Risk 2	2	6	5	60	
	Risk 3	1	5	7	35	
	Risk 4	1	5	7	35	
	Risk 5	0	5	7	0	
	<b>Total</b>				<b>165</b>	<b>29.79</b>
	<b>Max</b>				5000	
	<b>Overall</b>				3.30%	

With 5 risks, the worst case is a score of 5000. The initial system had a total RPN of 235, for an overall risk of 4.7%. The proposed system reduces the likelihood of Risk 1 (from 3 to 1), which gives a total RPN of 165, or 3.3%. The relative improvement is 29.8% reduced risk – calculated by comparing the old and new RPN total values. By using this, we can compare two systems and calculate the improvement, if any, a new system has to offer.

This system provides a simple mechanism to compare one or more proposed threat reduction systems. Therefore, this leads to a way to weigh the relative benefits of various protection mechanisms.

What is important is that this system is greatly affected by the threats with the largest Relative Priority Number. In other words, it helps identify the countermeasures that offer the greatest reduction in overall risk.

Step 10: Compare different architectures



### 3.11 Scope

Total risk is not a fixed value. Many things can change the calculations. A new vulnerability may be discovered. The likelihood of an attack may change because of political or social-economic changes. Systems may be used in more critical infrastructures. Be prepared to review the overall risk of a system. If the measurement system changes, older values may have to be adapted to reflect changes.

Existing systems may have alarms and detection systems built into them. The information can be used to revise the table. For example, detection of an attack that was thought to be unlikely should cause the table to be updated.

Step 11: Revisit and Review Architecture regularly

## 4. Conclusion

This process can be used to rank overall system security, to identify the greatest risks, to prioritize risks, and to compare different security solutions. It applies 6-sigma methodology to calculate total system security.

The methodology attempts to measure overall security, and to indicate those threats that have the greatest risk.

As the ranking is relative and subjective, and not objective, consensus is easier to achieve.

Experience shows that this methodology, because of the top-down nature, can identify risks that were overlooked. In one case, where a system's protection was based on a secret key hidden in the source code, this methodology identified the greatest risk was access to a backup tape. In this case, the proposed solution was a lock on the door, so the greatest threat was addressed by the lowest-cost solution.

Experience also shows that this process can be accomplished in a few days, again indicating the practical aspect of the methodology. It also provides a practical mechanism to compare solutions, which is understandable to non-security professionals.

This methodology also lends itself to an iterative process. The motivation and resources of Threat Agents changes over time, and the values generated can be used as a dashboard display.

## 5. Summary of Steps

Step 1: List all Threat Agents

Step 2: For Each Threat Agent, List all threats

Step 3: For Each Threat, List all Mechanisms that allows threat to occur

Step 4: For Each Mechanism list each possible method

Step 5: Prioritize Threat agents to address primary threats

Step 6: Determine relative values for failure modes

Step 7: Calculate a RPN for each risk

Step 8: Prioritize the possible risks

Step 9: Calculate the total RPN for an alternative architecture(s)

Step 10: Compare different architectures

Step 11: Revisit and review architecture regularly

## 6. Appendix A - Likelihood Ranking

Probability of Security Failure	Proposed Failure Rate	Ranking
Very High: Failure is almost inevitable	Several times a day	10
	Daily	9
High: Repeated failures	Weekly	8
		7
Moderate: Occasional failures	Monthly	6
	Yearly	5
Low: Relatively few failures		4
	Once every 10 years	3
Remote: Failure is unlikely	Once every 100 Years	2
	Once every 1000 years	1

## 7. Appendix B - Severity Ranking

Effect	Proposed Severity of Effect	Ranking
Hazardous without warning	Company's Reputation permanently damaged; Unable to repair major damage; Criminal Liability; Widespread abuse; Major Loss of market share; Loss of life, loss of large contract.	10
Hazardous with warning	Widespread abuse of software and/or system. Significant loss of market share	9
Very High	Large customers moving to competitors, loss of corporate accounts; Unfavorable publicity in Media	8
High	Large customers able to use products without paying for full services;	7
Moderate	Customers find ways to eliminate need for licensing products	6
Low	Customers able to gain access to service without paying	5
Very Low	Ability to redeploy products without paying for services	4
Minor	Lose of single customer's confidential information	3
Very Minor	Sluggish usage for single customer	2
None	No effect	1

## 8. Appendix C - Severity Ranking

Detection	Likelihood of Detection by Design Control	Ranking
Absolute Uncertainty	Design control cannot detect potential cause/mechanism and subsequent failure mode	10
Very Remote	Very remote chance the design control will detect potential cause/mechanism and subsequent failure mode	9
Remote	Remote chance the design control will detect potential cause/mechanism and subsequent failure mode	8
Very Low	Very low chance the design control will detect potential cause/mechanism and subsequent failure mode	7
Low	Low chance the design control will detect potential cause/mechanism and subsequent failure mode	6
Moderate	Moderate chance the design control will detect potential cause/mechanism and subsequent failure mode	5
Moderately High	Low chance the design control will detect potential cause/mechanism and subsequent failure mode	4
High	High chance the design control will detect potential cause/mechanism and subsequent failure mode	3
Very High	Very high chance the design control will detect potential cause/mechanism and subsequent failure mode	2
Almost Certain	Design control will detect potential cause/mechanism and subsequent failure mode	1

## 8. References

- [1] Common Criteria Official Document CC v3.1/CEM v3.1 (September 2006) Part 1 – Introduction and General Model (V3.1) [http://www.niap-ccevs.org/cc-scheme/cc\\_docs/CCPART1V3.1R1.pdf](http://www.niap-ccevs.org/cc-scheme/cc_docs/CCPART1V3.1R1.pdf)
- [2] Stallings, William, "Cryptography And Network Security – Principles and Practice", Prentice Hall ISBN 0-13-869017-0
- [3] Cryptogram #5, May 15, 2000 <http://www.schneier.com/crypto-gram-0005.html>

# Security Architecture for IEC 61850-9-2

Daniel Thanos, Bogdan Kasztenny  
GE Digital Energy

## 1. Abstract

This paper explores cyber security challenges and solutions for IEC 61850 process bus. NERC CIP requirements are used as a reference point, but the paper remains universal across different geographies and jurisdictions. An optimum process bus solution is derived from the intersection between the functional requirements for an architecture carrying the process bus data, and security threats to the assets belonging to the process bus network. The presented solution provides a practical approach for achieving a high level of cyber security by eliminating or minimizing entire classes of risks. Chief among those risks are remote access points and switched/routed networks, and the opportunity they afford for illegitimate cyber access and abuse.

## 2. Introduction

IEC 61850-9-2 process bus offers many improvements to substation automation in terms of cost savings, deployment time, skill-set requirements, personnel safety, and others. Obviously, eliminating copper wiring in favor of fiber optic communications without careful architecture design consideration could introduce potential cyber security risks. Whenever electronic and networked control elements are introduced to any protection and control environment, their abuse has the potential to negatively affect the security and availability of protection. Minimizing the risk of such abuse or innocent human mistakes with sound architecture ensures that the benefits of the new technology continue to be reaped without exchanging them for other problems.

Given the criticality of the application, process bus systems cannot afford to face cyber security problems.

First, high performance requirements in terms of availability of data, latency, and bandwidth would prevent or make it technically difficult and/or expensive to apply known enterprise security countermeasures used human interactive networks.

Second, extensive countermeasures call for extra workforce to deploy, maintain, and fulfill the regulatory requirements of logging and reporting. This would reduce the original gains in installation and ownership costs, as well as increase the demand on staff numbers and expertise level required to maintain the substation electronic assets.

Third, adding cyber security countermeasures to the long list of challenges that already face process bus as a concept would



slow down adoption of the technology, make interoperability more difficult to achieve, and delay large-scale deployment by years, if not decades.

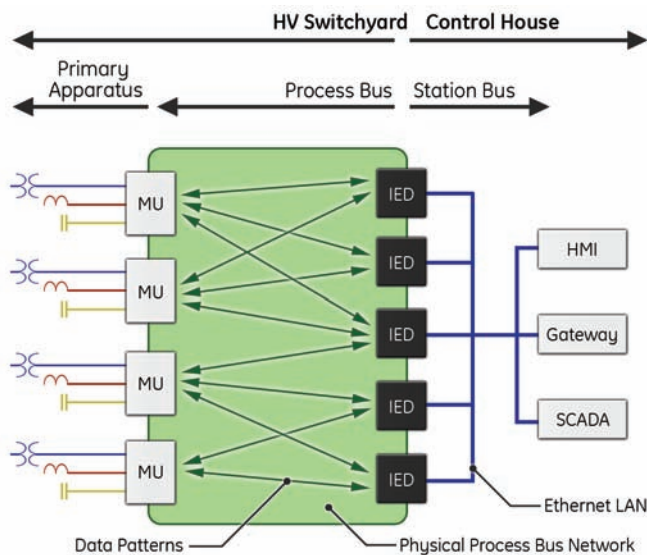
A successful process bus architecture needs to be simple and consider cyber security threats at the initial design stage, rather than offer add-ons to solve problems introduced as part of an organic development.

It is important to recognize the unique nature of the process bus network. With reference to Figure 1, a process bus is conceptualized as a physical connectivity of a sort between Merging Units (MUs) located in the primary power system switchyard and relays or Intelligent Electronic Devices (IEDs) located in the control house. Merging Units act as input-output interfaces to the primary equipment in a substation for the IEDs, which consume the data, process and act upon it, and typically provide post-processed data via a separate network to the higher order systems like SCADA and EMS.

Within the physical connectivity of the process bus network certain data path patterns exist that are determined by the fixed topology of power substations. The data paths are always well defined and

follow an overlapping and interlocked one-to-many and many-to-one pattern with a finite number of interconnections required [1]. The nature of the data paths is fundamentally different from a generic Ethernet LAN, where a potentially variable number of devices may establish any arbitrary set of interconnections, and therefore flexibility in the network topology is required.

Another important characteristic of the process bus network is that it is static as it reflects the topology of the underlying power substation. As such it is not meant to change unless the station topology itself changes due to additions or reconfigurations of the primary power apparatus. Normally, there is no need for human access to this static network except for local on-site maintenance of the physical components.



**Figure 1.**  
*Generic process bus concept*

The process bus level may be seen as an area of increased interest for cyber attacks. The process bus network is the layer closest to the primary equipment, potentially granting the most powerful, direct and unsupervised control access to the primary apparatus. IEDs may incorporate various interlocking schemes that would have to be defeated to do harm, or may implement simple supervisory functions external to the relay using analog devices with no communication capabilities. A process bus network is intended to carry raw data, which if altered, could cause harm because there is no other layer to stop the malicious activities. Any proposed process bus solution needs to address cyber security requirements during the initial design stage, in a manner that is practical for utility operators while not introducing new problems that would have to be addressed and managed.

The principal problems to address include ensuring that process bus data streams meet requirements for low-latency and high-speed communication while not being subject to tamper and disruption through illegitimate cyber access.

Not to be forgotten is the issue of management complexity as it can lead to security risks because of mis-configuration and human errors.

It should be noted, however, that these problems could have conflicting solutions. For example if the substation lacks proper access controls (Non-constrained and non-monitored access by personnel or individuals) and the process bus network is complex (many different device types), shared (different and concurrent application communications), and has few electronic boundaries (accessible with no/weak access controls), then providing security through encryption is required, due to the complete lack of a trusted environment. Process bus network encryption would likely produce unmanageable issues of latency, performance, and operational risk. Thus an optimal solution would provide strong security by first building a trusted environment without introducing unnecessary complexity.

There are many different types of network architectures that in theory can be used for communications between merging units and IEDs and they each have their own security and robustness properties. Those networks can include Point-to-Point (P-to-P), switched, routed and indeed they can be mixed in many solution implementations.

In general, there are functional advantages as one moves from the simplest network type (P-to-P) to the more sophisticated architectures that would include switching, routing and outside remote access. The increases in functionality and complexity would require countermeasures to provide security. A secure and robust process bus implementation does not require complex, highly flexible network architectures and should thus build its security through simple and mission focused design.

### 3. NERC Critical Infrastructure Protection

#### 3.1 Compliance standards

Cyber security threats to the North American power infrastructure have necessitated the formation of standards provided by the North American Reliability Corporation (NERC). These standards are known as the Critical Infrastructure Protection (CIP) standards [2] and form an organizational framework of directives that are meant to provide high-level security requirements in process and technology. CIP-002-1 through to CIP 009-1 forms the cyber security standards framework. It is important to note that the CIP standards are not tangible technical standards as it is left to critical infrastructure owners and vendors to provide reasonable translation and implementation of them. CIP is a collection of nine standards that are meant to provide direction in eight broad domains.

The CIP standards applicable to process bus are highlighted in Table 1, and will be examined in more detail.

Standard	Title	Purpose
CIP-002-1	Critical Cyber Asset Identification	Identification, enumeration, and documentation of Critical Cyber Assets
CIP-003-1	Security Management Controls	Audit and review processes with associated management controls.
CIP-004-1	Personnel & Training	Appropriate level of personnel risk assessment, background checks, training, and security awareness.
CIP-005-1	Electronic Security	Establish electronic security perimeter with reasonable access controls
CIP-006-1	Physical Security	Intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.
CIP-007-1	Systems Security Management	Controls to Detect/Deter/Prevent Compromise.
CIP-008-1	Incident Reporting	Identification, classification, response, and reporting of Cyber Security Incidents
CIP-009-1	Recovery Plans	Ensure Critical Cyber Asset restoration in case of compromise/disaster

**Table 1.**  
Summary of CIP Standards

All the domains represented in the NERC CIP standards involve having processes in place that go beyond specific technologies and equipment and thus should be viewed as a total organizational framework within which specific vendor products operate. It is beyond the scope of a single piece of equipment to provide compliance in all of these domains as they cover issues beyond the function of a single asset. The solution to compliance is not realized as a single technological feature but sound process, management practices, and the general technical architectures that cyber assets operate under. It is within this context that the proposed process bus solution can provide its secure function.

### 3.2 Process

In general, technical architectures and asset configurations should fulfill requirements of a security profile that is derived from a risk analysis, which is in turn based on a threat model. Threat modeling is the process of identifying known threats to an infrastructure, as well as providing an assessment of capabilities and motivations. Any process bus system is a key target because of its critical nature to the process of power system protection and its direct interface with primary apparatus. A threat that interrupts or otherwise impairs the functioning of the communications between merging units and IEDs could have a catastrophic effect on the ability to protect the power system. Once protection is disabled, an attacker could be free to launch other more damaging coordinated attacks.

The risk analysis process examines each threat, its associated means, and systems that can be affected. The risk analysis defines what threats will have the biggest impact on the operation of the system and the likelihood of specific attacks occurring. The value of the risk analysis process is ranking the likelihood and impact of each threat or attack. This information is used to form a security profile. The profile mandates a level of security for each risk based on its impacts and likelihood.

The security profile examines operations and infrastructure elements (networks, devices, software, etc.) and identifies critical ones necessary for continued fulfillment of the primary mission – in the case of process bus, the ability to provide fundamental power system protection and control. It then provides for specifications (in terms of technology and process) that address how critical elements will be protected as well as what is trusted (networks, devices, people) and to what level throughout the system.

For example, within the context of a process bus network, an attacker could remotely inject false data or malicious commands to trigger breakers in multiple substation sites in a coordinated effort with the hope of causing disruption to the power grid. If the means of access is provided to them it is a highly likely the attempt will be made to execute this attack. This constitutes a high-risk event that must be addressed and defended against. Thus within the class of threats and means, access to the process bus network must be restricted or eliminated entirely.

Finally, based on the security profile, an architecture of a network and/or a total system is developed and each asset it contains is configured to meet its requirements. The high level process to implement cyber security in control networks is shown in Figure 2. This is a continuing process to account for the evolving nature of cyber security threats.



**Figure 2.**  
A generic cyber security implementation process

This section summarizes a generic framework of evaluating and maintaining cyber security. Process bus networks are different in nature from generic communications networks, but they are subject to NERC compliance. The level of compliance will have to be established, monitored and maintained for every case of deployment of a process bus network. The following section summarizes the compliance dimensions.

## 4. Security Profile and Architectural Elements

A security profile has to mitigate the highest risks to an acceptable level while not allowing security methods to introduce unacceptable operational risks. The central goal of CIP compliance and any critical infrastructure cyber security program should be to keep the power system functioning and intact. The overriding goal of the security profile is to ensure that within the limits of reasonable risk mitigation the misuse of a cyber asset cannot critically impede the power system. The elements that will be discussed are based on these goals. The following are the minimal security elements that are recommended to be in place in order to provide secure and compliant function to many types of devices and networks, including the process bus network:

- Physical Security Boundary (CIP-006-1):** A critical cyber asset is only as secure as the environment with in which it operates. As per the CIP-006-1 standard, the substation must have proper physical barriers that prevent unauthorized access. If there is no such boundary no security for the substation is possible as disruption to local power systems could occur by brute physical damage to key apparatuses and control devices.
- Physical Access Controls and Monitoring (CIP-004/6-1):** Beyond having a physical security boundary CIP-006-1 also requires controlled access to the substation and its various facilities that can be monitored, traceable and limited to specific individuals. Examples of access control can include locked and carded access, on site security guards, or biometrics. Active monitoring through video cameras with the ability to detect and respond to events is equally important. Without proper physical security any cyber security is untenable in any circumstance.
- Remote and Local Network Boundaries (CIP-005/6-1):** Just as it is important to delineate physical boundaries it is equally important to delineate electronic or network boundaries. There are two boundaries to consider, local and remote. The local network boundary consists of all networking equipment, devices, and cabling that constitutes the network within a substation, encapsulated in the physical security boundary. If there are any network links outside of the physical boundary of the substation they are to be considered remote. Any network that is not part of the local substation boundary shall be considered a remote network. CIP standards require clearly identified network boundaries with specific, controlled local and remote access points in order to be compliant and secure. See Figure 3 for a brief representation of this concept.
- Cyber Access Controls (CIP-005/7-1):** There are two types of devices that one may find in the substation network: programmable (soft-configured) and non-programmable (hard-configured). A soft-configured device can have its operation affected without requiring any physical changes. Thus if a network port is present on such devices then operation can potentially be impacted remotely. As these types of devices are of a higher risk class an access control counter measure is needed (CIP-005/7-1). A reasonable access control is any mechanism that limits access to the cyber asset to only authorized individuals and systems based on privileged information, a process, or physical control. A common example of an access control to a device might be a login and password authentication. The password would have to be known by only authorized individuals. Depending on the function of the device there could be fine grained permissions in terms of what an authorized user can configure or examine based on role or password as well as requiring secondary authentication or intervention to commit any changes. An IED with programmable functionality and active network ports would be an example of a device that requires

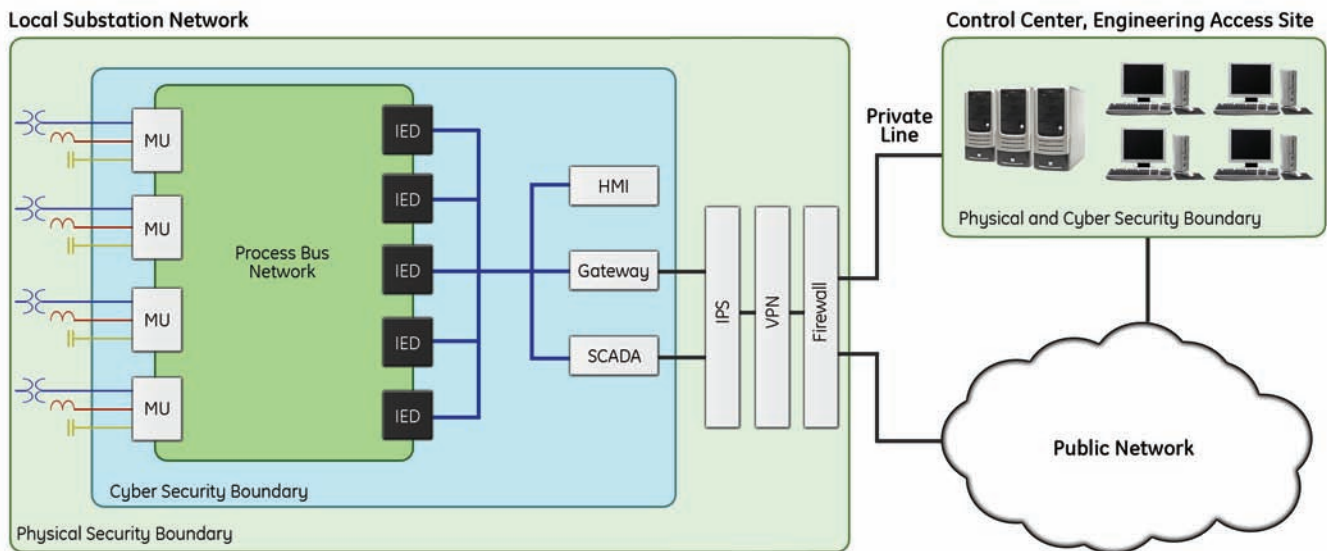


Figure 3. Substation network boundaries

these access controls. Devices that are hard configured are ones that cannot be re-programmed to change behavior, as it would require a physical change in configuration. Devices of this nature would not require access controls beyond the ones that exist by being in a secure network and physically secure environment. Any process bus solution because of its mission critical nature should make use of hard-configured devices for maximal security and robust operation.

- **Cyber Monitoring (CIP-007/8-1):** Monitoring is of great importance in any security implementation for two fundamental reasons:
  - To catch and deter many classes of attackers before greater damage can be done
  - To allow one to test the effectiveness of the security that is in place to improve it as necessary

Continuous access monitoring is required at both the network and individual device level, particularly for any user programmable devices where changes to configuration can occur without physical presence and intervention. Even for devices only accessible from within the local physical security perimeter, continuous monitoring and logging should be considered as a necessity.

Mission-focused hard-configured devices do not need cyber monitoring countermeasures as their operational behavior cannot be changed and their security is implicit by the physical nature of their environment. Again, any process bus solution should ideally be constructed of hard-configured infrastructure, to prevent remote cyber access threats, legitimate and accidental, that would otherwise require extensive monitoring with soft-configured devices.

- **Disaster Recovery (CIP-009-1):** Should there be an instance of cyber attack that causes a loss of function for a critical cyber asset or network and associated support systems, it is equally important that a plan exists for the rapid restoration of functionality. Depending on the nature of the system and types of devices, there are multiple recovery processes. It is important that a recovery plan exists that implements these processes and meets CIP standards as part of a broader organizational security program. The programmable devices in the substation network should support a broader program by providing at minimum periodic backup methods for critical device configurations. Hard-configured devices do not have files and settings that need to be backed up; it is sufficient to have their physical configuration documented in the event they need to be replaced because of damage or failure.
- **Robustness and Performance:** Any process bus network has key requirements to deliver high data rates, low latency, and determinism. A process bus solution would logically be the most mission critical element in the broader protection and control network. Maintaining these properties in a switched network topology that is shared with other substation devices and applications would be a considerable challenge and fraught with operational and cyber security risks. As mentioned earlier, network complexity (e.g. switching, routing, remote access, multiple types of devices, etc.) require burdensome cyber security countermeasures that would diminish performance and increase operational risk of the overall process bus solution. Any process bus implementation should mitigate or do away with as many of these risks as possible.

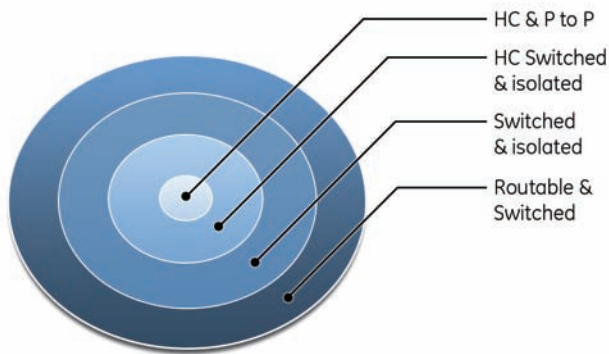
## 5. A Secure IEC 61850-9-2 Process Bus Solution

### 5.1 Attributes

Taking into account the security profile, architectural, and performance elements as discussed above, the following are the governing attributes of a practical, secure and optimal process bus solution.

- **Isolated:** A shared switched network that would also have routing and remote access poses unacceptable security and performance risks. Shared networks would allow arbitrary devices to be plugged into them as well as potentially carry other application communications that could impact the performance of the process bus. A process bus network should work isolated and therefore should be physically separated from the rest of the substation network, and only carry messaging specific to its application. One could argue that a switched and isolated network could provide that function, however a switched network must be built of active network switching devices. These switching devices require monitoring themselves, usually to a remote communications monitoring center. This monitoring requirement introduces additional, non-process bus traffic onto the network, and opens an external access issue that must be addressed and secured. Having a process bus solution implemented on an isolated point-to-point network, held to within a single physically secure perimeter, provides compliant cyber security by design and eliminates most risks.
- **Static:** The mapping of the process bus traffic between MUs and IEDs is static, and therefore the process bus network should be static as well. It is not necessary to support an arbitrary connection or reconnection of any device within the process bus system. A dedicated, point-to-point network provides for more reliable and secure operation and as the network is mission focused and isolated, security requirements can naturally be met. One should not confuse a fixed configuration of a given process bus network, with ease of scalability or expandability of the system in general.
- **Hard Configured (HC):** As presented throughout this paper, from a cyber security perspective the infrastructures that require the least amount of security and countermeasures are ones that are hard configured. When physical access is necessary to effect change in configuration the cyber security problem is simplified and solved by nature of design. This means that an occasional configuration tool should work in the point-to-point fashion with the configured cyber asset (e.g. merging unit) with the latter being disconnected from the operational process bus network. Hard configured devices also offer less operational risk by way of being less subject to error during isolation or testing.
- **Autonomous:** There should be little or no human operated devices in the network so that operational and cyber security risk is kept low. Isolated networks with hard-configured devices allow for the greatest autonomous operation.

Ensuring that all of the discussed attributes are met by a process bus solution would provide the most secure, optimal, and lowest risk operation. In terms of security and risk surface area a HC & P-to-P network architecture occupies the least amount (Figure 4).



**Figure 4.**  
Networking security and risk surface by network architecture

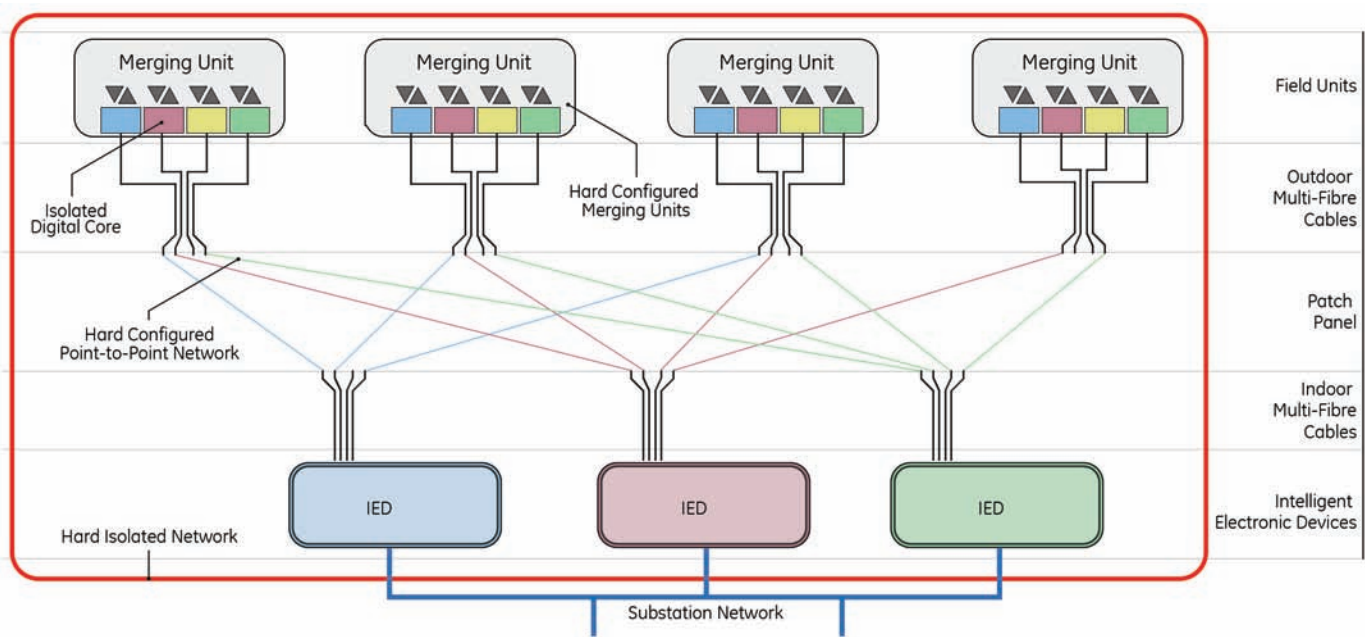
## 5.2 Optimal architecture

Taking into account the discussed attributes there is an optimal and secure process bus solution unto which one will converge. With reference to Figure 5, the optimum architecture is based on a Hard Configured and Point-to-Point network.

Under the recommended Security and Architectural elements outlined in this paper the proposed IEC 61850 process bus architecture of Figure 5 achieves compliance to CIP standards and the highest possible security and robustness by the nature of its design.

Here is some further commentary for the proposed architecture and its alignment to all the discussed security, compliance, and performance elements:

- **Hard Configured Merging Units:** As these devices cannot be programmed through any cyber access means and their configuration is based on physical presence of the configuration tool, they offer the most optimal fulfillment of CIP compliance and general robust performance requirements.
- **Hard Configured Point-to-Point Network:** In the recommend solution, merging units can only be connected to the IED using direct hardwired and closed point-to-point links and so no opportunity exists for unauthorized cyber access and configuration. The network itself is hard wired and configured. All access must be physical to change operation of the system. This provides the greatest amount of security and robust operation by nature of design. A point-to-point network is also necessary to meet process bus performance requirements in terms of data rates and latency.
- **Hard Isolated Network:** The process bus network is physically isolated from the station level/SCADA/EMS substation network. It does not have any switching or routing points and does not allow for any other communication traffic that is not part of the mission critical process bus function. Further, merging units have independent digital cores that are dedicated to specific ports and IEDs providing even more granular isolation to enhance the security and robustness of the system. The isolated nature of the solution also reduces operational risk and is necessary for the mission critical performance of process bus.



**Figure 5.**  
Optimum process bus architecture



- **Compliance:** The proposed process bus solution removes entire classes of cyber security risks. It does not require the deployment of any mentioned security countermeasures (e.g. monitoring, access controls, recovery, encryption, etc.) and reduces CIP compliance to its simplest elements. The design of the solution is optimally secure and compliant by design and nature of operation

This presented solution can currently be realized as an available product known as the HardFiber system [1,3]. HardFiber was designed under the security process and criteria outlined in this paper.

## 6. Summary

This paper has reviewed generic cyber-security requirements for a process bus-based protection and control system, using NERC CIP as a reference. A methodology of developing, monitoring and maintaining compliant networks has been discussed. General attributes and functional requirements for a process bus network have been described.

Applying the cyber security requirements to the functional process bus network, using the outlined methodology, has produced a point-to-point, hard-configured architecture as the optimal solution for process bus. This type of network is intuitively fit-for-purpose, enables robust and deterministic performance, supports scalability and substation expansions, and many other practical aspects [1].

The selected architecture also meets the requirement of simplicity of many P&C jurisdictions, mandating application of the simplest possible solution in the protection and control domain.

Instead of using an architecture that would be unnecessarily flexible, with security vulnerabilities requiring mitigation, the selected architecture is simple, avoiding the introduction of problems, rather than solving them with added complexity.

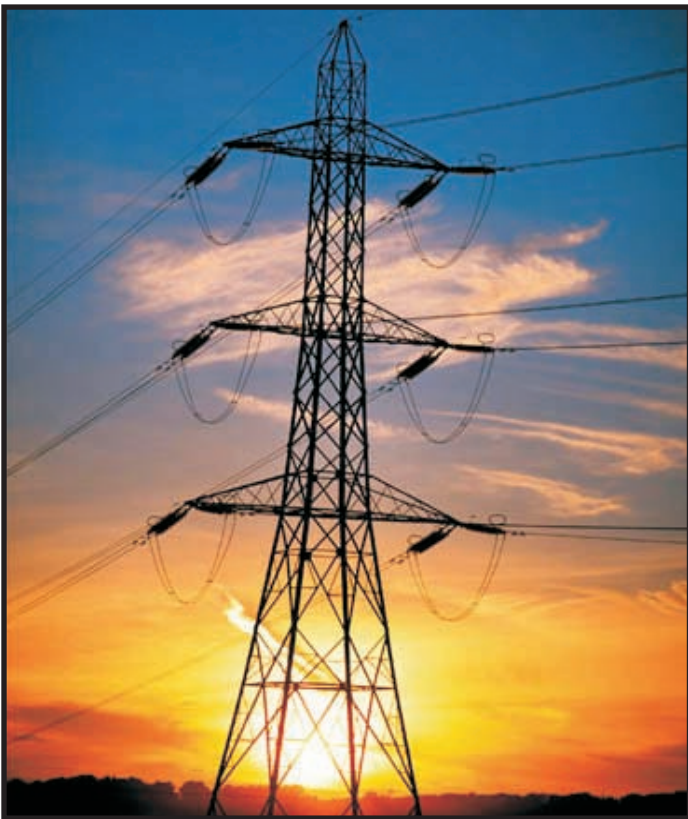
The selected architecture is inherently secure with no or minimum exposure. As such, the solution does not require the user to invest in training and resources to deploy any measures, technological or procedural, to maintain or monitor cyber security of the process bus networks.

## 6. References

- [1] B.Kasztenny, D.McGinn, S.Hodder, D.Ma, J.Mazereeuw, M.Goraj, "A Practical IEC61850-9-2 Process Bus Architecture Driven by Topology of the Primary Equipment" (42 CIGRE Session, Paris, August 24-29, 2008, paper B5-105).
- [2] NERC "Reliability Standards: Critical Infrastructure Protection" ([http://www.nerc.com/~filez/standards/Reliability\\_Standards.html](http://www.nerc.com/~filez/standards/Reliability_Standards.html))
- [3] HardFiber System Instruction Manual, GE Publication GEK-113500

Providing turn-key tailored integrated solutions using the latest technology in standard products to specifically suit your needs. Our friendly staff work with you from functional specification and establishing budgets to technical design, system development, site implementation and training; to ensure system performance.

ESAC offers services that will broaden your system's capabilities and increase the operations effectiveness with potential for growth in your organization. With an expanding client base, ESAC is equipped to fulfill your needs.



### **Electrical & Process Systems**

- Load flow, short circuit and protection coordination
- SLD, AC/DC, CWD and IED drawings
- IED, RTU and PLC programming
- Protection and automation models

### **Software & Graphic Systems**

- Communications, Historian and Web Interfaces
- HMI screens, databases and system manuals
- Custom software for user interfaces
- Database and graphic models

### **Technical Services**

- CSA Panel Shop
- Site investigations, maintenance and testing
- System retrofits and upgrades
- Training and support programs
- Strategic alliance partnering
- Project technical management
- Detailed conceptual design and budget reports

### **Projects Administration**

- Commercial contracts, project life cycle and scheduling
- Materials processing, assessments, operations and reporting

### **Distribution Automation**

- Fault localization, auto sectionalizing and restoration
- Distribution generation, voltage and VAR control

***Systems at Your Fingertips  
Integrated Protection, Control and Metering***

*Visit our website or contact us for further information  
[www.esac.com](http://www.esac.com) (519) 686-6722*

# Testing and Commissioning Protection & Control Systems Based On IEC 61850 Process Bus

Dave McGinn, Steven Hodder, Bogdan Kasztenny, Rich Hunt  
GE Digital Energy

## 1. Introduction

The Process Bus concept presented by IEC 61850-9-2 [1] is developing considerable interest worldwide in the protection and automation communities. This standard includes detailed guidance on information models, protocol stacks, datasets, VLANs, services, etc. However, little attention is paid to features necessary to engineer process bus based systems with architectures in which effective and safe system testing policies can be developed. Testing in this paper is understood as verification or re-verification of a deployed system during initial commissioning, periodically, or after a major re-work on the system such as protection system expansion, firmware upgrade or replacement of components. As such, testing is an essential part of initial startup and maintenance.

Conventional protection technologies provide for test polices that allow protection relays of a single zone to be isolated, safely modified, re-tested and restored while the protection for other zones remain in-service and unaffected. For the most part, this can be done without having to remove the protected power equipment from service, relying on redundant protection. To gain acceptance, protection systems based on process bus technology will have to provide equivalent or better capability in these areas.

When a process bus-based protection system is first constructed at a station, the protection system can be tested as a whole either before the associated power system equipment is placed in service or, in a retrofit situation, before the new process bus based protection system is integrated with the power system. In this setting, unforeseen interaction of newly added or modified components with other parts of the protection system does not impact the power system. Test signals can be safely injected to simulate fault and other unusual power system conditions, and measurements made of the impact on each part, establishing the performance adequacy of the protection system.

The problem, which is the subject of this paper, is that once a station is in-service using process bus-based protection, modifications or tests that could have unanticipated outcomes are of particular concern. It is not, in general, practical to isolate the entire process bus for the station to retest it in the same manner as was possible during commissioning. Process bus systems must therefore have an architecture that supports the ability to design and perform tests with the same flexibility as existing systems.



A practical IEC 61850-9-2 process bus system is now available for use. This paper reviews key highlights of this process bus architecture which is fully described in referenced works [2], [3] and [4], and outlines a testing policy for it that allows the protection of each zone to be securely isolated from other protections and the power system for testing, for test signals to be injected, and for correct protection system reaction to be verified. The architecture of this system inherently controls process bus traffic such that protection performance is not compromised by system expansion or changes in power system topology, and thus testing issues associated with switched networks such as variable latency and data loss due to congestion are not an issue. The proposed isolation, testing and restoration procedures are well aligned with today's practice, allowing for fast user acceptance and compliance with external regulations.

## 2. Architecture for a P&C System Based on IEC 61850 Process Bus

Recognizing the driving forces for electric utilities as well as their existing cost structure, a technical solution for protection, control and automation has been developed that is simple and practical with a significant potential for rapid acceptance. The architecture is focused on reducing overall costs and providing a system that is conceptually similar to existing applications, while physically distinct in terms of media used and association of physical interfaces to primary equipment. The solution addresses all major concerns identified in previous work [5], in particular system reliability and testability.

In reference to Figure 1, the system, known as the HardFiber System, includes HardFiber Bricks mounted directly at the primary apparatus, the relay, pre-terminated cables, and cross connect panels for cross-connecting the HardFiber Bricks and relay.

HardFiber Bricks implement the IEC 61850 concept of “merging unit”, and are designed to interface with all signals typically used for substation automation and protection as close to the respective origins of the signals as practical, including AC currents and voltages from instrument transformers, breaker status and alarms, breaker control, disconnect switch status and control, temperature and pressure readings, etc.

Each HardFiber Brick contains four independent digital cores each composed of a microcontroller with an individual bi-directional fiber link providing dedicated point-to-point communications with a single relay. Sampled value communications conform to IEC 61850-9-2, GOOSE communications conform to IEC 61850-8-1. These cores share common input/output hardware, implementing a fail-safe design strategy that ensures total isolation and independence of the digital cores. Improved overall reliability and availability of protection is optionally supported via duplicated HardFiber Bricks. No protection or control algorithms are implemented within the HardFiber Bricks; instead their sole

function is to be a high-speed robust IEC 61850 interface to the switchyard.

Cross connect panels are used to land and organize the fiber cables from the HardFiber Bricks and from the relays, and to distribute and individually fuse the dc power to the HardFiber Bricks. Standard patch cords are used to accomplish “hard-fibering”, making all the necessary connections between the relays and the HardFiber Bricks as dictated by the station configuration on a one-to-one basis, without the use of switched network communications.

Each relay has eight optical fiber ports, and thus can access directly up to eight HardFiber Bricks. Each relay provides protection for one basic zone, conforming to established protection philosophies. It receives the signals to perform its function over a secure and dedicated network consisting of direct hard-fibered links to each of the associated HardFiber Bricks. Due to the completely dedicated communications links between relays and HardFiber Bricks, with a convenient point to “break” this link, traditional testing methods may be used to test both the HardFiber Bricks and the relays much in the same way relays are tested today.

## 3. Testing Strategy for Traditional P&C Systems

Protection and control systems need to be tested to verify that they are capable of correctly performing their intended functions when initially placed in-service and when modifications are made. They need to be tested periodically in order to detect any hidden failures that may develop. Testing is required to isolate an operational problem to a specific component, and to verify system performance following repair. Tests must cover the entire protection and control system, not just the relay. The “test zones” as they apply to traditional P&C systems are summarized in Table 1.

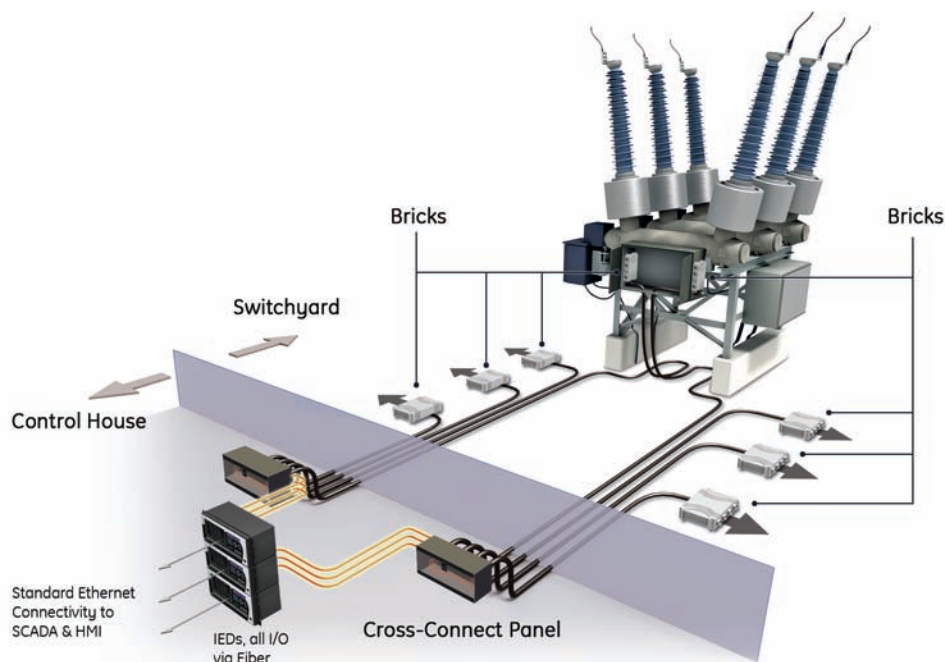


Figure 1.  
HardFiber process bus architecture

Test Zone	Purpose	Methodology
Relay	<ul style="list-style-type: none"> <li>• Device, including I/O</li> <li>• Firmware</li> <li>• Settings</li> </ul>	<ul style="list-style-type: none"> <li>• Isolate</li> <li>• Secondary ac injection (5A, 115/66.4V)</li> <li>• Short contact inputs</li> <li>• Monitor output contact closures</li> </ul>
Instrument Transformers, Position Sensors, Condition Monitors, Control (e.g. Trip/Close) Circuits	<ul style="list-style-type: none"> <li>• IT ratios and location</li> <li>• Primary sensor/monitor functionality</li> <li>• Control circuit functionality</li> </ul>	<ul style="list-style-type: none"> <li>• Excitation check</li> <li>• Ratio check</li> <li>• Functional test of position sensors and condition monitors</li> <li>• Control circuit operational tests</li> </ul>
Relay/Switchyard interconnection	<ul style="list-style-type: none"> <li>• Verify cables and connections</li> </ul>	<ul style="list-style-type: none"> <li>• Ring-out wiring</li> <li>• On load metering checks</li> <li>• Trip tests from relay panel</li> </ul>

**Table 1.**  
Traditional P&C Testing Strategy

It is worth noting up-front that traditional protection test procedures are based on the use of test switches (e.g. FT switches) at the relay location, but that such test switches are impractical with HardFiber applications as all copper wiring is terminated at HardFiber Bricks located at primary equipment in the switchyard. Instead, the HardFiber System is designed for the ability to isolate trip outputs and analog signals by disconnecting the fiber optic cabling between the relay and the HardFiber Bricks. This method provides the same functionality as traditional test switches, and does so in a simpler and more error-proof manner.

## 4. Testing Strategy Overview

As shown in Figure 2, the high-level test strategy is to divide the protection into three test zones:

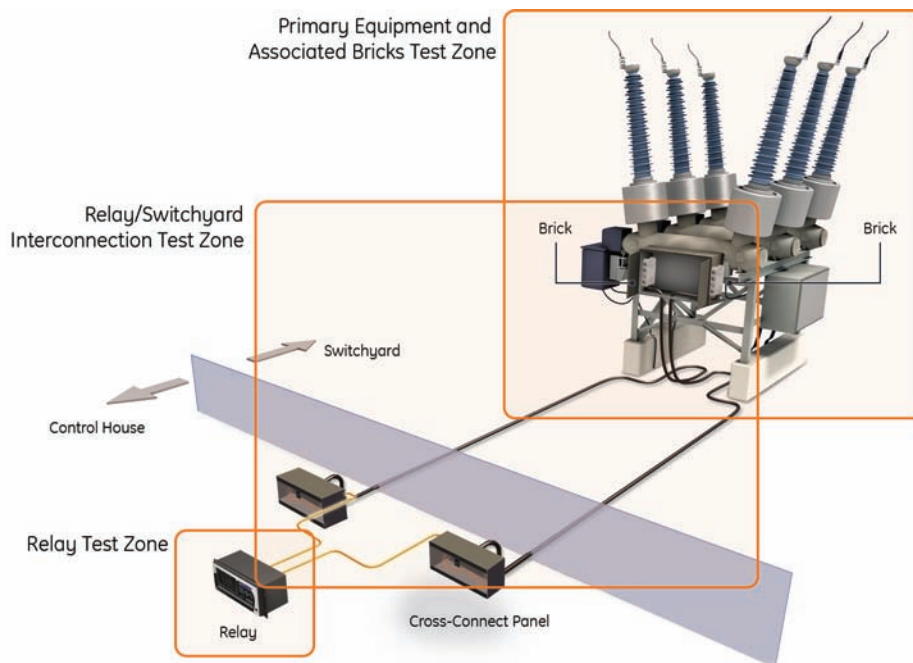
- 1) The relay
- 2) The primary equipment and associated HardFiber Brick(s)
- 3) The relay/switchyard interconnections

Each of these three zones are tested independently, with testing properly overlapped to establish correct inter-zone interaction, and thus correct operation of the system as a whole. To emphasise an important and novel point here, HardFiber Bricks are blended into primary equipment in the same way the wires they replace are blended by traditional test strategies. As one would for instance, initiate a test trip from the control house to check that both the copper cabling conducts the trip signal to the breaker's trip coil, and at the same time check that the breaker actually opens when trip is applied to the coil. Here a test trip from the control house checks that the fiber cabling and HardFiber Brick combination conducts the trip signal to the breaker's trip coil and at the same time checks that the breaker actually opens.

The overlapping "test zones", as they apply to the process bus implementation, are summarized in Table 2.

Test Zone	Purpose	Methodology
Relay	<ul style="list-style-type: none"> <li>• Device, including I/O</li> <li>• Firmware</li> <li>• Settings</li> </ul>	<ul style="list-style-type: none"> <li>• Isolate</li> <li>• Injection of AC input sampled values</li> <li>• Force contact input signals on optical fiber ports</li> <li>• Monitor contact outputs on optical fiber ports</li> </ul>
HardFiber Brick & Instrument Transformers, Position Sensors, Condition Monitors, Control (e.g. Trip/Close) Circuits	<ul style="list-style-type: none"> <li>• IT ratios and location</li> <li>• Primary sensor/monitor functionality</li> <li>• Control circuit functionality</li> <li>• HardFiber Brick functionality</li> </ul>	<ul style="list-style-type: none"> <li>• Excitation check</li> <li>• Digital ratio check (primary input to sampled values)</li> <li>• Functional test of position sensors and condition monitors (primary state to signal on optical fiber)</li> <li>• Control circuit operational tests digitally forced from optical fiber link</li> </ul>
Relay/Switchyard interconnection	<ul style="list-style-type: none"> <li>• Verify cables and connections</li> </ul>	<ul style="list-style-type: none"> <li>• Continuous self-checking</li> <li>• On-load metering checks</li> <li>• Trip tests from relay</li> </ul>

**Table 2.**  
HardFiber Testing Strategy



**Figure 2.**  
Test Zones

It is important to note that when Table 1 is compared with Table 2, the total coverage remains the same between the traditional and process bus-based systems, although the methodology is different.

## 5. Test Procedure for Relays

In overview, the procedure for testing a Universal Relay (UR) in a HardFiber process bus system is the same as testing a Universal Relay in a conventional system, and consists of isolating the relay test zone, doing any required work such as hardware replacement, settings or firmware changes, followed by the actual testing, and then finally restoring the relay test zone to service. The difference is in the physical methods used to isolate the zone, and the means to inject and monitor relay signals. The test zone for this procedure is the UR and any process bus fiber cabling between the relay and the point where the relay is physically disconnected to isolate the relay from the remaining in-service protection system. The test zone may also include some station LAN components and conventional copper I/O beyond the scope of this paper.

### 5.1 Relay isolation

A critical testing step in the in-service environment is the isolating (blocking) of relay outputs from external circuits to prevent unintentional operation of those circuits (e.g. tripping). Failure to perform this step properly can result in the testing effort causing much more harm than it could potentially do good. For this reason the UR relay firmware provides a manual command that puts the relay in a "Test-Isolated" mode, wherein all process bus command outputs from the relay are disabled. This is equivalent to opening the output test switches in a conventional copper

connected protection, except that all of the command outputs are blocked with a single user action – there is no chance that wiring or personnel error can result in one output being overlooked and left operational. When in this mode, a front panel "In-Service" indicator is turned off, a "Test Mode" indicator is turned on, and the critical failure contact put in the alarm position, so that there is little chance of even one output of the relay being inadvertently left in this blocked state when work is complete. This mode is non-volatile; the only way to return to the normal in-service mode is by specific user command action.

In the testing methodology state diagram of Figure 3, the state transition resulting from this step is labelled "Command Test-Isolated Mode".

With conventional copper connected protection schemes, external circuits connected to the relay inputs must also be safely isolated from test conditions harmful to the external circuits (e.g. opening a CT circuit), and test actions (e.g. AC injection) with an adverse effect on other users of the signals. There is no equivalent concern with the HardFiber process bus implementation. There is no equipment harm in opening the fibers, and the fibers associated with the relay under test have no other client, due to the point-to-point process bus architecture.

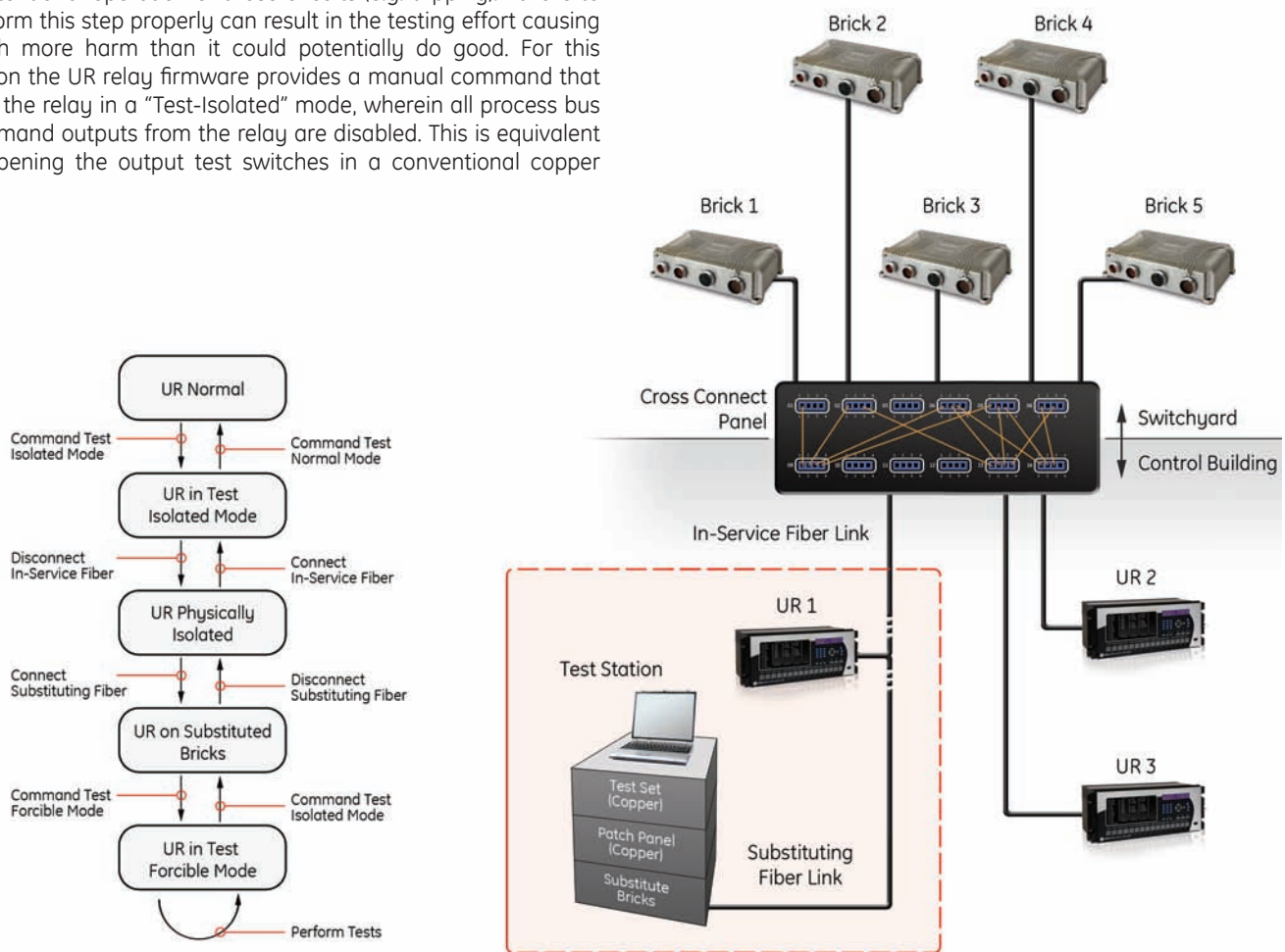


Figure 3. Relay test methodology and facilities

## 5.2 Relay injection testing

Traditionally, relays are tested by injecting signals, to check their current, voltage and contact input hardware, to check that the measuring elements and scheme logic are operating correctly, to check that their settings are correct (e.g. that the technician or settings engineer did not accidentally type 15.0 instead of 1.50 for a pickup value), and to check the contact output hardware. Now with process bus, the relay has no physical current, voltage or contact inputs, so there is no corresponding hardware to check. The hardware performing a somewhat analogous function, the optical transceivers, PHY chip, etc., are continuously self-tested with signal level margin detectors and with data security codes (i.e. CRC), so there is little, if any, value in further testing the relay's process bus input/output hardware. The firmware that implements the measuring elements and scheme logic is continuously checked again by CRC, and the processors by watchdog timers. A strong argument can be made that injection testing for checking the settings is of little value, that there are other less complex and more secure means of verifying the settings [6]. There seems to be little value for using injection testing on the relays. Never-the-less, simulating power system faults and observing relay reaction has value as a method for checking the settings in a way that does not involve a human understanding of how the relay interprets its settings, and thus can be done by personnel with a different perspective than the settings engineers, and thus less likely to make the same mistake. This makes it advisable to have the ability to do injection testing with process bus.

Traditionally, injection testing uses a relay test set connecting to the relay under test via test switches (e.g. FT switches). With the HardFiber process bus architecture a conventional relay test set is still used, but is connected to the relay's optical fiber ports through test or "substitute" HardFiber Bricks, identical to the permanent HardFiber Bricks. The substitute HardFiber Bricks and the relay test set together form a "test station", which can be thought of as a process bus relay test set. It injects inputs and monitors outputs from the relay's process bus ports analogous to the way a conventional relay test set injects and monitors conventional current/voltage/contact ports.

The HardFiber Bricks have no "personality"; except for their serial number and order code, the permanent HardFiber Bricks are fully interchangeable with substitute test HardFiber Bricks. HardFiber Bricks have no settings, which would otherwise differentiate them, and the initial HardFiber Brick firmware version is irrelevant as the relay's version is automatically downloaded. The connection between the relay and the substituted/permanent HardFiber Bricks are both direct point-to-point hard-fibered links, and need no settings to setup. Therefore one may be confident that the test signals delivered to the relay by the substituted HardFiber Bricks are the same as those from the permanent HardFiber Bricks, and vice versa.

This hardware substitution test strategy tests outputs by checking the output signals using the test station as a measuring device. The assumption is made that a signal that made an output of the substituted HardFiber Brick operate would have made the permanent HardFiber Brick operate. Traditional relay test strategy for checking outputs is by measuring voltage signal levels at a break in the signal path made by an FT test switch, using a multimeter or a relay test set. The assumption is made that if the FT switch

were instead closed, the connected breaker would trip. Thus it can be seen that the hardware substitution strategy is more realistic than the traditional test strategy; to be comparable the traditional strategy would have to use a "test breaker" to confirm outputs are capable of supplying breaker trip level currents.

To use this technique, after putting the relay in the test-isolated mode, the user disconnects the in-service process bus fiber connections either at the relay itself or at the cross connect panel, and connects instead substituting fiber to the test station. Proper fiber handling practices need to be observed while disconnecting and reconnecting the fiber.

At this point if required, the relay can be swapped out, new firmware loaded, and/or new settings applied. The user then issues a command to the relay causing it to switch from the test-isolated mode to the "test-substituted" mode, wherein the commands are again enabled onto the process bus, which now connects only to the test station. In addition, the configuration locking mechanism that normally prevents communications between a relay and a HardFiber Brick with other than the set serial number is bypassed, to allow the relay under test to communicate with substituted HardFiber Bricks. The front panel indicators and critical fail output continue to show that the relay is not in-service.

Refer to the correspondingly labelled steps in the state diagram in Figure 3. Once in this test-substituted mode, the conventional relay test set may be used to perform any functional tests that could have been performed on a non-process bus system. The nature of these tests, and how they accommodate station bus or conventional contact I/O, is beyond the scope of this paper.

## 5.3 Relay restoration to service

Once the testing is complete, it is necessary to restore the relay to service in a safe and secure way. One needs to avoid the trap of closing a switch, making a connection, or restoring a mode that results in undesired action such as tripping a circuit breaker. Without due care, such could occur for instance due to the seal-in of a protection scheme or the response to having some but not yet all live inputs restored. This can be accomplished by reversing the actions of the previous steps, moving up in the Figure 3 state diagram. First the user commands the test isolated mode so that when the permanent HardFiber Bricks are re-connected, no process bus commands can result in undesired action such as tripping. The substituted HardFiber Brick fiber links are disconnected, and the permanent HardFiber Bricks re-connected. Just before commanding the switch to the normal in-service mode and going live, the user should check the actual values of the relay's process bus outputs, that they are in a state that will not cause problems when re-enabled. At this time the user should check that the relay has not raised any alarms resulting from missing or misconnected permanent HardFiber Bricks, or unacceptable signal margins. One may also check that the data being received from the permanent HardFiber Bricks is reasonable, internally consistent, and matches indications from other equipment. However, as neither the permanent HardFiber Bricks nor their connections to the power equipment have been disturbed by this test procedure, and as the relay announces any problem communicating with the HardFiber Bricks, this crosschecking may not be worth the effort.

## 6. HardFiber Brick/Primary Equipment Testing

### 6.1 Initial installation/major rework

The proposed high level test strategy combines the HardFiber Brick testing with the testing of the associated primary equipment functions. For a particular function, such as a breaker trip command, the checking of the HardFiber Brick, the primary equipment and the interface between the two is efficiently verified with one test. This strategy also eliminates the need for test switches between the HardFiber Brick and the primary equipment.

Testing of functions using HardFiber Brick contact inputs is accomplished by forcing a change of state in the primary equipment and observing the result on the signal transmitted by the HardFiber Brick. For instance, breaker position status contact inputs are tested by opening or closing the breaker and observing the signal change on the HardFiber Brick fiber port. The transmitted signal may be observed either using the permanent relays, or with a substitute relay used in a way similar to how substitute HardFiber Bricks were used in testing the permanent relays. A substitute relay may be more convenient than a permanent relay, as the substitute may be made portable and used adjacent to the HardFiber Brick/primary equipment. A substitute may also be used when the permanent relay or fiber cabling is not available such as at the primary equipment factory, during initial on-site installation before the fiber cable and/or permanent relay is installed, or while the relays are in-service and cannot yet be configured for the new incoming HardFiber Brick/primary equipment.

Testing of functions using HardFiber Brick contact outputs is by activating that output from the substitute or permanent relay and observing the correct primary equipment response (e.g. tripping).

CT and VT functions are checked by observing the analogue values transmitted by the HardFiber Brick with primary voltage or current present. The observed magnitude and phase indication is compared with other devices metering the same primary quantity. In the case of initial testing before the primary equipment can be energized, the checks may be either by primary injection using the appropriate injection test equipment, or by separately testing the HardFiber Brick (with secondary injection) and the instrument transformer (with conventional techniques). Test cables are required with a plug to inject secondary signals to the HardFiber Brick and a receptacle to breakout the secondary signals from the instrument transformer. Where this separate testing technique is used, the comparison technique should also be used immediately after the primary equipment is energized to verify the correct connection between the instrument transformers and the HardFiber Brick.

### 6.2 HardFiber Brick replacement

Although HardFiber Brick design is such that failures will be rare, a strategy for handling such cases in a cost effective manner is still required. The design should be such that HardFiber Bricks can be replaced without undue worker safety risk, and ideally without outage to the associated power system element. Isolating means are therefore built into the HardFiber Brick itself that do not consume additional space or field labour for installation. The HardFiber Brick has all electrical and optical fiber connections

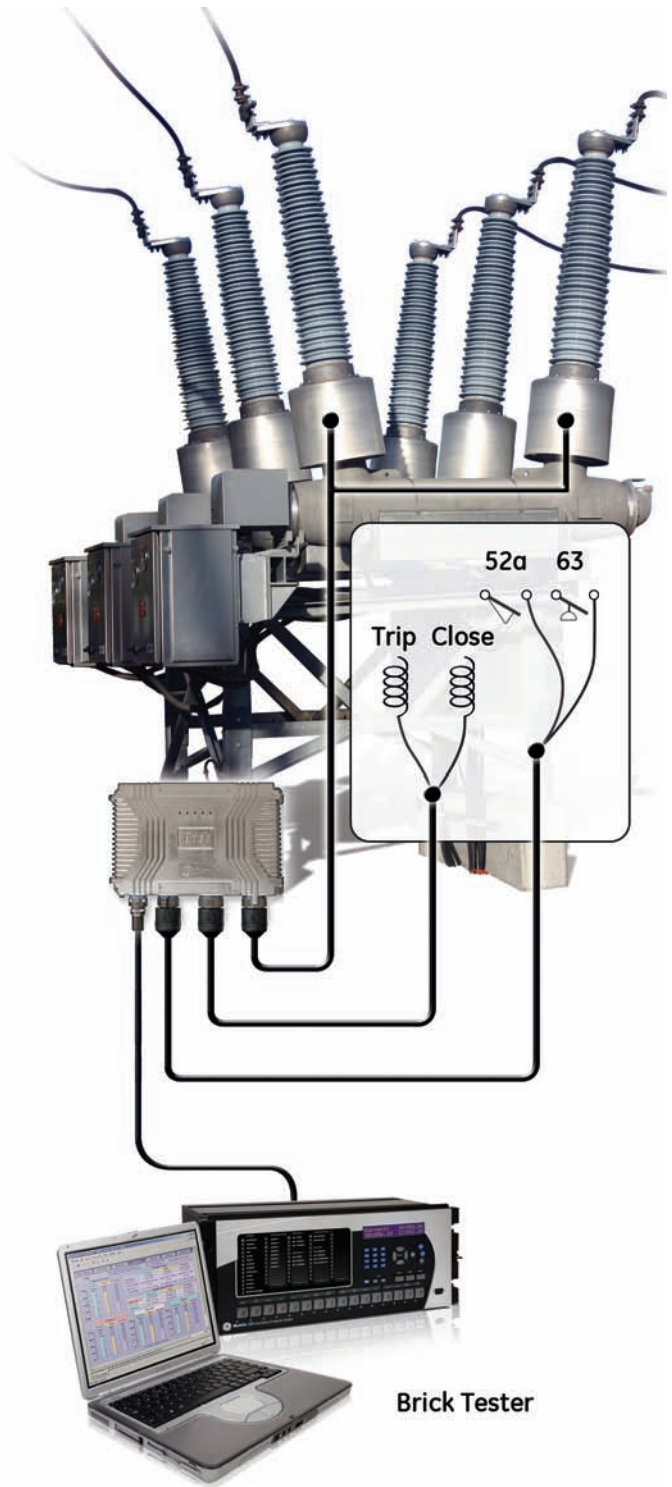


Figure 4.  
HardFiber Brick/Primary Device testing



equipped with highly reliable quick mating connectors in the proven MIL-DTL-38999 series. However, with this particular series of connector, if one wishes to have the ability to replace a HardFiber Brick with the CT circuit live, additional facilities are required to bypass live CT current loops. Careful consideration should be made on whether the ability to replace a HardFiber Brick without primary equipment outage is worth the addition cost, complication and safety risk involved with working on live CT circuits.

Prior to connecting the new HardFiber Brick, it can be fully tested in a safe environment using the HardFiber Brick tester and a conventional relay test set. Once the fiber cable plug-in connections to the in-service relays are made, the communications system testing described below is executed. Typically the replacement activity would conclude with a check that the controls are operational (i.e. trip and close breaker, which can be done via SCADA if it uses the same hardware), a check that the currents' and voltages' magnitude and phase are reasonable and consistent with other sources, and that breaker and alarm status is correct.

### 6.3 Routine periodic testing

Regulations in some jurisdictions mandate that protection systems be periodically re-tested to verify that it is capable of performing its intended protection function. Most requirements of such regulations are satisfied by the continuous self-testing and event recording the process bus system provides. For instance, the optical signal is continuously monitored in the system and degradations that may affect signal adequacy are alarmed. Event reports can be used to locate and verify the correctness of recent breaker operations, usually avoiding the need for trip tests. Any individual items not covered by either of these can be accomplished using the techniques described in the above sections.

## 7. Relay/Switchyard Interconnections Testing

The objective of the relay/switchyard interconnections testing is to check those process bus functions not covered either by the relay injection testing or by the HardFiber Brick/primary equipment testing. Relay injection testing using substituted hardware establishes that the relay properly consumes data streams presented to its process bus optical fiber ports, and properly generates control data streams on these same ports. HardFiber Brick/primary equipment testing establishes that the HardFiber Brick and primary equipment working together generate a data stream that properly encodes the primary quantities and properly executes commands received. What remains in checking the protection system as a whole is to establish that with the protection system fully in-service, the data streams generated by the relays and the HardFiber Bricks are reaching the correct destinations with adequate signal levels.

With the HardFiber process bus implementation, the "hard-fibered" approach eliminates interconnection testing issues such as LAN congestion, correctness of LAN configuration settings required to automatically re-route around failed switches, non-

deterministic latency, etc.; issues that make thorough testing very difficult in a packet switched network. Use of single bi-directional fiber technology eliminates the concern present with double simplex fiber links and with multi-conductor copper cabling that the link is only partially correct – correct communications of any bit of data in either direction establishes that all data on that link is communicated correctly. All that is necessary is to establish that there is a continuous optical path from each port of the relay to/from the correct HardFiber Brick, and that path losses leave adequate signal margin.

Excessive optical path losses can result from manufacturing problems or damage occurring during shipment or installation, though the more likely the cause is contamination in the optical fiber connectors introduced during installation or maintenance. Establishing the value of path losses (and thus operating margin) is easily done in the system, as the optical transceivers at both ends are equipped with diagnostics that continuously measure the send and receive light levels even while the link is in normal operation. The relay then generates alarms should any level fall out of tolerance. Establishing the correct operation of these alarms should be part of the relay injection testing and the HardFiber Brick/primary equipment testing.

The "hard-fibered" architecture means that incorrect interconnection between relays and HardFiber Bricks can only result from incorrect installation of the fiber cables or patch cords. There are no settings that result in cross-connections. Correct interconnection can be established in any of several ways:

- Physically tracing the cable and patch cord routing from the back of the relay to the HardFiber Brick.
- Observing the data received by the relay over the link is reasonable and matches other indicators. For example indicated current/voltage magnitude and phase matches other indicators of these same quantities.
- Causing some change of state and observing its correct communication over the link. For example, observe the reported effects of initiating a breaker operation or a tap change. Initiation may be from the operator's HMI where it uses the same fiber link.
- The relays are designed such that when normally in-service, they alarm and reject data on a port when the HardFiber Brick serial number that is included with the data fails to match the relay setting for that that HardFiber Brick's serial number. The relay serial number value is included with outgoing commands, and the HardFiber Bricks are designed to accept commands only when the accompanying serial number matches its own serial number. Thus, once the HardFiber Brick serial numbers are correctly entered into the relay settings, the fact of normal communications establishes that the link is correct. The serial number setting in the relay can be manually checked against the serial number on the HardFiber Brick's nameplate.

Thus it can be seen that testing of the passive interconnection system is quite simple, and that after commissioning is complete, it can be entirely automatic.

## 8. Conclusions

This paper presented a complete and simple testing procedure for the HardFiber process bus architecture. In particular the following important advantages are provided:

- Opportunities for inadvertent operations due to employee error are reduced due to easy comprehension on the part of test personnel of the simple architecture.
- Improved safety for test personnel as all relay testing work is done in the safety of the control house, separated from the hazards present in the switchyard, and isolated from high energy CT and VT circuits by fiber optics.
- The comprehensiveness of the relay test method proposed is assured though use of the traditional strategy of isolating the relay's outputs, injecting signals simulating power system conditions such as faults to the relay's inputs, and monitoring the relay's response. Traditional methods are also used to test the complete protection system.
- Training of test personnel is minimal as conventional relay test sets are used in familiar ways, with additional HardFiber Bricks adapting the conventional test set to the optical fiber format used by the relay.
- The system is self-monitored. Most or all of routine re-verification and much of commissioning testing can be accomplished without disturbing the in-service system.

## 9. References

- [1] IEC International Standard "Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/IEC 8802-3", (IEC Reference number IEC/TR 61850-9-2:2004(E), IEC, Geneva, Switzerland).
- [2] HardFiber 61850 Process Bus System Instruction Manual, GE Publication GEK-113500
- [3] B.Kasztenny, D.McGinn, R.Mao, D.Baigent, N.Nazir, S.Hodder, J.Mazereeuw, "An Architecture and System for IEC 61850 Process Bus" (GE Multilin Protection & Control Journal, August 2008)
- [4] B.Kasztenny, D.McGinn, S.Hodder, D.Ma, J.Mazereeuw, M.Goraj, "A Practical IEC61850-9-2 Process Bus Architecture Driven by Topology of the Primary Equipment" (42 CIGRE Session, Paris, August 24-29, 2008, paper B5-105).
- [5] B.Kasztenny, D.Finney, M.Adamiak, E.Udren, J.Whatley, J.Burger, "Unanswered Questions about IEC 61850 - What needs to happen to realize the vision?" (Proceedings of the 31st Annual Western Protective Relay Conference, Spokane, WA, 2005).
- [6] S.Fulford, M.Thompson, "An Examination of Test Switches in Modern Protection and Control Systems" (Proceedings of the 34th Annual Western Protective Relay Conference, Spokane, WA, 2007).

# Scalability of IEC 61850 Process Bus Solutions

Dale Finney, Bogdan Kasztenny  
GE Digital Energy

---

## 1. Introduction

Too often solutions are proposed that conceptualize process bus architectures by depicting a single merging unit, or at best a few merging units, and a single or a few relays, interconnected by a “magic cloud” of a Local Area Network (LAN).

Such conceptual sketches are practical and useful in the field of engineering to communicate mature ideas and abstracts in situations when there is a common understanding of the basic principles behind a concept. Common understanding of basic principles may be established by tradition, formal education or on-the-job training of the involved individuals, practical usage and installations, existing products, and common sense. Process bus schemes have not matured enough to yield common understanding that would justify conceptual sketches neglecting the actual physical nature of the problem at hand, and its scale.

It is therefore understandable that prospective process bus users challenge conceptual sketches by asking variety of questions such as: What is a merging unit? What is its function? Where is it located? Does it work with conventional instrument transformers, or only with optical instrument transformers? How about status signals and control commands - do they fit in the merging unit concept? How do I engineer the “magic cloud”, interconnecting the devices? How do I know the “magic cloud” will work after adding a new device? How do I test and commission a process bus scheme through the “magic cloud”?

And finally, how does any solution scale up and down to accommodate substations of any size, following a retrofit of any scope and sequence?

A successful IEC 61850 process bus architecture needs to be scalable. Scalability in this context means adding devices to build a coherent system of any size without the need to address size issues along the way. In other words, setting up a process bus consisting of 150 merging units and 100 relays should be as easy as setting up a system with 3 merging units and 1 relay. Moreover, procedures and methods used to isolate, maintain, test and operate a system with 3 merging units and 1 relay should be applicable for larger systems without significant modification.

In contrast, one can consider the characteristics of systems that are not easily scalable. For instance, a system in which the impact of system performance must be re-evaluated each time a device is added cannot be regarded as easily scalable. A system that requires reconfiguration of in-service devices that are responsible for protecting other circuits in the substation in order to add a new device also cannot be regarded as easily scalable.

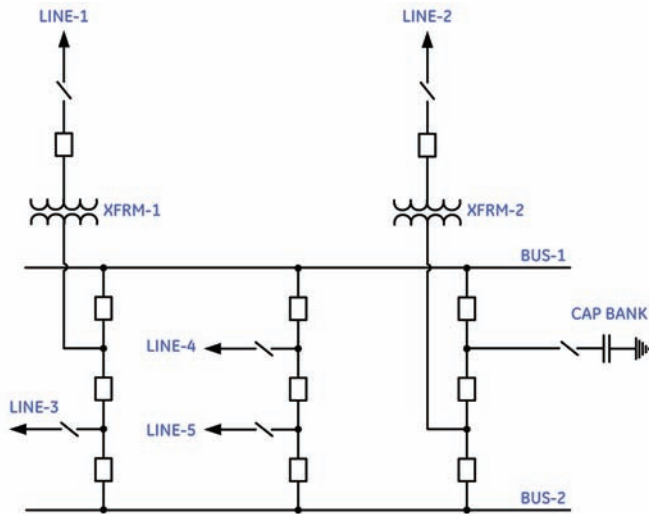


This paper will explain the need for and benefit of scalability by using a simple breaker-and-a-half substation, and the process bus architecture of the HardFiber system from General Electric [1].

The Hard-Fiber system eliminates custom control wiring within the station and replaces it with rugged field devices, known as Bricks, distributed throughout the switchyard and interconnected with substation IEDs through a standardized optical fiber network.

The fundamental components of the Hard-Fiber system are:

- Bricks – convert analogue copper signals to/from digital optical signals, including CTs, VTs, contact inputs and contact outputs.
- Copper Cables – make the connections between the copper terminals inside the power equipment to the Bricks typically mounted on the outside of the equipment.
- Outdoor Fiber Cables – make the optical connection between the Bricks in the switchyard and the cross connect panels in the control house. Also powers Brick internal electronics.
- Cross Connect Panels – panel where individual fibers of outdoor cables are patch corded to individual fibers of indoor cables, completing the station specific Brick/relay associations. Also DC distribution panel for Bricks.
- IED Process Card – converts Brick optical signals to/from the signal types used by the standard Universal Relay [2-9] elements.
- Indoor Fiber Cables – make the optical connection between the ports of the process card in the UR and the cross connect panel.



**Figure 1.**  
Sample substation considered

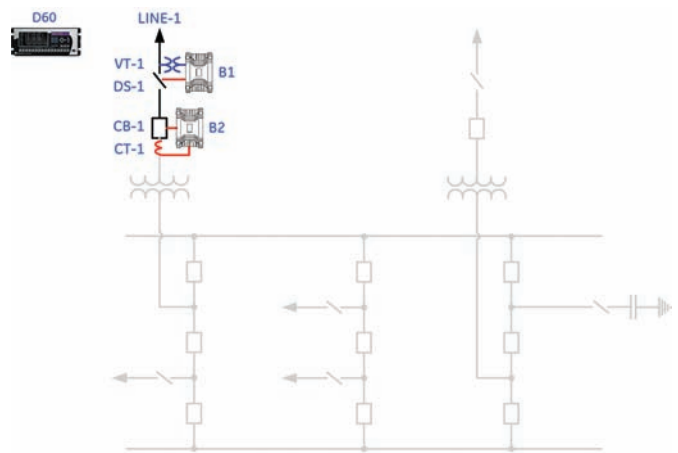
## 2. Sample station

(Figure 1.)

Figure 1 depicts a sample breaker-and-a-half substation with two transformers and corresponding transmission lines, two buses, several sub-transmission lines, and a capacitor bank terminated on a breaker-and-a-half position.

It is assumed that this station ultimately is to be entirely retrofitted using a process bus system, specifically the HardFiber system [1].

In order to explain and illustrate scalability as it relates to the deployment of a process bus-based protection and control system, the paper will consider the retrofit on a zone-by-zone basis, and progress gradually to cover the entire substation. In the process it will not only become clear that the solution is scalable, but also exceptionally flexible allowing applications in substations of any topology and any practical protection and control practice.



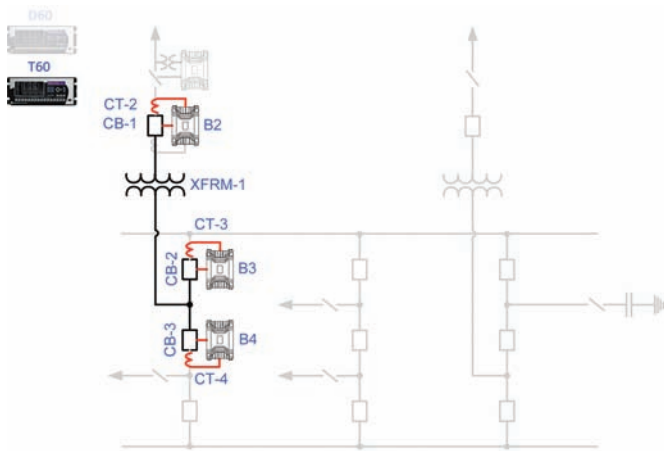
**Figure 2.**  
Line 1 distance protection example

### 2.1 LINE-1 zone

(Figure 2.)

In order to protect and control LINE-1, a Brick B1 is installed to connect the line potential (VT-1) and possibly interface the line motor-operated disconnect switch (DS-1). A second Brick, B2, is deployed to interface the line breaker (CB-1) and provide the measurement of the zone current (CT-1). These two Bricks can be wired to a variety of other signals associated with the line and breaker apparatus such as breaker position and alarms, position of breaker disconnect switches, and so on. The application is completed by patching the two Bricks to an appropriate line protection relay, the D60 Distance Protection System [2] in this example. The relay is configured to use VT-1 and CT-1 for its fundamental protection functions, and trips CB-1 upon detecting a fault in the LINE-1 zone. A variety of other functions are available in the D60 relay model such as metering, control, an array of backup functions, teleprotection schemes, integrated breaker failure, and embedded Phasor Measurement Unit (PMU).

Note that the LINE-1 P&C refurbishment work can be done in total isolation from the rest of the station, without disrupting other zones of protection or the primary equipment, and without forcing the user to retrofit the entire substation. For commissioning, only LINE-1 needs to be taken out of service.



**Figure 3.**  
Transformer 1 protection example

## 2.2 XFRM-1 zone

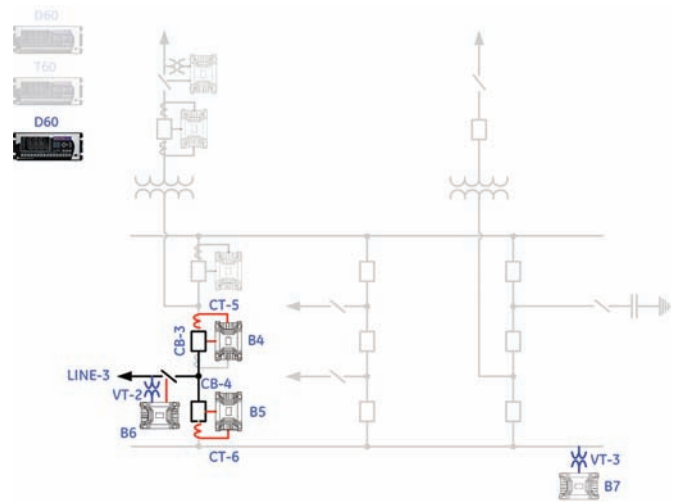
(Figure 3.)

The transformer is terminated on a breaker-and-a-half diameter. Bricks B2, B3 and B4 are used to provide tripping capabilities toward the associated breakers CB-1, CB-2 and CB-3, respectively; as well as to measure all the currents of the transformer protection zone: CT-2, CT-3 and CT-4, respectively.

Note that the B2 Brick is already deployed as a part of the LINE-1 zone. To support the XFRM-1 zone, this Brick is wired to the CT-2 set of currents, and communicate with the transformer relay on its second digital core [1]. In this way the B2 Brick is shared between line and transformer relays. A stand-alone Breaker Failure (BF) relay may be deployed for the CB-1 breaker, such as the C60 Breaker Protection System [3], being the third relay connected to the B2 Brick. Note that although the B2 Brick is shared by several relays, there are no shared subsystems that introduce interdependencies between protection applications.

The transformer zone application is completed by patching the B2, B3 and B4 Bricks to a transformer protection relay, a T60 Transformer Protection System [4] in this case.

The considered transformer protection zone spans the associated breakers. Alternatively, its zone can be deployed from the transformer's bushing CTs with Bricks installed at the transformer, rather than at the associated breakers. In such a case, the transformer Bricks will pickup alarms and status signals for the transformer, tap changer status and control, and other signals naturally related to a power transformer, while the breaker Bricks will still be connected to execute the trip commands.



**Figure 4.**  
Line 3 distance protection example

Neutral point currents required for Restricted Earth Fault (REF) protection of wye-connected windings can be wired to transformer Bricks if installed, or to the nearest Brick associated with any of the transformer breakers. Quite often a dedicated Brick will be installed at the transformer regardless of the protection measurement and tripping Bricks to pick up additional trip signals like Bucholtz relays or tap changer gas relays.

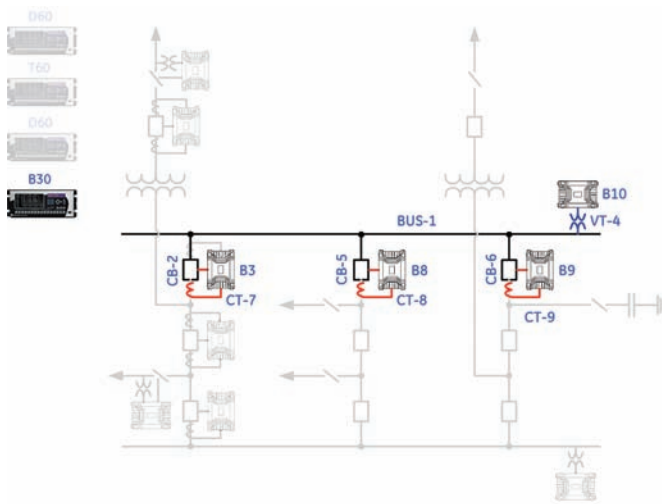
The T60 relay deployed in this example supports a multitude of functions such as overcurrent and distance backup, harmonic and power measurement, and so on [4].

## 2.3 LINE-3 zone

(Figure 4.)

LINE-3 is terminated as a breaker-and-a-half power element, and therefore Bricks B4 and B5 are used to interface the associated breakers (CB-3 and CB-4), as well as to measure the zone currents (CT-5 and CT-6). Note that the B4 Brick is already installed as a part of the XFRM-1 zone, and needs to measure the second set of currents, CT-5, at that breaker to support the LINE-3 zone. The third Brick, B6, is required to interface the line potential, VT-2, and possibly the line disconnect switch. It is assumed a synchrocheck function is incorporated for the CB-4 breaker therefore B7 Brick is deployed to measure the bus voltage via VT-3 potential source.

A line protection relay, D60 Distance Protection System [2] is connected to the B4, B5, B6 and B7 Bricks to complete the application for the LINE-3 zone. Having five zones of distance protection, the D60 can be used to provide time-coordinated reverse-looking backup for the substation and associated circuits.



**Figure 5.**  
*Bus 1 differential protection example*

## 2.4 BUS-1 zone

(Figure 5.)

A bus differential relay, a B30 Bus Protection System [5] in this example, is deployed to protect BUS-1. The relay is patched to Bricks B3, B8 and B9 to measure the bus zone currents, CT-7, CT-8 and CT-9; and to execute the trip command toward breakers CB-2, CB-5 and CB-6. Optionally, it may connect to the B10 Brick for the voltage signal, VT-4 in order to provide for under-voltage trip supervision or power metering.

Note that the B3 Brick is shared between the B30 and T60 relays. Additionally, a stand-alone BF relay, such as the C60 [3] can be deployed for each of the CB-2, CB-5 and CB-6 breakers. In such a case, the C60 relays are patched to Bricks B3, B8 and B9, respectively.

## 2.5 BUS-2 zone

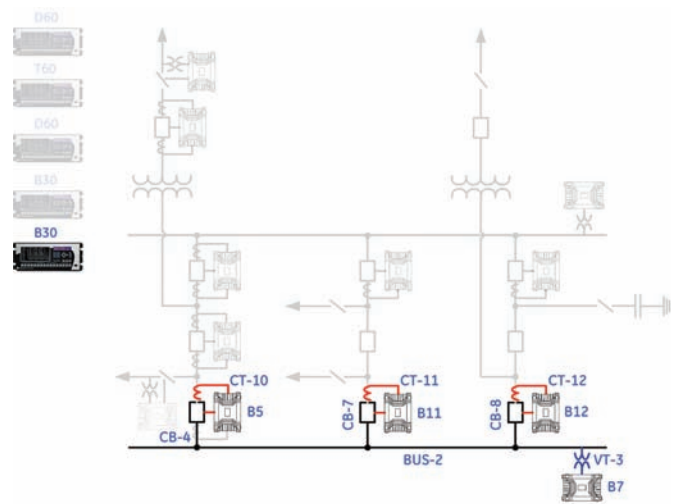
(Figure 6.)

Similarly, a bus differential relay, B30 Bus Protection System [5] in this example, is deployed to protect BUS-2. The relay is patched to Bricks B5 (already installed for the LINE-3 protection), B11 and B12 to measure the bus zone currents, CT-10, CT-11 and CT-12; and to execute the trip command toward breakers CB-4, CB-7 and CB-8. Optionally, it may connect to the B7 Brick for the voltage signal, VT-3 in order to provide for under-voltage trip supervision or power metering.

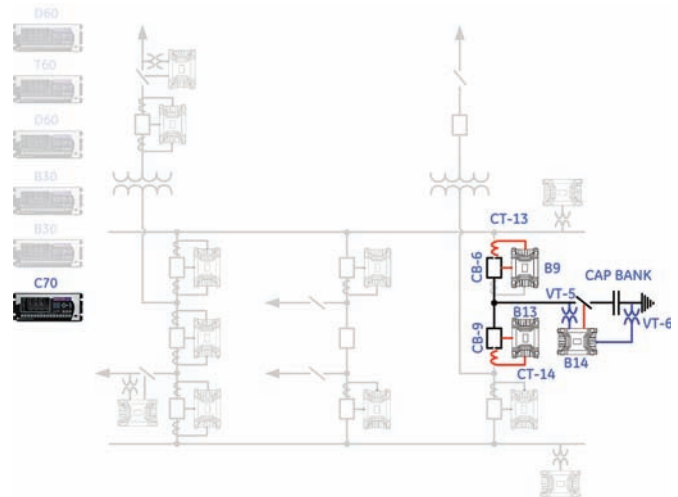
## 2.6 CAP BANK zone

(Figure 7.)

Consider the capacitor zone next. A capacitor bank relay, the C70 Capacitor Bank Protection and Control System [6] in this example, is connected to Bricks B9 and B13 in order to interface currents CT-13 and CT-14 for short circuit protection and metering, as well as to trip the dual-breaker connection via CB-6 and CB-9. In addition The B14 Brick is installed to provide for sensitive voltage-based bank unbalance protection such as voltage differential, or neutral voltage unbalance by measuring the VT-5 and VT-6 potentials. This Brick may interface with the shown disconnect switch and other signals associated with the installation as required.



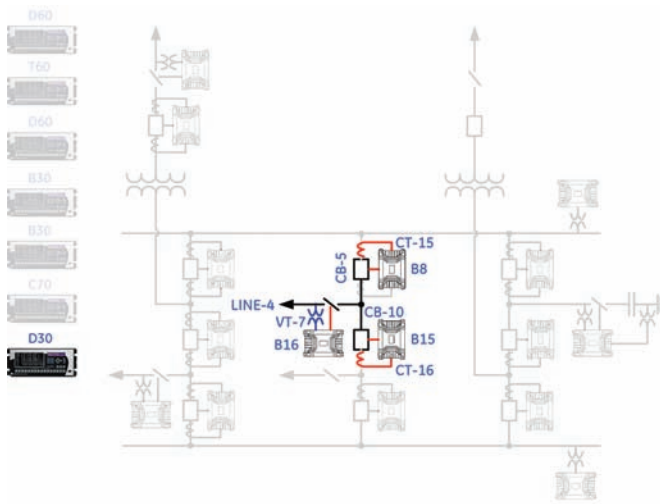
**Figure 6.**  
*Bus 2 differential protection example*



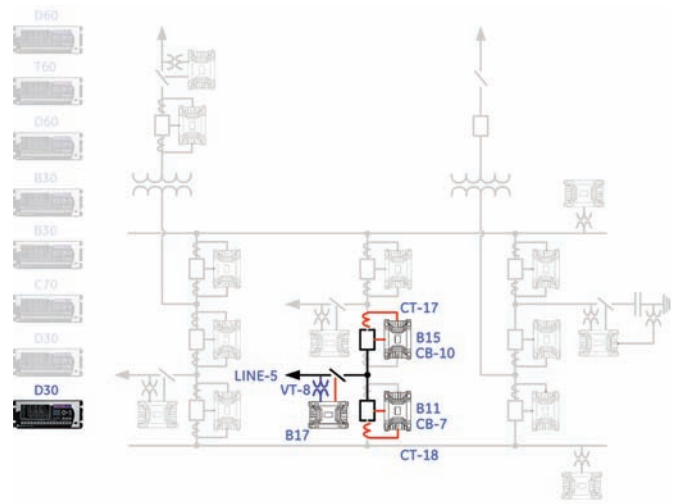
**Figure 7.**  
*Capacitor bank protection example*

The capacitor bank application is a good example of scalability within a given zone of protection. Imagine a very complex cap bank arrangement with parallel banks, multiple current and voltage measurement points, multiple protection principles deployed such as phase current unbalance, neutral current unbalance, voltage differential, neutral voltage unbalance or multiple coordinated controllers for multiple capacitors or banks. In such a case a number of Bricks can be installed to interface all required signals, and more than one C70 can be used to provide all required functions.

Additionally, capacitor banks tend to be added long after a station has been built, usually in remote areas of the switchyard. The long distances to the control house makes a process bus solution a natural choice for elimination of copper wires.



**Figure 8.**  
*Line 4 distance protection example*



**Figure 9.**  
*Line 5 distance protection example*

## 2.7 LINE-4 zone

(Figure 8.)

Three Bricks (B8, B15 and B16) are connected to a line relay, D30 Distance Protection System [7] in this example, in order to interface the zone currents (CT-15 and CT-16) and voltages (VT-7). The B16 Brick may interface the line disconnect switch if appropriate, and Bricks B8 and B15 execute trip commands upon relay operation toward the associated breakers CB-5 and CB10.

Again, the B8 Brick was already in place as a part of the BUS-1 protection.

## 2.8 LINE-5 zone

(Figure 9.)

Three Bricks (B15, B11 and B17) are connected to a line relay, D30 Distance Protection System [7] in this example, in order to interface the zone currents (CT-17 and CT-18) and voltages (VT-8). The B17 Brick may interface the line disconnect switch if appropriate, and Bricks B15 and B11 execute trip commands upon relay operation toward the associated breakers CB-10 and CB7.

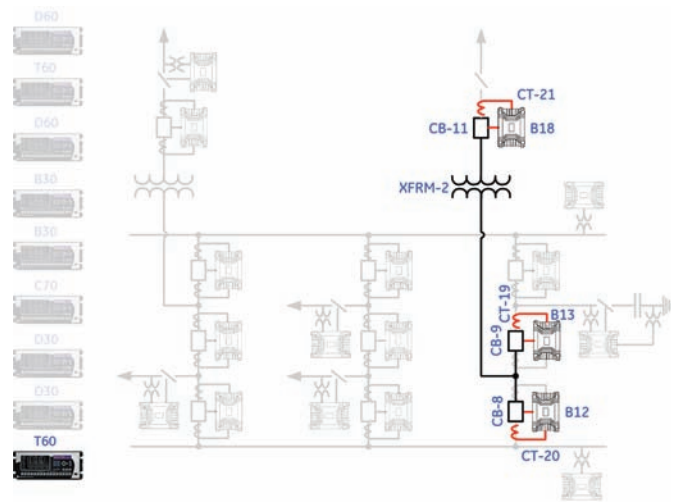
Again, the B15 and B11 Bricks were already in place as a part of the LINE-4 and BUS-2 protection.

## 2.9 XFRM-2 zone

(Figure 10.)

Similarly to XFRM-1, the second transformer protection employs the T60 Transformer Protection System [4] connected to Bricks B12, B13 and B18 with the application of tripping breakers CB-8, CB-9 and CB-11, accordingly; and for the measurement of current signals CT-20, CT-19 and CT-21, respectively.

Again, the transformer zone can be stretched from bushing CTs calling for extra Bricks at the transformer. Yet another Brick may be connected to interface voltage for power metering.

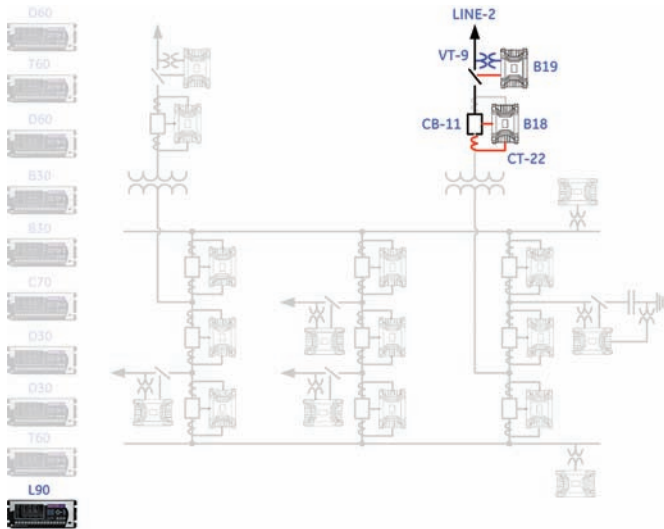


**Figure 10.**  
*Transformer 2 differential protection example*

## 2.10 LINE-2 zone

(Figure 11.)

The second transmission line protection employs the L90 Line Current Differential Protection System [8] connected to Bricks B18 and B19 to obtain the zone current (CT-22 from B18), voltage (VT-9 from B19), and executing the trip command toward CB11 via B18.



**Figure 11.**  
Line 2 differential protection example

## 3. Summary of Zone Protection Applications

The presented example substation uses 10 relays. This is natural as the presented substation incorporates 10 tripping zones given the number and position of the breakers. Extra relays may be deployed to accommodate stand-alone breaker failure (C60 [3]) or provide protection for transformers spanning their tanks rather than breakers (T60 [4] or T35 [9]), or alternatively one may provide separate protection for transformer leads (B30 [5]). These extra relays may be patched toward the existing Bricks to get their signals and execute commands as required.

The application involves 19 Bricks to cover the major signal clusters in the switchyard. In practice more Bricks may be needed if some of the CTs are free-standing CTs and cannot be wired back to the breaker Bricks, if stand-alone Bricks are deployed to interface disconnect switches, or when more potential points are available and metering is required for the transformer windings.

At minimum two Cross Connect Panels are needed to land and organize the Brick and relay cables, and to make associations between relays and Bricks.

Table 1 below summarizes the cross connections between relays and Bricks.

Zone	IED	Merging Units (Bricks)																			Comments
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	
Line 1	D60	x	x																		CT-1, VT-1 for protection, trip and reclose for CB-10
Line 2	L90																		x	x	CT-22, VT-9 for protection, trip and reclose for CB-11
Line 3	D60				x	x	x														CT-5, CT-6, VT-2 for protection, trip and reclose for CB-3 & CB-4
Line 4	D30								x							x	x				CT-15, CT-16, VT-7 for protection, trip and reclose for CB-5 & CB-10
Line 5	D30										x					x		x			CT-17, CT-18, VT-8 for protection, trip and reclose for CB-7 & CB-10
XFRM 1	T60		x	x	x																CT-2, CT-3, CT-4 for protection, trip CB-1, CB-2 & CB-3
XFRM 2	T60												x	x					x		CT-19, CT-20, CT-21 for protection, trip CB-8, CB-9 & CB-11
Cap Bank	C70									x					x	x					CT-13, CT-14, VT-5 for protection, trip for CB-6 & CB-9
Bus 1	B30			x					x	x	x										CT-7, CT-8, CT-9, VT-4 for protection, trip for CB-2, CB-5 & CB-6
Bus 2	B30					x		x				x	x								CT-10, CT-11, CT-12, VT-3 for protection, trip for CB-4, CB-7 & CB-8
Total	10	1	2	2	2	2	1	1	2	2	1	2	2	2	1	2	1	1	2	1	An average each Brick feeds 1.58 IEDs. With stand alone BF, 11 more BF IEDs (C60) are needed – in such a case each Brick feeds 2.16 IEDs on average.

**Table 1.**  
List of IEDs and association of functions for the substation of Figure 1



## 4. Breaker Failure Protection

Once the wiring between the relays and switchyard equipment has been eliminated, the Breaker Failure function remains as the last major application wherein extensive wiring is required to exchange critical signals.

Two signaling paths are required for Breaker Failure protection: initiation by relays tripping a given breaker, and tripping surrounding breakers should the associated breaker fail. The latter task may be seen as cumbersome, involving a variable number of breakers depending on the application. The task of BF tripping, however, can be unified by observing that all zones of protection that normally trip a given breaker contain all of the breakers that need to be tripped upon breaker failure.

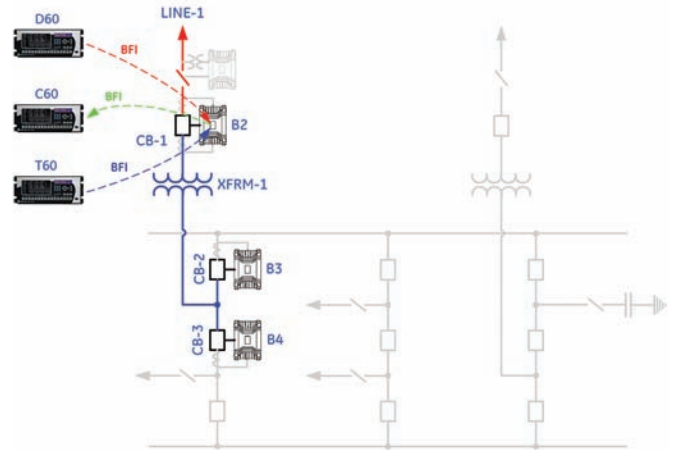
In general, the BF initiation and tripping can be accomplished in three ways:

1. By using traditional copper wiring. This solution is practiced today, and may be a requirement during a retrofit when some of the protection zones are implemented utilizing the process bus solution, while the remaining portion is hard-wired. Naturally, this approach is scalable and poses low risk as the existing workforce is more than familiar with the approach. The drawback is in lower savings due to keeping some copper wiring in the control house.
2. By using peer-to-peer signaling between digital relays over the station LAN (GOOSE). This approach is used today and is maturing relatively quickly with configuration and test tools emerging, and with fundamental issues being worked out, such as isolation and testing.
3. By using merging units as natural “mailboxes” to exchange the BF related signals. The remainder of this section describes this novel but simple concept.

The HardFiber system provides a fast, deterministic means for peer to peer messaging which is based on a fundamental premise of protective relaying: that critical signals need to be exchanged primarily between IEDs within the same zone or adjacent zones. The Shared I/O feature [1] uses the Brick itself as a “mailbox” to exchange these messages and can support several types of messaging: one-to-one, one-to-many, many-to-one and many-to-many. By design, Shared I/O signals are confined to the zones in which they operate. The benefit of this approach is that these signals can never be compromised due to activities (configuration, testing) occurring in other parts of the substation, supporting the concept of scalability – additions or modifications to other zone would not call for re-engineering, re-configuration or re-testing of other zones.

Refer once again to the example system and focus on the CB-1 breaker. A C60 relay has been added to implement Breaker Failure protection for CB-1 (Figure 12). According to the principles of protective relaying, any protections that trip CB-1 will also initiate breaker failure; in this case the D60 and the T60 must send breaker failure initiate to the C60. If the C60 relay subsequently detects that CB-1 has failed, all breakers in the zones adjacent to CB-1 must be opened. Note that these breakers are under the direct control of the D60 and T60 relays.

With reference to Figure 12, the D60 and T60 relays are connected to the B2 Brick. They will send a BFI flag to this Brick. This flag will arrive simultaneously with the trip command for CB-1, and will be reflected back to the all the relays connected to the B2 Brick before the breaker even starts to open. At this point in time the initiating relay (assume the D60), the other relay for the zone that overlaps at the breaker (T60), and the stand-alone BF relay (C60) have been informed a BFI had been issued for CB-1.



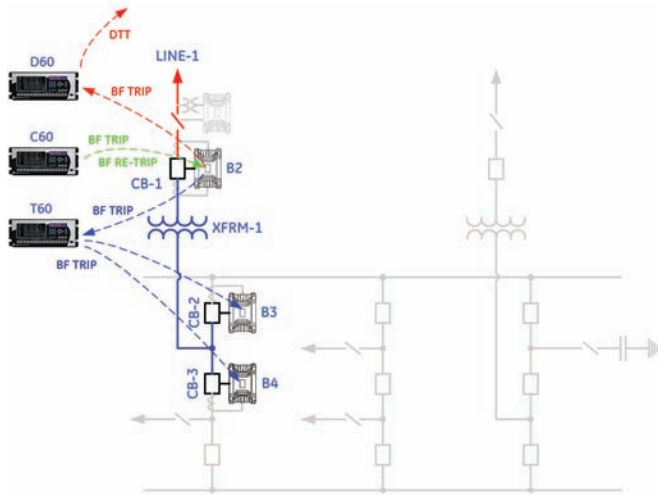
**Figure 12.**  
*BF initiate scenario for CB-1*

At least one of these relays (the C60 in this example) has the BF function enabled and starts monitoring the CB-1 breaker. Assume now that the breaker fails to open. With reference to Figure 13 the C60 relay issues a BF Trip command, communicated via the B2 Brick to both the D60 and T60 relays. The relays are configured to execute the breaker fail trip command by tripping all breakers surrounding their zones and – possibly depending on the protection philosophy – initiating BF for those breakers. Therefore, the T60 relay will trip and lockout CB-2 and CB-3 via the B3 and B4 Bricks, respectively. A non-volatile, latching output contact is provided within each Brick for the purpose of providing a breaker lockout. The D60 relay, in turn, will send a Direct Transfer Trip (DTT) to the other end(-s) of the line.

By examining Figures 12 and 13 four important observations can be made:

1. The BF configuration is very simple. Almost no settings are required if one uses properly prepared setting templates.
2. The scheme is universal and will work for any type of station and for any zone of protection, with integrated or stand-alone BF function. As the Shared I/O points are programmable, exceptions can easily be handled.
3. The BF initiate and BF trip signaling paths are locally contained. These signals are not published across the entire station potentially causing false operations, or burdening the network.

- The scheme is inherently robust. To issue a trip in the first place the tripping relay needs to communicate with the breaker Brick – as such it is always capable of sending the BFI to that Brick. To perform a BF function the BF relay needs to communicate with the breaker Brick to obtain the current data – as such it is always able to receive the BFI and send the BF Trip signals back.



**Figure 13.**  
BF trip scenario for CB-1

There may be a concern about using Brick B2 to route the breaker failure signals due to its proximity to the failed breaker. This represents a very low, albeit non-zero risk. However an alternate Brick could be chosen to eliminate this risk. For instance the breaker failure signals could as easily be routed via Brick B1 (associated with the VT). This would require that a digital core from this Brick be assigned to the C60 – entailing the placement of one additional patch cord at the cross connect panel.

## 5. Conclusions

This paper has explains the meaning of scalability as it relates to process bus solutions, and identifies the need for scalability for such systems.

Practical process bus solutions should be free from the problems of scale: systems with 10, 100 or 1000 devices should be equally robust and manageable. Unrealistic solutions may appear reasonable when sketched for a few devices. The ability to scale up, be deployed gradually, and remain naturally aligned with traditional protection principles, is what differentiates practical solutions from conceptual sketches.

The paper demonstrates natural scalability and flexibility of one particular solution, the HardFiber system [1].

The analyzed solution scales naturally owing to the following:

- Rational definition of the merging unit.
- Dedicated point-to-point connectivity.
- Simple and robust time synchronization.
- Separation and independence of the Brick's digital cores when interfacing with multiple relays.

The sample substation described in this paper uses a variety of relay models to cover all of the protection zones. No process bus solution can be considered complete and scalable unless it addresses every practical protection application (distance, line current differential, bus, transformer, capacitor bank, feeder, breaker failure, etc.).

This paper also illustrated that the HardFiber system is scalable because it does not depart from the proven signal routing topologies that have been employed within substations for decades. HardFiber merely integrates and standardizes the interface between the relays and the primary equipment resulting in protection systems that are simpler to design, install, and maintain. The HardFiber process bus solution can be implemented for any one zone of protection in the substation, or all zones of protection. Each zone of protection can be converted to process bus independent of any other zones, as work resources and equipment outages can be scheduled.

## 6. References

- [1] HardFiber System Instruction Manual, GE Publication GEK-113500.
- [2] D60 Line Distance Protection System, Instruction Manual, GE Publication GEK-113482.
- [3] C60 Breaker Protection System, Instruction Manual, GE Publication GEK-113479.
- [4] T60 Transformer Protection System, Instruction Manual, GE Publication GEK-113492.
- [5] B30 Bus Differential System, Instruction Manual, GE Publication GEK-113476.
- [6] C70 Capacitor Bank Protection and Control System, Instruction Manual, GE Publication GEK-113480.
- [7] D30 Line Distance Protection System, Instruction Manual, GE Publication GEK-113481.
- [8] L90 Current Differential Protection System, Instruction Manual, GE Publication GEK-113488.
- [9] T35 Transformer Protection System, Instruction Manual, GE Publication GEK-113491.

# unmatched...



**D90Plus** Line Distance Protection System

The most advanced line distance protection system in the market, GE Multilin's **D90Plus** delivers maximum performance, flexibility and functionality. Designed as a true multifunction device, the **D90Plus** eliminates the need for external devices reducing system complexity, commissioning time and capital costs.

Featuring advanced automation and control, dedicated digital fault recording, comprehensive communications including IEC61850, and an extensive local HMI, the **D90Plus** represents the next benchmark in protective relaying.



Digital Energy  
Multilin

# First IEC 61850 Process Bus Installation at American Electric Power (AEP)

John F. Burger, American Electric Power  
Bogdan Kasztenny, GE Digital Energy

Early July American Electric Power (AEP) commissioned its first IEC 61850 Process Bus installation with GE Merging Units (HardFiber Bricks) and Universal Relays. This live system tryout involves twelve HardFiber Bricks, a total of 2.7km (1.7mi) of outdoor fiber cables, D60 and C60 relays, and associated cross connect panels. The system is connected to traditional iron-and-copper instrument transformers, status signals and control outputs in the switchyard.

Here are a few photos from this exciting project. Papers describing installation details and presenting operational experience will follow in the near future.



Site survey

Factory Acceptance Testing

Installation

Commissioning

The HardFiber System is simple to use, and required no GE assistance or training during the first deployment of this new technology.



Relay panel with three UR relays and two redundant HardFiber Patch Panels (top and bottom). No copper signaling in the back of the relays.

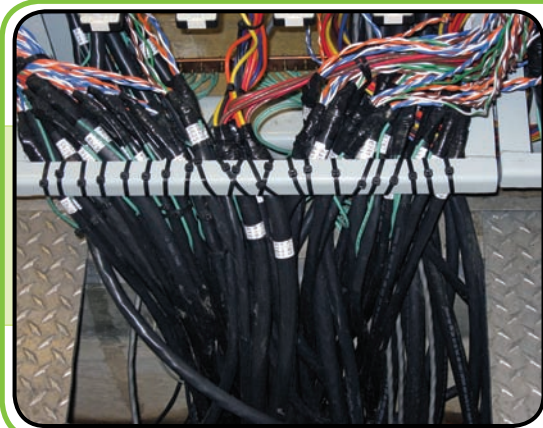


The 345kV switchyard of the AEP Corridor substation spans 300m (1000ft). HardFiber Bricks have been installed in the upper portion of the yard.



HardFiber Bricks in the process of installation on the single-pole-mechanism breaker marshalling box (left) and underneath the breaker cabinet (right). The connectorized copper cables are ready for wiring to the primary equipment. Duplicate HardFiber Bricks deployed for each measuring point in the yard.

A HardFiber Brick mounted directly on a breaker support structure.



Before and after: traditional cabling to a relay panel position (left); outdoor fiber cabling for the process bus HardFiber panel (right).

# Engineering Quick Tip: Enabling Peer-to-Peer Communications



GOOSE Messaging is a means for transmitting data from one device to another. There are three different types of GOOSE messaging systems available in the UR family of relays.

The first is GSSE or UCA2.0 GOOSE. GSSE consists of one dataset of 64 digital points. Similarly, Fixed GOOSE consists of one dataset of 64 digital points that are transmitted for direct transfer trip and/or blocking schemes. However, there are some changes added to it by the IEC 61850 standard.

Configurable GOOSE consists of 8 datasets of 64 bits, that can be either digital or analog values. Figure 1 shows the differences in GSSE, Fixed and Configurable GOOSE Datasets.

GSSE (original UCA 2.0)	Fixed GOOSE	Configurable GOOSE
- One dataset consisting of 64 digital points transmitted upon power-up, state change, and time	- One data set consisting of 64 digital points transmitted upon power-up, time, and state change	- Digital and analog
- State changes detected every protection scan (approximately every 2 seconds)	- State changes detected every protection scan (approximately every 2 seconds)	- Eight block of 64 items
	- One block and one name	- Support tag based on VLAN's
	- Supports VLAN's	- Supports priority
	- Supports priority	- First block: if only 16 digitals will be sent at power up, time, and within 6ms after change in state
		- If digital and analog will transmit every 100 msec upon digital change of state
		- Data set 2 through 8 will transmit at power up, time, and within 100ms after digital state change or analog exceeds deadband or state

Figure 1.

Fixed GOOSE in the UR family of relays is a messaging system based on the UCA 2.0 communications model with an IEC 61850 twist. Fixed GOOSE is defined by the IEC 61850 standard and is used to transfer digital data from one IEC 61850 compliant device to another IEC 61850 device. These devices can include intelligent electronic devices (IEDs) such as, protection devices, meters, control systems, DCS, etc...

Configurable GOOSE is also defined by the IEC 61850 standard, however, it is used to send both digital and analog values between two IEC 61850 compliant devices. The data is structured differently in Configurable GOOSE and the differences can be seen in Figure 1.

Both Fixed and Configurable GOOSE use what is known as a publisher-subscriber communication relationship. The publisher-subscriber relationship refers to the way data is transmitted and received by a device. Once one of the GOOSE messaging systems is enabled, the 'publisher' will continually generate packets of data on the network (publish), regardless of whether any devices are actually 'listening' to it. In this type of relationship, most of the burden is placed on the subscriber (receiver) side.

When configuring Fixed GOOSE in the UR relays, there are several settings that must be configured before communications will function. The settings for both the transmitting and receiving devices are shown in Figure 2.

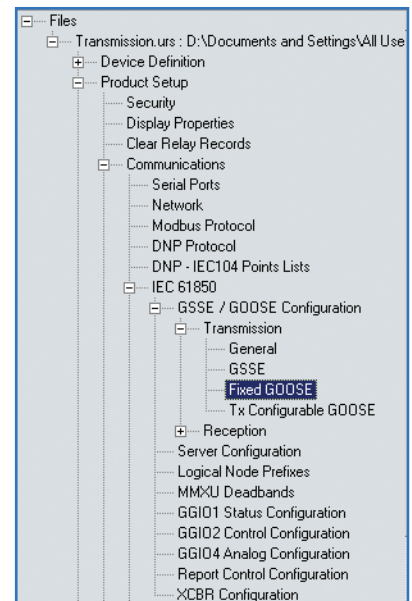
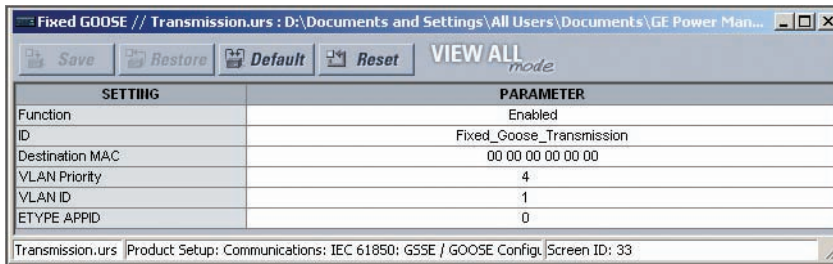


Figure 2.  
Menu structure for configuring the Transmission of Fixed GOOSE



**Figure 3.**  
Settings required to configure the Transmission of Fixed GOOSE

The settings found under the Product Setup – Communications- IEC61850 – GSSE / Goose Configuration – Transmission - Fixed Goose need to be configured properly, to ensure that the transmission device is generating the necessary data packets.

\*Note, when using a MultiLink Ethernet Switch, the VLAN ID should be set to 1, see Figure 3.

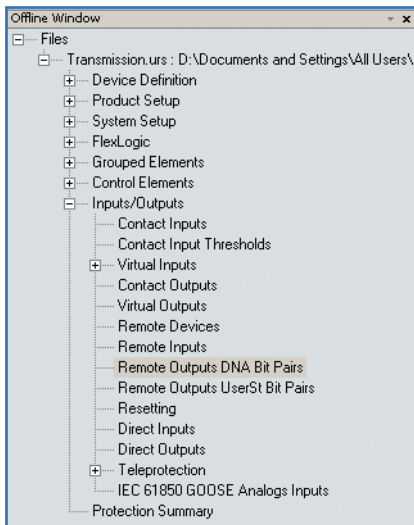
Once the transmit function is enabled, the device will begin to generate data packets on to the network. These packets will include the Device ID, as set above, the 64 available bits (Remote Outputs, shown below) and the time for retransmission of the next packet.

The remote output bits are split into two different categories, each consisting of 32 bits, used to transmit digital data from one device to another. The categories are called DNA bits and User ST bits. All 64 bits are identical and there is no difference in terms of which bits are used for the transmission of the data. They are configured under Inputs/Outputs – Remote Outputs DNA Bit Pairs or User ST Bit Pairs.

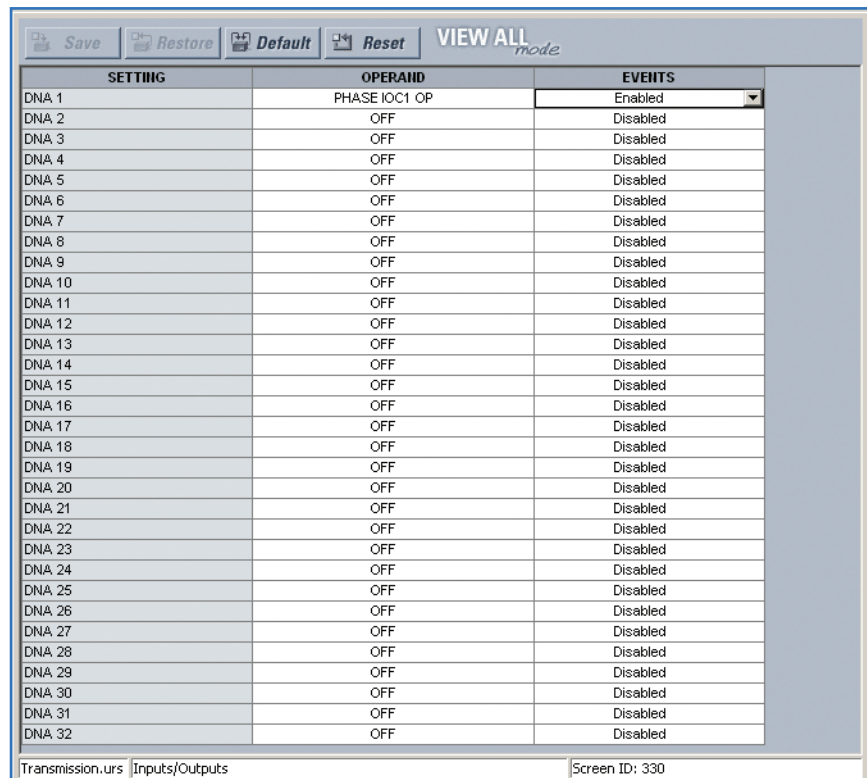
Device ID	64 Remote Output Bits	Time to retransmit
-----------	-----------------------	--------------------

In the following example, we will use the operation of a Phase IOC (50P) element to drive the Remote Output DNA Bit Pair 1. As this element operates, the DNA bit will be asserted.

**Figure 4.**  
Fixed GOOSE packet structure



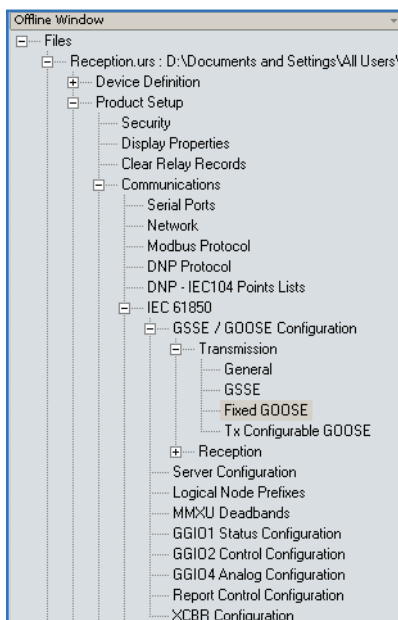
**Figure 5.**  
Menu structure for configuring Remote Output Bits



**Figure 6.**  
Settings required for Remote Outputs - DNA Bit Pairs

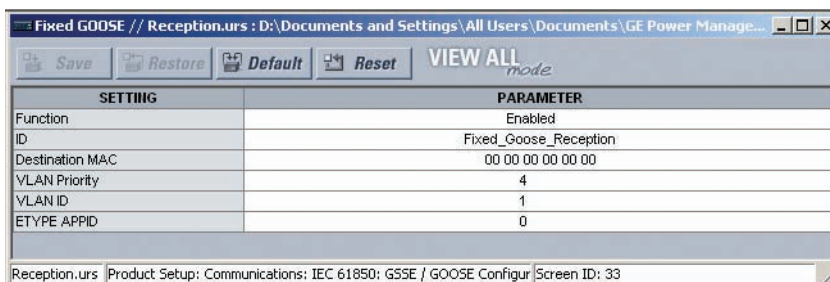
The reception device (subscriber) must now be configured. There are several settings that must be configured in order for the Fixed GOOSE to operate correctly. The first of these settings is the same as the transmission side and they are found under Product Setup – Communications- IEC 61850 – GSSE / Goose Configuration – Transmission - Fixed Goose. See Figure 7.

Once the function is enabled and the device is given a unique ID, the actual reception of the data needs to be configured. These settings are found under Inputs / Outputs – Remote Devices. The Remote Devices are a listing of the devices (Publishers) that the Receiving Device (Subscriber) could receive data from.

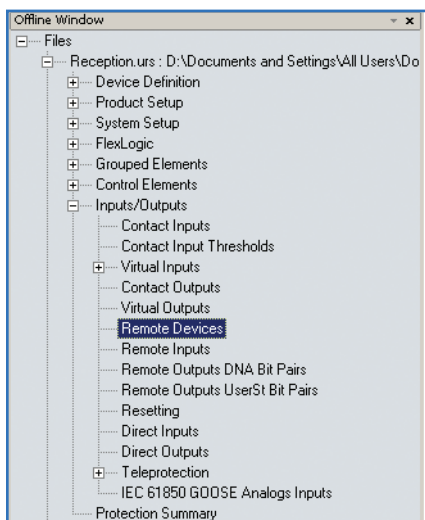


**Figure 7.**  
Menu structure for configuring the Reception of Fixed GOOSE

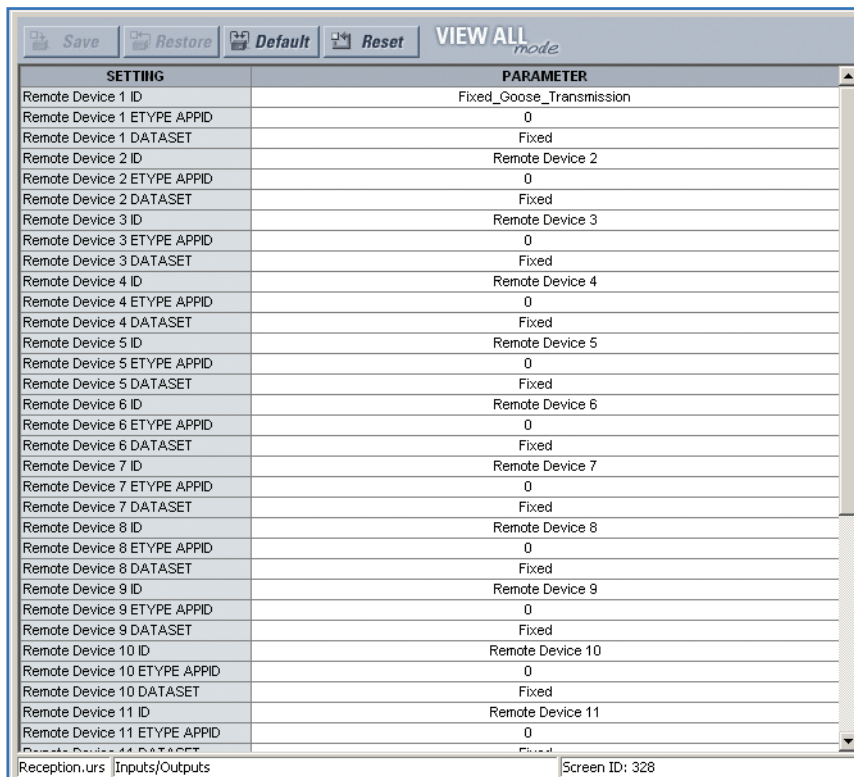
Up to 16 Remote Devices may be configured for the reception of Fixed GOOSE messages. It is critical that the name of the transmitting device (Publisher) is identical in the Remote Device list of the Receiving Device (Subscriber).



**Figure 8.**  
Settings required for configuring the Reception of Fixed GOOSE



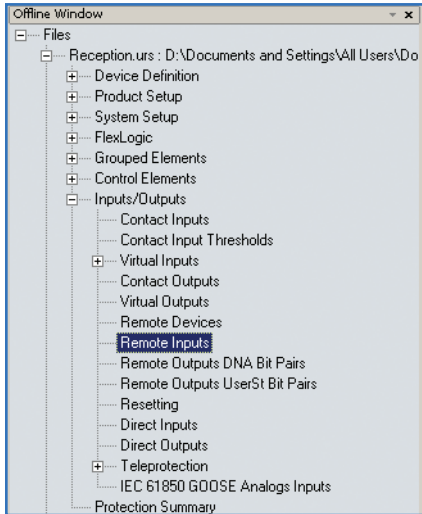
**Figure 9.**  
Menu structure for configuring Remote Devices (Subscriber)



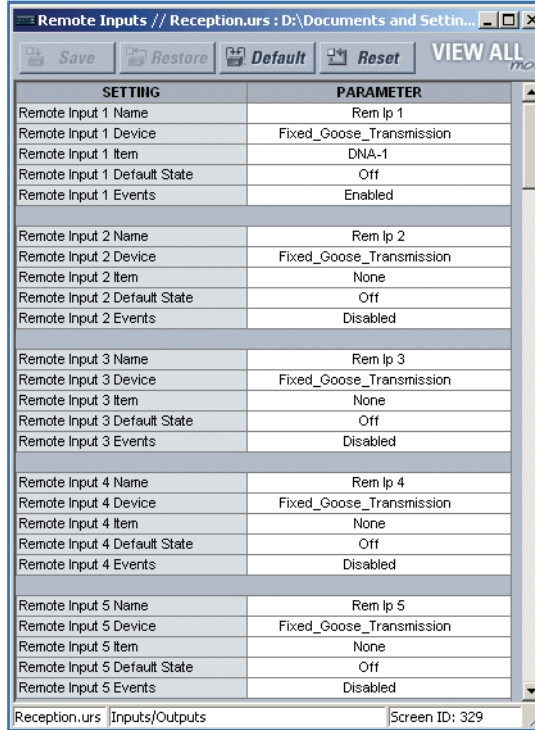
**Figure 10.**  
Settings required for Remote Devices



The final step for configuration is to define which data bit(s) the receiving device will use from the transmitting device. This is done under Inputs / Outputs – Remote Inputs. See Figures 10 & 11 for details.



**Figure 11.**  
Menu structure for configuring the Remote Inputs



**Figure 12.**  
Settings required for Remote Inputs

Only the devices that are configured under the Remote Devices setting can be selected as transmission devices under Remote Inputs. Once a remote output bit is selected from that transmitting device, the receiving device will begin to look for packets from that device.

The time to retransmit that is part of the packet from the transmitting device is used by the receiving device to determine the health of the transmitter. After the first packet is received from the transmitting device, a counter is started within the device. The receiving device then begins to look for packets from that device within that time period. If 5 of these packets are missed, the receiver will declare that the device is offline and no longer transmitting. There are several operands available that can be used to determine the current status of the transmitting device. The status of the Remote Device(s) and Remote Inputs can be seen under Actual Values – Status – Remote Device Status and Remote Inputs.



## Featured Innovation

### IEC 61850 Process Bus Now Available

#### Multilin HardFiber™ System

GE Digital Energy - Multilin

[www.GEMultilin.com/HardFiber](http://www.GEMultilin.com/HardFiber)

The Multilin HardFiber™ System eliminates the need for thousands of copper wires in a substation and replaces them with a few fiber optic cables. By eliminating thousands of copper wires used for signaling and monitoring in electrical substations, utilities can save up to 50% of protection and control installation and maintenance costs, while at the same time increasing worker safety and power system reliability.



### Powerful, Dynamic Range Test Equipment

#### CMC 356

Omicron

[www.omicronusa.com](http://www.omicronusa.com)

OMICRON Electronics proudly introduces the CMC 356, uniquely designed for the modern requirements of protection & control testing and commissioning/maintaining substations. It exceeds expectations with powerful, wide dynamic range current sources (1mA resolution, 6x32A or 3x64A or 1x128A rms @ max 6x430VA). Unmatched versatility: test high-burden, electro-mechanical relays (or an entire panel of them), up to 12 additional low-level analog outputs, and optional: IRIG-B sync for End-to-End or PMU testing, IEC 61850 device testing, or EnerLyzer (analog measurement) with just one test set.



### Wireless Solar-Friendly Long Range SCADA

#### MDS SD4

GE Digital Energy - MDS

[www.GEMDS.com](http://www.GEMDS.com)

The MDS SD4 is the next generation in licensed narrowband radios at 400 MHz. With a software-defined modem and an optimized hardware platform, this radio is the ideal platform for both current and future deployments of SCADA and telemetry systems. Monitor and control oil & gas wells, compressor stations, pipelines, fluid storage tanks, pole tap transformers, circuit reclosers, capacitor banks, plus many other applications.



### InfraCAM™ SD Low Cost, High Quality

#### InfraCAM™ SD IR Camera

Flir

[www.flir.com](http://www.flir.com)

The new and improved SD model of the InfraCAM gives you more image storage, more image quality and more post-processing capabilities! Detect hot spots, avoid electrical failures, increase safety and even prevent fires.

- Stores 1,000 Radiometric JPEG Images
- Razor-Sharp Thermal Image Quality
- Long 7 Hour Battery Life
- Ultra-Portable, Weighs Just 1.2 lbs.
- Built-in Laser LocatIR™, Removeable SD Memory Card
- Includes New Powerful QuickReport Software
- Easy-to-operate Large 3.5 Full Color LCD
- Find Problems Faster & Easier





## Cost Effective Sub-transmission Protection

### L30 – Line Differential System

GE Digital Energy - Multilin

[www.GEMultilin.com/L30](http://www.GEMultilin.com/L30)

The Multilin L30 is a next-generation integrated protection, control, and monitoring device for sub-transmission and distribution feeder and cable protection applications. Based on a proven algorithm for sensitive and secure line current differential protection, the Multilin L30 delivers a truly cost effective solution with the advanced capabilities customers expect from Multilin's Universal Relay (UR) platform of protection & control devices.



## New Generation in Transformer Condition Monitoring

### MULTITRANS - Multi Tank Gas Analyser

kelman

[www.kelman.co.uk](http://www.kelman.co.uk)

Dissolved Gas Analysis (DGA) has been recognized as the most important tool for transformer condition assessment. Reliable on-line DGA allows invaluable insight into the condition of transformers and gives real benefits. The MULTITRANS is a new generation of on-line DGA equipment based on the TRANSFIX. MULTITRANS can monitor up to three separate oil tanks, and is ideal for monitoring a bank of three single-phase transformers that are situated close to each other.



## Your Ultimate Solution for High-Accuracy Asset Management

### GeoXH™

Trimble

[www.trimble.com](http://www.trimble.com)

For high-accuracy GIS data collection and asset relocation, the Trimble® GeoXH™ handheld from the GeoExplorer® 2008 series is the ultimate integrated solution. Engineered with Trimble H-Star™ technology, the GeoXH handheld delivers the accuracy you need when you need it. It is ideal for electric and gas utilities, water and wastewater services, land reform projects, and other applications where on-the-spot positioning is crucial.



## Motion Measurement for all Circuit Breakers

### TDR900 Circuit Breaker Test System

Doble Engineering Company

[www.doble.com](http://www.doble.com)

Performs timing functions for up to 4 breaks per phase with motion measurements for any circuit breaker. The TDR900 is a state-of-the-art Circuit Breaker Test System engineered to test all types of circuit breakers. The TDR900 provides efficient and accurate performance measurements for circuit breakers. It allows simple to complex testing of circuit breakers using a single, rugged, field-portable instrument.





## Uninterrupted Intelligence

### 750kVA SG Series Digital Energy UPS

GE Digital Energy

[www.GEDigitalEnergy.com/pq](http://www.GEDigitalEnergy.com/pq)

GE Digital Energy's 750kVA SG Series Digital Energy UPS offers a maximum efficiency greater than 94 percent, in a 30 percent smaller footprint. Operating in a double conversion mode with true continuous on-line VFI (voltage and frequency independent) operation, the 750kVA uses GE's Intelligent Energy Management™ (IEM), which automatically determines the most efficient mode of operation for the Redundant Parallel Architecture™ (RPA) system.



## True-rms Utility Multimeter Designed for Basic Electrical Tests

### Fluke 113 Utility Multimeter

Fluke

[www.fluke.com](http://www.fluke.com)

The Fluke 113 Utility Multimeter gives utility users the means to quickly and easily do basic meter set and reconnect testing. This meter is simple-to-use and has the features needed to repair most electrical problems. The Fluke 113 has significant improvements over Fluke's original 7-600, and other utility multimeters. Using the Fluke VCHECK™ LoZ low impedance measurement function, users can simultaneously test for voltage or continuity.



## Reduce Arc Hazard with Switch Rated Plug

### Decontactor Series

Meltric

[www.meltric.com](http://www.meltric.com)

Meltric's Decontactor Series products are a combination electrical plug and receptacle and disconnect switch in the same device. Decontactors are designed to allow users to safely make and break connections under full load even in overload and short circuit conditions. Protection from exposure to live parts and arc flash is ensured at all times during the operation of the device.



## Rugged and Portable Insulation Resistance Testers

### Insulation Resistance Testers

Megger

[www.megger.com](http://www.megger.com)

To be fully in conformance with the most modern testing requirements, Megger offers a family of the highest quality insulation testers at voltages above 1 kV. At the core of high-voltage testing, 5 kV, the MIT510/2 and MIT520/2 afford the highest level of quality testing along with prime safety, convenience and portability.



# Upcoming Events



CIGRÉ

Aug 24 - 29

Paris, France



CIGRÉ is a permanent, non-governmental and non-profit international association, founded in France in 1921. Issues related to planning and operation of power systems, design, construction, maintenance and disposal of HV equipment and plants, protection of electrical systems, telecontrol and telecommunication equipment and data management are at the core of CIGRÉ's mission. Electricity markets, regulation and environment are also within the field of concern of CIGRÉ.

Palais des Congrès  
[www.cigre.org](http://www.cigre.org)

**Visit GE Digital Energy - Multilin, at stand #74**

### GE Digital Energy Papers to be Presented

- Considerations for process bus deployment in real-world protection and control systems: a business analysis
- A practical IEC61850-9-2 process bus architecture driven by topology of the primary equipment
- Constraints and solutions in testing IEC 61850 process bus protection and control systems

### Other GE Papers to be Presented

- Intelligent Power System Protection Data Management and its Practical Impact Upon Protection & Automation Lifecycle Management Strategies
- Control Centre Applications of Integrated WAMS-based Dynamics Monitoring and Energy Management Systems

UTC Canada

Sept 8-11

Winnipeg, Manitoba, Canada



The Utilities Telecom Council (UTC) Canada Conference and Exposition targets core transport technology issues from a Canadian utility perspective. As these systems evolve, utility telecom professionals are faced with upgrading, while continuing to meet the fundamentals, ensuring the safety and reliability of core utility services.

Fairmont Hotel  
[www.utc.org/events/upcoming](http://www.utc.org/events/upcoming)

**Visit GE Digital Energy - Multilin, Lentronics, & MDS at Booths #305/307**

ASGMT

Sept 15-18

Houston, Texas, United States



The ASGMT is the largest gas measurement school in the United States devoted to natural gas measurement, pressure regulation, flow control and measurement related arenas. The purpose of the ASGMT, the sponsoring associations, and the operating companies within the petroleum and natural gas industry, is to provide instruction on technical subjects for people in the industry.

In addition to the classes, 108 leading industry manufacturers will exhibit their wares. This offers an exceptional opportunity to see the latest product offerings available to the natural gas industry.

Mariott House Westchase  
[www.ASGMT.com](http://www.ASGMT.com)

**Visit GE Digital Energy - MDS at booth #105**

# Upcoming Events



IEEE IAS PCIC

Sept 22-24

Cincinnati, Ohio, United States



The PCIC is an international forum for the exchange of electrical applications and technology related to the petroleum and chemical industry. The annual PCIC conference is rotated across North American locations of industry strength to attract national and international participation. User, manufacturer, consultant and contractor participation is encouraged to strengthen the conference technical base.

Cincinnati Hilton Hotel  
[www.ieee-pcic.org](http://www.ieee-pcic.org)

### GE Digital Energy - Multilin Papers to be Presented

- Cost Efficient Applications of Bus Transfer Schemes Utilizing Microprocessor Base Relaying Technology
- Safety First: The Detection of Downed Conductors and Arcing on Overhead Distribution Lines

### Other GE Papers to be Presented

- Revisions to IEEE 1068: Standard for the Repair of AC Electric Motors in Process Industries
- Large Motors Made to IEC/Zone1 and NEC/CEC Division 1: Are They the Same?
- API 546 3rd Edition – Making Synchronous Machines Better

### GE Hospitality Suite – Hyatt Regency

- Nightly from Sunday, September 21st through Tuesday, September 23rd – Suite 2108

UTC Regional Events

Sept / Oct

Various Locations



UTC Regional meetings are a great way to stay connected with peers in your region that are facing similar issues as you. Regional meetings offer educational programs covering current hot topics such as Smart Grid Vision and Applications, Interoperability for Utilities, and more. Check the individual region programs for detailed information.

[www.utc.org/events/upcoming](http://www.utc.org/events/upcoming)

Region 2 - Sept 18-19

Visit us at Tables 5/6, Sheraton Hotel  
 Atlantic City, New Jersey, United States

Region 1 - Sept 25-26

Visit us at Tables 13/14, Crowne Plaza Hotel  
 Nashua, New Hampshire, United States

Region 3 - Oct 1

Fredericksburg Hospitality House & Conference Center  
 Fredericksburg, VA, United States

NRWA

Oct 5-8

Reno, Nevada, United States



The National Rural Water Association is a non-profit federation of state Rural Water Associations. The association provides support services to state Associations who have more than 25,735 water and wastewater systems as members.

Grand Sierra Resort & Casino  
[www.nrwa.org/evLForum.htm](http://www.nrwa.org/evLForum.htm)

Visit GE Digital Energy - MDS at booth #430

# Upcoming Events



ISA

Oct 14-16

Houston, Texas, United States



ISA Expo is an exhibition for promoting Automation and Control Technology. ISA is a leading, global, nonprofit organization that is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems. Based in Research Triangle Park, North Carolina, ISA develops standards; certifies industry professionals; provides education and training; publishes books and technical articles; and hosts the largest conference and exhibition for automation professionals in the Western Hemisphere. ISA is the founding sponsor of The Automation Federation.

Reliant Center  
[www.isa.org](http://www.isa.org)

**Visit GE Digital Energy - at booth #1406**

WPRC

Oct 20-23

Spokane, Washington, United States



The Western Protective Relay Conference (WPRC) is an educational forum for the presentation and discussion of broad and detailed technical aspects of protective relaying and related subjects. This forum allows participants to learn and apply advanced technologies that prevent electrical power failures.

Spokane Convention Center  
<http://capps.wsu.edu/conferences/wprc/>

### **GE Digital Energy - Multilin Papers to be Presented**

- Detection of Incipient Faults in Underground Medium Voltage Cables
- Design & Implementation of an Industrial Facility Islanding and Load Shed System
- Impact of CT Errors on Protective Relays – Case Studies and Analysis
- Bus Protection for Impedance Grounded Systems
- Requirements for a Fault Recording System
- Ensuring Correct Settings when Applying Power Swing Blocking in Distance Relaying Applications

### **Seminar - The Dream of Process Bus Realized**

This seminar introduces and explains a commercially available, practical process bus system: the HardFiber system from GE. The HardFiber system is built on UR relays and open standard IEC 61850. Experience with or knowledge of IEC 61850 is not required – 61850 is “under the hood”, allowing users to focus on protection and control, rather than on bits and bytes.

- Monday, October 20th – 8:00 am to 4:00 pm
- Spokane Center – Registration is free and lunch is included
- Register today at [www.gemultilin.com/WPRC2008-1](http://www.gemultilin.com/WPRC2008-1)

### **GE Hospitality Suite – Red Lion Hotel at the Park – Room 5109/5110**

- Nightly October 20th, 21st and 22nd – 6:00 pm to 10:00 pm

# Upcoming Events



MIPSYCON

Nov 4-6

St. Paul, Minnesota, United States



This conference provides electric utility engineers and consultants the opportunity to stay abreast of today's power system technology. The conference emphasizes the unique challenges faced by electric utilities in the Midwest United States. The conference also serves as a forum for power engineers to meet their colleagues from other utilities to discuss mutual concerns. Topics include substations, utility industry futures, delivery systems, project management, relaying, distribution automation and distributed resources.

**Continuing Education & Conference Center**  
[www.cce.umn.edu/mnpowersystems](http://www.cce.umn.edu/mnpowersystems)

**Seminar - Radisson Hotel Roseville - Salon C**

- Monday, November 3rd - 8:30 am to 4:00 pm (Lunch included) Earn PDH credits

**GE Digital Energy Hospitality Suite - Radisson Hotel Roseville - Salon D**

- Monday, November 3rd - 6:00 pm to 10:00 pm

IEEE CONCAPAN

Nov 19 - 21

City of Guatemala, Guatemala



CONCAPAN is IEEE's biggest technology event in Central America. During this event, technical conferences in electric energy, telecommunications, computing, management engineering and other areas related to electric and electronic engineering will take place.

**Westin Camino Real International Convention Center**  
[www.concapan2008.org](http://www.concapan2008.org)

**Visit GE Digital Energy at stand #72**

POWER-GEN

Dec 2 - 4

Orange County, California, United States



Now celebrating its 20th Anniversary, POWER-GEN International offers information on power generation market trends and strategies, as well as sessions covering environmental issues, power plant technology, renewable energy, distributed generation/on-site power, operations and maintenance, and more.

**North/South Building, Orange County Convention Center**  
<http://pgi08.events.pennet.com/fl//index.cfm>

**Visit GE Digital Energy - at booth #4600**



# Advanced Training



## GE Multilin 2008/2009 Course Calendar

Comprehensive Training Solutions for Protection, Control and Automation

### SCHEDULED COURSES IN NORTH AMERICA

Courses for 2008/2009	Tuition*	CEU Credits	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
Fundamentals of Modern Protective Relaying	\$2,400	2.8	15-18		17-20		19-22			20-23			20-24	
MM300 2 Days Hands-on	\$1,800	1.4								6-7		1-2		
Introduction to the IEC61850 Protocol	\$1,800	2.1		6-8				2-4				15-17		
Distribution Protection Principles & Relaying	\$1,800	2.1	3-5						10-12					
Motor Protection Principles & Relaying	\$1,800	2.1		1-3		2-4			2-4				6-8	
UR Platform	\$1,800	2.1			3-5			16-18		15-17		22-24		17-19
UR Advanced Applications	\$3,000	3.5		27-31							11-15			
Energista Viewpoint Monitoring	\$600		19		6				13	8				

All North American courses are located in Markham, Ontario, Canada unless otherwise stated

\*Tuition quoted in US dollars

### SCHEDULED COURSES IN EUROPE

Courses for 2008/2009	Tuition*	CEU Credits	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG
UR Advanced Applications	\$2,400	2.8	22-26		10-14		16-20				18-22			21-25
UR Platform	\$1,800	2.1	17-19		5-7		11-13				13-15			16-18
Distribution Protection Principles & Relaying	\$1,800	2.1							10-12				7-9	
Fundamentals of Modern Protective Relaying	\$2,400	2.8				15-18						8-12		
Motor Management Relays	\$1,800	2.1							24-26				21-23	
F650 Platform	\$1,800	2.1		6-8		3-5				20-22		23-25		
Introduction to the IEC61850 Protocol	\$1,800	2.1		9-10						23-24				

All European courses are located in Bilbao, Spain unless otherwise stated

\*Tuition quoted in US dollars

Course dates are subject to change. Please visit our website at [www.GEMultilin.com/training](http://www.GEMultilin.com/training) for the most up-to-date schedule.

# Protection & Control Journal

## Content Index

### Articles

<b>Design &amp; Implementation of an Industrial Facility Islanding and Load Shed System</b> .....	7
Mark Adamiak, Bernard Cable	
<b>Business Considerations in the Design of Next Generation Protection and Control Systems</b> .....	15
Bogdan Kasztenny, Jeff Mazereeuw, Steven Hodder, Rich Hunt	
<b>An Architecture and System for IEC 61850 Process Bus</b> .....	19
Bogdan Kasztenny, David McGinn, Wei Wang, Roy Mao, Drew Baigent, Nadejda Nazir, Steven Hodder, Jeff Mazereeuw	
<b>The Advantages of IEC 61850 Process Bus Over Copper-Based Protection and Control Installations</b> .....	29
Steven Hodder, Rich Hunt, Dave McGinn, Bogdan Kasztenny, Mark Adamiak	
<b>Detection of Incipient Faults in Underground Medium Voltage Cables</b> .....	35
Bogdan Kasztenny, Ilia Voloh, Christopher G. Jones, George Baroudi	
<b>Using 6-Sigma Methodology to Review System Security</b> .....	45
Bruce Barnett	
<b>Security Architecture for IEC 61850-9-2</b> .....	51
Daniel Thanos, Bogdan Kasztenny	
<b>Testing and Commissioning Protection &amp; Control Systems Based On IEC 61850 Process Bus</b> .....	59
Dave McGinn, Steven Hodder, Bogdan Kasztenny, Rich Hunt	
<b>Scalability of IEC 61850 Process Bus Solutions</b> .....	67
Dale Finney, Bogdan Kasztenny	

### Advertiser Listings

<b>Megger</b> .....	2
www.Megger.com	
<b>GE Multilin</b> .....	6, 14, 75, 91
www.GEMultilin.com	
<b>Virelec</b> .....	13
www.virelec.com	
<b>GE Power Quality</b> .....	44
www.GEIndustrial.com/750	
<b>MP Husky</b> .....	34
www.mphusky.com	
<b>ESAC</b> .....	58
www.esac.com	
<b>Omicron</b> .....	92
www.omicronusa.com	

### Product Listings

<b>Multilin HardFiber System</b> .....	82
GE Multilin	
<b>CMC 356</b> .....	82
Omicron	
<b>MDS SD4</b> .....	82
GE MDS	
<b>InfraCAM™ SD IR Camera</b> .....	82
Flir	
<b>L30 – Line Differential System</b> .....	83
GE Multilin	
<b>MULTITRANS</b> .....	83
kelman	
<b>GeoXH</b> .....	83
Trimble	
<b>TDR900 Circuit Breaker Test System</b> .....	83
Doble	
<b>750kVA SG Series Digital Energy UPS</b> .....	84
GE Digital Energy	
<b>Fluke 113 Utility Multimeter</b> .....	84
Fluke	
<b>Decpmtactor Series</b> .....	84
Meltric	
<b>Insulation Resistance Testers</b> .....	84
Megger	

### Trade Shows/Conferences

<b>Cigre</b> .....	85
Paris, France	
<b>ASGMT</b> .....	85
Houston, Texas, United States	
<b>IEEE IAS PCIC</b> .....	86
Cincinnati, Ohio, United States	
<b>UTC Canada &amp; Regional Events</b> .....	85 & 86
Various Locations	
<b>NRWA</b> .....	86
Reno, Nevada, United States	
<b>ISA</b> .....	87
Houston, Texas, United States	
<b>WPRC</b> .....	87
Spokane, Washington, United States	
<b>MIPSYCON</b> .....	88
St. Paul, Minnesota, United States	
<b>IEEE CONCAPAN</b> .....	88
City of Guatemala, Guatemala	
<b>POWER-GEN</b> .....	88
Orange County, California, United States	

# Switch Your Frame of Mind

Reduce substation communication costs by up to 70%

A breakthrough in networking hardware that can reduce up to 70% of your total communications costs, the Multilin UR Switch Module is a fully managed, embedded Ethernet switch for the Universal Relay (UR) family. This advanced, 6-port Ethernet Switch eliminates the need for external, rack-mounted switches and significantly reduces the total costs associated with hardware, installation, wiring and troubleshooting, required for today's traditional substation communication architectures.

For a mere \$200 more\*, when compared to the cost of selecting the redundant Ethernet option on a UR, the Multilin UR Switch Module delivers full station management, monitoring, and control functionality, with complete communications redundancy.

\* USD List Price



UR Ethernet Switch Module



Digital Energy  
Multilin



# Change Is A Good Thing.

*When we decided to expand our testing capabilities, we knew things would change.*

Transformation is often a natural progression. In our world you either change with the times or you are gone with the wind.

For years we have been leading the way, and now with more expansions, new products and a larger scope of resources our test systems reach new heights... providing new solutions for your testing needs. For more information, please call or visit our website.



**CMC 256**

Protection Relay & Meter Testing  
(including IEC 61850)



**CPC 100**

Transformer & Substation Testing



**CPC with CP TD1**

Power Factor Testing



**CPC with CP CU1**

Impedance Measurements



**FRAnalyzer**

Frequency Response Analyzer



**CT Analyzer**

**World Leader in Innovative Power System Testing Solutions**

**OMICRON**



[www.omicronusa.com](http://www.omicronusa.com)

email: [info@omicronusa.com](mailto:info@omicronusa.com)

OMICRON electronics Corp. USA • Houston, Texas • Tel: +1 713 830-4660, +1 800-OMICRON  
OMICRON electronics Asia Limited • Hong Kong • Tel: +852 2634-0377  
OMICRON electronics GmbH • Austria • Tel: +43 5523 507-0