Protection & Control Journal

8th Edition

$19.95 USD

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

Advertising Opportunities

Learn more about how to reach today's protection and control professionals.
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

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.

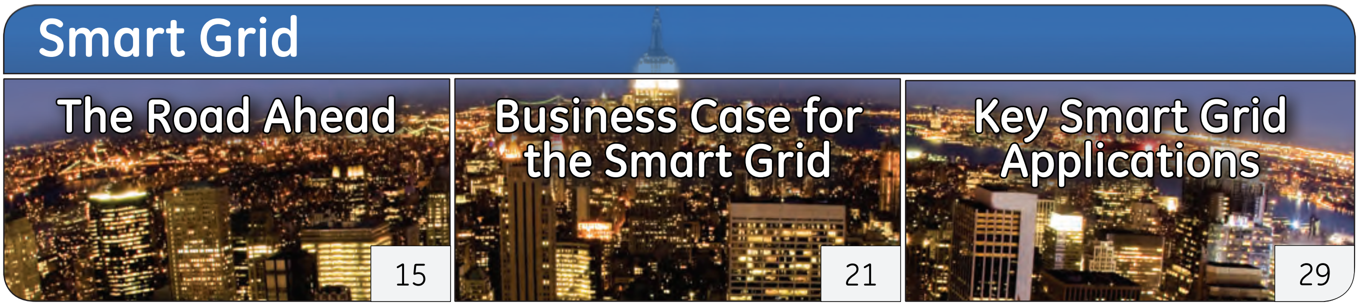
The Protection & Control Journal is published by GE Digital Energy, 215 Anderson Avenue, Markham, Ontario, Canada, L6E 1B3.

www.GEDigitalEnergy.com

ISSN 1718-3189

Protection & Control Journal
8th Edition

Contents



Richard Hunt
Market Development Leader

What is the Smart Grid Really?

Anyone working in the electric utility industry, and in fact most of the general public, have heard something about "Smart Grid".

Utilities are undertaking Smart Grid initiatives, and every vendor in the electric utility area now seems to have a Smart Grid "solution". Even service suppliers that are traditionally outside the utility industry are now, (if you believe the television commercials), Smart Grid providers.

But what is Smart Grid really? Is it just an Advanced Metering Infrastructure (AMI) with "smart" communicating meters? Is it integrating renewable or distributed energy sources with the existing utility grid? Is it real-time pricing for customers to make informed decisions? Or is Smart Grid really something else?

To define Smart Grid, lets look at some challenges facing the present electric utility grid. The grid is designed to be operationally reliable while serving peak demand. And with a reliability of 99.97%, the electric grid is very successful at meeting this goal. The demand for electricity is such, however, that an outage can easily result in losses to customers of $1 million dollars a minute. In the United States alone, the demand for electricity is growing with an anticipated growth of 2% per year. This works out to a 50% increase in demand over the next 20 years. And there is a growing focus on the environmental costs of this huge demand for electricity. So, in short, the present utility system must serve a growing demand, while increasing reliability, with little or no increase in environmental impact.

A cursory look shows that the present model of the electric grid really can't meet these challenges. The traditional centralized model for generation and distribution of power requires huge capital investments in generating plants, transmission lines, and distribution networks, to improve reliability and to meet the requirements for new demand. Let's not forget, our current system is also aging, with 60% to 70% of the transformers, transmission lines, and circuit breakers nearing the end of their usable life. So clearly, something must change for utilities to afford the capital costs of new construction. So what is Smart Grid, and how will it meet these challenges? Smart Grid is a new model for the utility grid, with a vision towards operating the utility system as efficiently as possible with connectivity to real-time data through advanced communications, while integrating more efficient methods of producing electricity. A Smart Grid has several characteristics, including the ability to self-heal from disturbances, being secure against attack, providing power quality for future needs, accommodating all power generation and energy storage options, and having an intelligent communications infrastructure. Smart Grid solutions can be implemented at any level of the utility system: generation, transmission, distribution, and power consumers.

From this definition of Smart Grid, one can list many Smart Grid solutions. Much talked about solutions include thin-film solar panels to provide local generating capacity, smart appliances to reduce residential demand during peak load periods, microgrids to efficiently integrate distributed renewable resources, and wide-area protection schemes that make the transmission system self-healing and secure. Which solution, or set of solutions, to adopt is going to be based on the operating needs, philosophy, history, and regulatory considerations of a specific utility. The best step a utility can take right now, is to define and build a framework that supports future use of real-time data and information technology.

The framework for Smart Grid must meet four major requirements. It must be cost effective, both in terms of capital costs, and in operating and maintenance costs. It must provide useful information, such as pricing of electricity, in real-time. It must provide this useful information where it is needed, whether at a substation, a control center, or at a customer's residence. Finally, whatever steps are taken to develop a framework for Smart Grid, they must respect the traditional operating requirements for the utility system: reliability, safety, and the use of industry standards to support open solutions.

While there is a lot of talk about what Smart Grid is, and what a Smart Grid framework could be, it's good to know about solutions that have been done. Look at the real and practical solutions described in this issue of the Protection and Control Journal. Developing a business case for Smart Grid solutions. Designing the communications infrastructure to transmit information between utilities and customers. Making sure your distribution management system can actually operate a distribution system that includes distributed energy resources, intelligent outage management information, and self-healing capabilities. Using the new data from synchrophasors to improve the operation of the transmission system. And the use of innovative technology to replace copper wiring in protection and control systems, making traditional substations more efficient and reliable to build and operate.

The more you know about the multi-faceted Smart Grid, the better equipped you will be as you journey towards realizing your own smarter solutions.

Application of Phasor Measurement Units for Disturbance Recording

Mark Adamiak, Rich Hunt
GE Digital Energy

1. Introduction

This paper looks at the specific application of Phasor Measurement Units (PMUs) for disturbance recording, with a special emphasis on wide area cross-triggering of recording PMUs during events. Disturbance recording, or long-term recording of phasor data, provides valuable information when analyzing wide area disturbance and power swings in the utility system. The newly approved NERC PRC-002 and PRC-018 standards require the installation of disturbance recording equipment at strategic points on the power system. The value of this equipment is only realized when discrete records are captured simultaneously at all points on the power system, to provide a complete snapshot of a specific event. Traditional recorders rely on local triggers to capture the data, however, an individual recorder may not trigger for a specific event, or may trigger in a different time frame than other recorders on the system, and not capture valuable data. A practical challenge is adding the disturbance recording function to existing substations and relay systems.

Ongoing projects, such as the Eastern Interconnect Phasor Project, promote the installation of PMUs to provide real time measurement of the state of the power system, by streaming highly accurate synchrophasors at a high sampling rate. The PMUs are generally installed at the same strategic substations that require disturbance recording. In addition, today's digital relays (such as a line distance relay or current differential relay) are capable of synchronous phasor measurements. In addition to streaming data to a centralized database, PMUs may have the ability to record data at the PMU based on local trigger conditions. The record may include synchrophasor data as well as additional analog values and digital status. This recorded data meets the disturbance recording requirements set by NERC. The paper discusses the applicability of synchrophasor data to disturbance recording, and the capabilities of PMUs to capture the appropriate data.

This paper also discusses practical aspects of using the IEEE Synchrophasor standard communications in conjunction with IEC61850 communications for wide area cross-triggering of PMUs. Also discussed are communications channels requirements and expected performance of cross-triggers. Other disturbance recording applications exist in the industrial domain, such as motor starting failure events on large motors. Synchronized measurements provide the ability to correlate the failure with other events in the industrial process. This paper will discuss industrial applications of PMUs.

2. Phasor Measurement Units and recording

In the context of this paper, disturbance recording is defined as recording of phasor or RMS values of data over a long period of time. Disturbance recording is intended to show the response of the power system and equipment due to power system faults, such as an out-of-step condition, as opposed to power equipment faults, such as a short circuit. The time interval for these "long term" events can range from 1 second (in the case of a fault and high-speed reclose) to many minutes (in the case of system oscillations). The fast sample rates (30 to 60 phasors per second) of today's synchrophasors-based disturbance recording devices can be used to analyze both power system faults and the more traditional power equipment faults. The term Dynamic Swing Recorder (DSR) is also often used to describe a device that captures disturbance data over a long period of time. A more complete description of these terms is available in [1].

NERC has issued Standard PRC-002-1 entitled: Define Regional Disturbance

Monitoring and Reporting Requirements. Section R3 specifically addresses criteria for dynamic disturbance recording, including location of recorders, electrical quantities to record, recording duration, and sampling rate. The NERC standard essentially states that DSRs are to be situated at key locations, are to record voltage, current, frequency, megawatts and megavars for monitored elements, and are to record the RMS value of electrical quantities at a rate of at least 6 records per second.[2]

The Regional Reliability Councils (RCCs) of NERC are responsible for refining these standards for a specific operating region. By reviewing the standards as interpreted by some of the RCCs, it is possible to provide a good overview of disturbance monitoring requirements.

Location of DSRs. DSRs are to be located at key substations for the power system. Key substations are generally defined as transmission substations with significant connected generation, large transmission substations (containing 7 or more transmission lines), transmission substations that interconnect to another regional authority or company, at major load centers (such as load centers greater than 2500 MW), or where undervoltage load shedding schemes are implemented.

Electrical quantities to record. The NERC requirement is to record voltage, current, and frequency, with the ability to derive or record megawatts and megavars for each monitored element. The minimum requirements defined by the RCCs are:

- Bus voltages: at least one three-phase measurement per voltage level, with two measurements per voltage level recommended
- Frequency: at least one frequency measurement for every voltage measurement
- Three-phase line currents for every critical line
- Megawatts and megavars, three-phase, for each monitored line.

Record length. Disturbance recording, and DSRs, are intended to capture longer term power system faults. DSRs therefore require longer record times. The recording length is typically specified as 90 to 180 seconds, including 30 seconds of pre-fault data. DSR records may be require to automatically extend in length when additional triggers occur during recording.

A second option for record length is to use continuous recording. A DSR therefore always captures data for all analog channels, and typically stores the last 30 days of data. The challenge with continuous recording is to manage the large amounts of data. Also, it is important to be able to retrieve the key pieces of the data to analyze an event.

Triggers. Triggers are necessary to initiate recording for the typical DSRs that have a discrete record length. For continuous recording, triggers provide markers into the key pieces of data during an event. The ability to "share" triggers between multiple sites is also necessary in order to capture a wide-area view of an event.

There are many types of triggers available in DSRs, including:

- Magnitude triggers, on voltage, current, frequency, real power, reactive power and apparent impedance
- Rate-of-change triggers, on voltage, current, frequency, real power, reactive power and apparent impedance
- Harmonic content triggers, on a specific harmonic frequency, or on total harmonic distortion
- Delta frequency triggers
- Contact triggers, such as breaker operation or communications channel operations
- Symmetrical components trigger

Frequency rate-of-change and voltage rate-of-change triggers are the most commonly applied triggers. Previous papers at Various conferences have suggested that real power rate-of-change triggers also have the sensitivity and selectivity to trigger recording for power system faults, without triggering recording for power equipment faults.[1] Impedance triggers are an interesting case for this paper. Impedance triggers will only operate when the center of impedance of a power system fault is close to the location of the DSR. However, there are some events, such as load encroachment, or when the DSR is located close to the center of impedance, where this trigger can capture valuable data.

Sampling rate. The minimum sampling rate required by NERC is 6 Hz. However, a higher sampling rate, such as 30Hz or 60Hz, provides a more accurate picture of the measured electrical quantities during a power system event, providing frequency responses up to 15 and 30 Hz respectively.

The requirements for disturbance recording as described in this section are a synthesis of the requirements as defined by a few of the Regional Coordinating Councils of NERC. For complete details of an individual RCC, please see [3], [4], [5].

The term Dynamic Swing Recorder is a generic term to describe any device capable of capturing RMS or phasor values of electrical quantities. While typically a DSR is simply a function available in a digital fault recorder, other devices may have the capability to capture this type of data. One such device is the Phasor Measurement Unit (PMU), a device that measures synchrophasors, a highly accurate time-synchronized phasor measurement. The typical PMU is designed to communicate these synchrophasors to system operators for real-time control of the power system.

However, some PMUs have the ability to trigger on system anomalies, and record synchrophasor data, to meet the requirements of disturbance recording.

2.1 PMU as disturbance recorders

An AC waveform can be mathematically represented by the equation:

$$x(t) = X_m \cos(\omega t + \theta)$$

where X_m = magnitude of the sinusoidal waveform,

ω = $2 * \pi * f$ where f is the instantaneous frequency

ϕ = Angular starting point for the waveform

Note that the synchrophasor is referenced to the cosine function. In a phasor notation, this waveform is typically represented as:

$$\overline{X} = X_m \angle \theta$$

Since in the synchrophasor definition, correlation with the equivalent RMS quantity is desired, a scale factor of $1/\sqrt{2}$

must be applied to the magnitude which results in the phasor representation as:

$$\bar{X} = \frac{X_m}{\sqrt{2}} \angle \theta$$

Adding in the UTC-based absolute time mark, a synchrophasor is defined as the magnitude and angle of a *fundamental frequency* waveform as referenced to a cosine signal (Figure 1).

In Figure 1, time strobes are shown as UTC Time Reference 1 and UTC Time Reference 2. At the instant that UTC Time Reference 1 occurs, there is an angle that is shown as "$+\theta$" and, assuming a steady-state sinusoid (i.e. – constant frequency), there is a magnitude of the waveform of X_1. Similarly, at UTC Time Reference 2, an angle, with respect to the cosine wave, of "$-\theta$" is measured along with a magnitude or X_2. The range of the measured angle is required to be reported in the range of $\pm\pi$. It should be emphasized that the synchrophasor standard focuses on steady-state signals, that is, a signal where the frequency of the waveform is constant over the period of measurement.

In the real world, the power system seldom operates at exactly the nominal frequency. As such, the calculation of the phase angle, θ, needs to take into account the frequency of the system at the time of measurement. For example, if the nominal frequency of operating at 59.5Hz on a 60Hz system, the period of the waveform is 16.694ms instead of 16.666ms – a difference of 0.167%.

The captured phasors are to be time tagged based on the time of the UTC Time Reference. The Time Stamp is an 8-byte message consisting a 4 byte "Second Of Century – SOC", a 3-byte Fraction of Second and a 1-byte Time Quality indicator. The SOC time tag counts the number of seconds that have occurred since January 1, 1970 as an unsigned 32-bit Integer. With 32 bits, the SOC counter is good for 136 years or until the year 2106. With 3-bytes for the Fraction Of Second, one second can be broken down into 16, 777,216 counts or about 59.6 nsec/count. If such resolution is not required, the C37.118 standard allows for a user-definable base over which the count will wrap (e.g. – a base of 1,000,000 would tag a phasor to the nearest microsecond). Finally, the Time Quality byte contains information about the status and relative accuracy of the source clock as well as indication of pending leap seconds and the direction (plus or minus). Note that leap seconds (plus or minus) are not included in the 4-byte Second Of Century count.

2.2 Synchronized phasor reporting

The IEEE C37.118 revision of the IEEE 1344 Synchrophasor standard mandates several reporting rates and reporting intervals of synchrophasor reporting. Specifically, the proposed required reporting rates are shown in Table 1 below.

System Frequency Reporting Rates	50 Hz		60 Hz				
	10	25	10	12	15	20	30

Table 1.
Synchrophasor reporting rates

A given reporting rate must evenly divide a one second interval into the specified number of sub-intervals. This is illustrated in Figure 2 where the reporting rate is selected as 60 phasors per second (beyond the maximum required value, which is allowed by the standard). The first reporting interval is to be at the Top of Second that is noted as reporting interval "0" in the figure. The Fraction of Second for this reporting interval must be equal to zero. The next reporting interval in the figure, labeled T_0, must be reported 1/60 of a second after Top of Second – with the Fraction of Second reporting 279,620 counts on a base of 16,777,216.

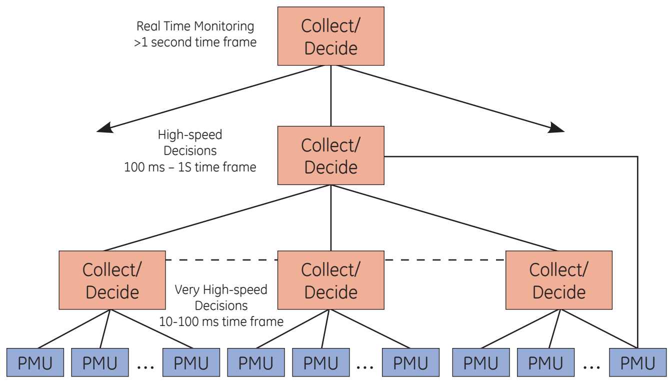


Figure 2.
Synchrophasor reporting hierarchy

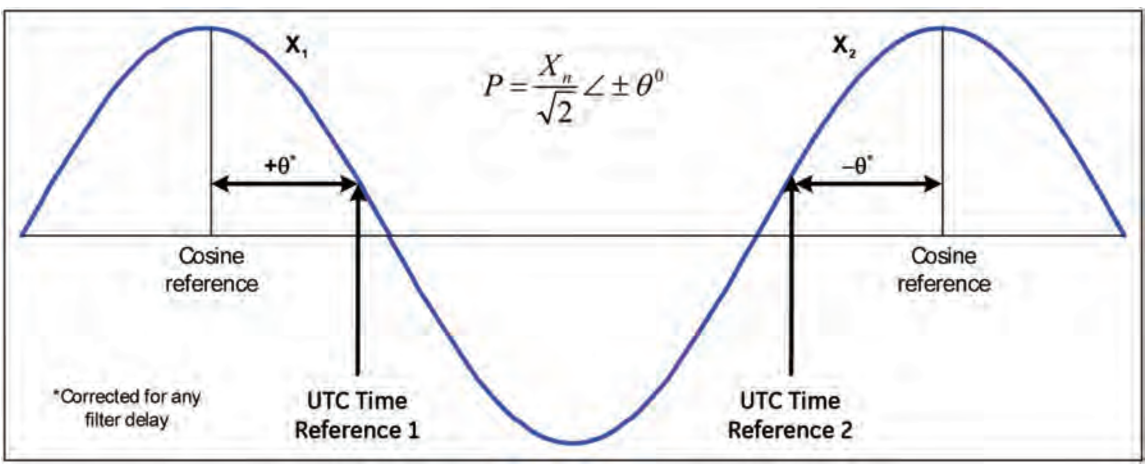


Figure 1.
Synchrophasor definition

2.3 PMU Distributed Architecture

The Synchrophasor standard and associated communication protocol was designed to aggregate data from multiple locations. As each dataset is transmitted synchronous to top of second and as each transmitted dataset contains a precise absolute time stamp, the data aggregation function becomes a simple matter of combining sets of data with common time stamps. The "box" that performs this function is known as a Phasor Data Concentrator or PDC. In a "total" system, there will be a hierarchy of PDCs as shown in Figure 2. The hierarch is designed to support different performance criteria/data rates – depending on the application. With the assumption that higher-level PDCs operate at lower data rates, the data from the lower layer PDCs provides the most frequency resolution. Depending on type and number of PMUs installed in a substation, a substation-based PDC may or may not be required as this function can be integrated into the PMU.

A major advantage of Synchrophasor measurements compared to a normal DSR is that, as a result of standardization, data from multiple manufacturers can be seamlessly integrated. This is possible because the Synchrophasor standard requires that magnitude and phase angle errors resulting from magnetic and filter components be compensated in the final result.

Throughout North America, there exist today "pockets" of data concentration. Specifically, the Eastern Interconnect Phasor Project (now the North American SynchroPhasor Initiative – NASPI) has created a network of PMUs that span most of the eastern half of the continent. Data is being streamed at a rate of 30 phasors/ sec into a Super Phasor Data Concentrator as operated by TVA. Communication bandwidths in the order of 64,000 to 128,000 bits per second will be required – depending on the number of data items and the selected stream rate. At the receiving site, real-time visualization of the data is available. Additionally, the data is archived and can be retrieved to perform system dynamic analysis as well as forensic analysis for larger system events.

In as much as remote communications may be disrupted by an event, most PMUs/PMU Systems have the ability to locally store synchrophasor data based on a range of event triggers. Typical triggers include over/under frequency, rate of change of frequency, over/under voltage, over current, over/under power, and status change. Synchrophasor recording times in excess of 20 minutes can be obtained within the confines of existing PMU memories.

3. Wide Area Recording

The benefits of disturbance recording, or power swing recording, are already well established. The phasor data captured in these records are used to validate system models of the power system, validate the operation of system integrity protection schemes and wide area protection schemes, and to provide root-cause analysis of equipment operation during power system faults. Some typical uses for the data include identifying the impact on the system due to a loss of generation or loss of a significant transmission line. Another use for this data is to analyze the performance of distance relays due to power swings. [6],[7] In all of these cases, for proper analysis, the phasor data must be measured simultaneously at various points on the power system. By collecting and coordinating records from multiple locations, the engineer can evaluate the response of the system, and specific equipment, to a power system or power equipment fault. The challenge is to capture simultaneous recordings across the system.

The present method of disturbance recording is to use discrete recording equipment, and local triggers. DSRs are placed at key locations on the system. Each DSR is configured much like a protective relay: trigger criteria are specific for the location of the DSR. Therefore, a DSR will only create a record when a power system fault is observable at the location of the DSR. Therefore, the more remote a DSR is from the center of inertia of an event, the less likely the DSR will capture a record for an event. Also, local triggers are dependent on the propagation time of the event across the system. A common trigger for DSRs is rate-of-change of frequency. In one known case, full load rejection of a 1,100 MW generating station took approximately ½ second to propagate across the utility power system.[7] Local triggers will therefore be problematic in such a case. With discrete DSRs, and local triggers, records (such as for the load rejection example) may be created at different instances in time. An engineer must identify, retrieve, and combine the appropriate records from multiple devices. And this assumes that all the DSRs in use are accurately time synchronized, typically to Coordinated Universal Time using GPS clocks.

Wide area recording or wide area cross-triggering can solve some of these issues. Wide area recording creates one synchronized record across the power system when any local DSR triggers a recording. The challenges in a wide area recording system are similar to that of local recording, with the added complexity of communications channel time delays. The only wide area recording system presently available is a closed, proprietary solution. This solution links DSRs as part of a client-server software system. When one DSR triggers a recording, this DSR sends a message to the server. The server then sends a message to trigger a recording, with the same trigger time, on all other connected DSRs. This system solves communications channel delay by using a rolling data buffer to store data in the DSR. Once the recording is finished, the server then retrieves the records from all the DSRs. This system absolutely requires that each DSR is accurately time synchronized, to ensure the data in the individual records are in phase.

Wide area cross-triggering sends a cross-trigger command to other DSRs via communications when one DSR triggers for a power system fault. Wide area cross triggering has not been used, in part due to the challenges of communications, as the cross-trigger signal must be sent to multiple DSR locations simultaneously. Therefore, the complexity of communications is added to the same challenges in creating simultaneous records. However, the use of a PMU as the DSR can reduce these challenges.

In a typical DSR, although the records are time synchronized, there is no agreement among manufacturers as to how and when a measurement is made. However, when using a PMU as a DSR, the measurement is standardized and time synchronized per standard. Therefore, the trigger time of the record is not vitally important. The data from records captured at two different PMUs with different trigger times can be coordinated based only on absolute time.

The other challenge in wide area cross-triggering is sending the cross-trigger signal to multiple locations across the power system. This assumes an intact communication channel. Speed is not critical as long as the PMU can provide pre-trigger data memory. By setting the pre-event memory to be longer than the trigger and retrigger communication time, no data is ever lost. The IEEE Synchrophasor standard has, as part of the message format, a trigger signal that is typically sent as a PMU-to- PDC signal. Once in the PDC, logic is needed to receive the trigger signal and then to forward it to all PMUs connected to the detecting PDC. Once the signal is received by one PMU in a station, that PMU can issue a GOOSE message to trigger other data captures or execute controls in other devices in the substation. Figure 3 illustrates this architecture.

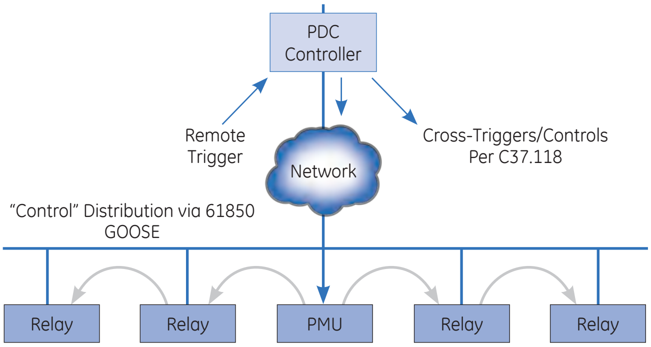


Figure 3.
Phasor measurement unit cross-triggering

3.1 The need for cross-triggering PMUs

PMU installations are normally designed to stream PMU data via communications to a centralized database that stores synchrophasors quantities for later analysis of the power system. This seems to eliminate the need for cross-triggering recording, as the data is readily available at a central location. However, the data is not necessarily available. As more devices, such as protective relays, can provide synchrophasors data, the less likely these devices will continuously stream data to the centralized database. The bandwidth of communications channels may limit data transmission, and data storage requirements may limit reception of data. Also, protection engineers may not have the same easy access to stored synchrophasors data as the system operations and system planning departments do.

In addition, for analysis of relatively local events, there may be the need to capture additional data beyond synchrophasors, such as power, power factor, and impedance. The cross-trigger signal can also be used to initiate recording in a traditional DSR as well.

4. Applications of PMU data for analysis

4.1 Large motors

In the industrial environment, many processes have start-up and shut-down times that are in the multi-second time frame and sometimes, problems occur that either abort a startup or initiate an undesired shut-down. Traditional oscillography, although high-resolution, is typically set to record data only during fault conditions and, as such, will not record the longer start-up or shut-down events. Moreover, most industrials will own neither a swing recorder nor an oscillograph. Synchrophasor capability in motor protection can enable data capture in these instances and can provide a high-resolution, long-term view of these events. In addition, with proper trigger settings, the effects of power system disturbances on plant processes can be observed.

4.2 AGC / SIPS analysis

System Integrity Protection Schemes (SIPS) is rapidly becoming a common occurrence in many utilities around the world. A SIPS event is usually a last ditch effort to prevent a complete power system shut down. It is very desirable to measure the effect of a SIPS action on the electric power grid. This measurement is most easily effected through the collection of synchrophasors across the system. Using the cross-triggering methodology previously described, the wide-ranging effects of a SIPS action can be observed and used to validate system studies and models.

One such scheme protects large multi-generator power plants against the severe disturbances that occur on transmission lines. Based on the disturbance severity, the typical results are intensive swings or loss of plant synchronism, which will lead into loss of the entire generation complex either by out-of-step protection, or unit shutdown by protective devices reacting to voltage dips at auxiliary buses. Wide area recording of synchrophasors allows the analysis of the power swing phenomena across the system, to verify the operation of the SIPS scheme.

4.3 Capacitor Bank Performance

Capacitor Banks are used to help maintain a flat voltage profile on the transmission system. Capacitor bank installation typically use some type of automatic control to switch in and switch out the capacitor bank. This switching operates on some criteria involving time of day, voltage magnitude, reactive power magnitude, or power factor. The performance of the capacitor bank is monitored at the system operations level by direct observation of the changes in the system voltage. Direct recording of the changes to local part of the system could provide some interesting insights into the impact of capacitor bank operation on the system voltage.

The primary data necessary to analyze the performance of a capacitor bank is the voltage magnitude and the reactive power flow. PMUs directly record the voltage and current synchrophasors, and can also record the real power, reactive power, power factor, and system frequency. Consider the arrangement of Figure 4. Rich Substation is a major load substation, with a switched capacitor bank that operates on voltage magnitude. Recording PMUs are installed at both Rich Substation and Mark Substation, a major transmission substation. The PMU at Rich Substation is configured to trigger a recording on operation of the capacitor bank controller. Both PMUs are configured to send a cross-trigger command via IEC61850 GOOSE messaging.

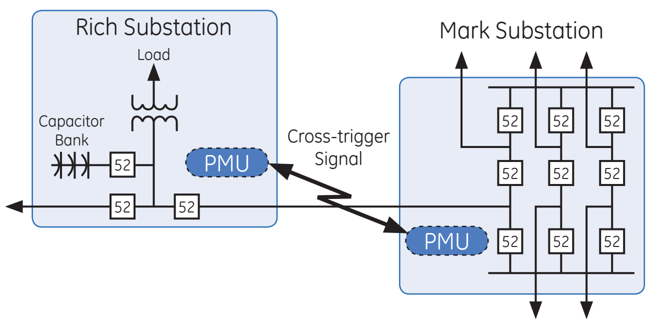


Figure 4.
PMU cross-trigger for capacitor bank operation

A voltage profile may look something like that of Figure 5, where increasing load drags the system voltage down. The voltage recovers after the capacitor bank is switched in.

Recording the data at both PMUs can provide some valuable information. The basic information includes the voltage magnitude at each bus. Once the capacitor bank is switched in, the data will show the impact on the voltage at each bus, the amount of overshoot on the voltage correction, and the time lag between capacitor switching and voltage correction at the remote bus. The end goal of using this type of data is to improve the efficiency of capacitor bank switching, to ensure that bank switching procedures result in the desired improvement in system voltage level.

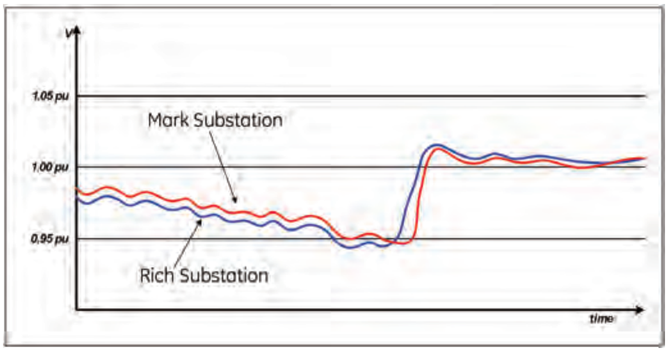


Figure 5.
Capacitor bank operation voltage profile

There are two advantages to using IEC61850 GOOSE messaging as the cross-trigger signal. The first advantage is the GOOSE message can be sent to one specific device or group of devices, or it can be sent to all devices on the system. In this example, GOOSE messages need only be sent between the two PMUs. The second advantage is the non-proprietary nature of IEC61850. There are two advantages to using IEC61850 GOOSE messaging as the cross-trigger signal. The first advantage is the GOOSE message can be sent to one specific device or group of devices, or it can be sent to all devices on the system. In this example, GOOSE messages need only be sent between the two PMUs. The second advantage is the non-proprietary nature of IEC61850.

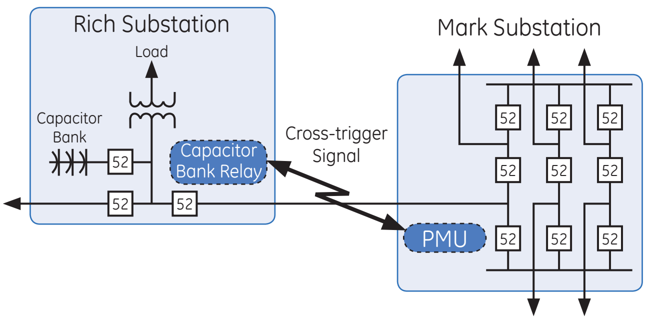


Figure 6.
Load substation without PMU

4.4 Capacitor Bank Performance

Underfrequency and undervoltage load shedding schemes are used to prevent system collapse. The typical scheme uses a local relay with a fixed threshold against voltage or current. A block of load is shed when the frequency or voltage drops below this threshold. Multiple thresholds are typically used to shed multiple blocks of load. The power system phenomenon that predicates the use of a load shedding scheme is a reduction in the system frequency or system voltage due to a significant imbalance between generation and load. At an individual device location, the apparent impedance will fluctuate in response to the changes in the system voltage and current.

Analysis of the performance of a load shedding scheme requires both verifying the performance of local devices, and verifying the performance system-wide. Recording synchrophasors in the substation, along with power flow and device data, can verify the local operation of the load shed devices, and the local impact on load. Capturing this data across the system can verify the performance of the load shed scheme system-wide. In addition, this information can be used to determined the center of inertia of the system during the event, and how close the system was to the voltage instability point.

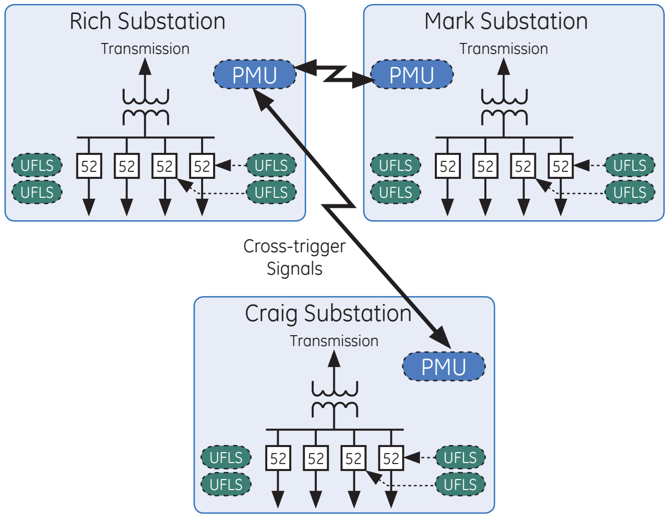


Figure 7.
Cross-triggers for load shedding analysis

4.5 Distance relay performance during small disturbances

Not all disturbances need to be a system-wide phenomenon to be of interest to study. Significant changes in voltage or current may cause the operation of a distance relay. Of special concern are distance relays that use a large over-reaching zone as remote backup of lines from the next station. Even small disturbances, such as the loss of a nearby generator, or heavy line loading, may cause the operation of this distance element. PMUs can be used to identify events where the apparent impedance of the line comes close to a tripping zone of the relay.

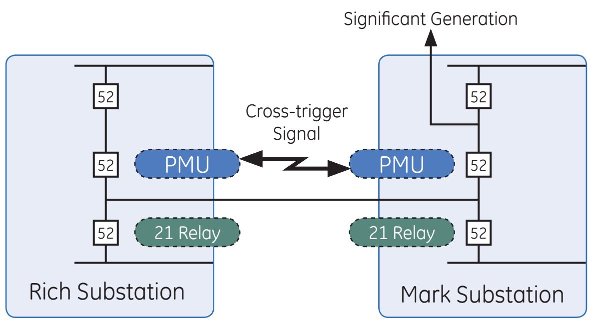


Figure 8.
Transmission line example

Consider the simple transmission system of Figure 8. There is significant generation located one bus away from Mark Substation. When this generation trips off, a small power swing occurs. This power swing may encroach into the relay operating zone for the relay at Rich Substation.

The data that is most interesting is the apparent impedance as seen by the distance relays at both ends of the line. This requires the recording of the current and voltage by both PMUs. In terms of the total power system, this disturbance may not be significant, and may not trigger criteria. However, the local PMUs can be configured to recognize the power swing conditions, and capture a recording. The cross-trigger signal can be an IEC61850 GOOSE message that is only received by these two PMUs. A big advantage of PMU data, is the synchrophasors data is always synchronized.

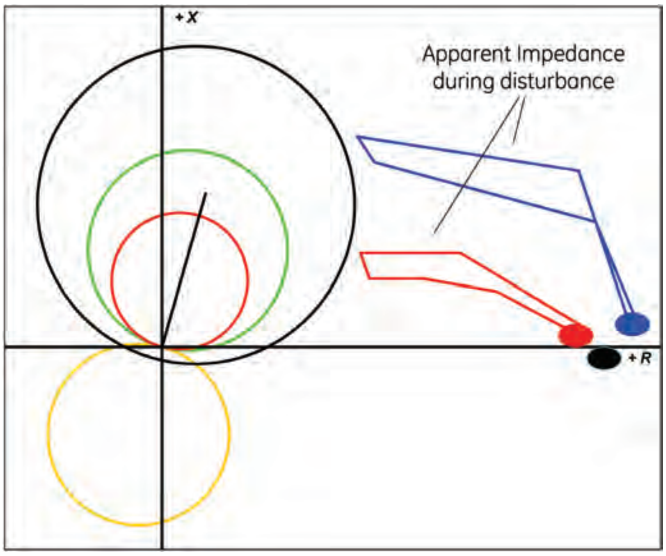


Figure 9.
Apparent impedance during disturbance

Figure 9 shows some results for a small-scale disturbance. The apparent impedance seen by the relay came close to the largest tripping zone of the distance relay. This small margin justifies a contingency study to determine if the reach settings for this zone are secure against local small-scale system disturbances.

5. Conclusions

The value of disturbance recording to analyze the response of the power system to power system faults is well established. For this reason, the NERC guidelines for recording require utilities to capture RMS or phasor values of voltage, current, frequency, and power to analyze power system faults. Phasor measurements with recording capabilities are ideal devices to provide disturbance recording. The explicitly time-synchronized synchrophasors data meets the accuracy requirements and time requirements of the NERC guidelines.

The real strength of using PMUs for disturbance recording is the ability to easily support wide area recording using existing communications networks. Capturing data at various points on the system provides better analysis of system performance during power system faults. The challenges of synchronizing data are eliminated, as each piece of data is explicitly time synchronized. Cross-triggering signals are sent via nonproprietary communications, such as defined in the IEEE Synchrophasor standard and IEC 61850 standards.

6. References

[1] L. Swanson, J. Pond, R. Hunt, "An Examination of Possible Criteria for Triggering Swing Recording in Disturbance Recorders", 2005 Fault and Disturbance Analysis Conference, Georgia Tech, Atlanta, GA, April 25th – 26th, 2005.

[2] NERC Standard PRC-002-1 – Define Regional Disturbance Monitoring and Reporting Requirements, North American Electric Reliability Corporation, Washington, DC, August 2006.

[3] NPCC Document B-26 Guide for Application of Disturbance Recording Equipment, Northeast Power Coordinating Council, New York, NY, September 2006.

[4] SERC Supplement Disturbance Monitoring Equipment (DME) Requirements, SERC Reliability Corporation, Birmingham, AL, August, 2006.

[5] DRAFT Standard RFD-PRC-002-1 Disturbance Monitoring and Reporting Requirements, Reliability First Corporation, Canton, OH.

[6] A. Klimek, R. Baldwin, "Benefits of Power Swing Recording", 2204 Fault and Disturbance Analysis Conference, Georgia Tech, Atlanta, GA, April 26th – 27th, 2004.

[7] R. J. Murphy, "Disturbance Recorders Trigger Detection and Protection", IEEE Computer Applications in Power, Institute of Electrical and Electronic Engineers, New York, NY, January 1996.

Smart Grid:
The Road Ahead

Larry Sollecito
GE Digital Energy

1. Introduction

From the time that Thomas Edison commissioned the world's first power system in 1882, the electric power industry has continually moved forward – working to improve the functionality, efficiency, and availability of electricity. Through evolutionary advancements in technology, the electrical power industry has transformed the way we generate, deliver, and consume power today.

As the electric power industry begins the next century, it is on the verge of a revolutionary transformation as it works to develop a Smart Grid to meet the needs of our digital society. Society's expectations and Utility Commission incentives/penalties are driving changes to the industry where secure data is required quickly, on-demand, and in an easy to search way. Customers are demanding higher reliability and greater choice, and are willing to examine and change their energy usage patterns.

To achieve the end-goals stated above, a unified vision of the road to the Smart Grid is needed. Without a unified vision, the issues currently facing the power system will be addressed piecemeal by utilities, government agencies, and related power system organizations. The result of isolated development activities will be a power system that is plagued by islands of separation. Subsequently, the power system of the future may only be realized in limited areas or on a small scale. This article presents a definition of the Smart Grid and examines the road ahead to its development, which is only possible when power system organizations work together to provide a more capable, secure and manageable energy provisioning and delivery system. (IntelliGrid Architecture Report: Volume 1, IntelliGrid User Guidelines and Recommendations, EPRI, Palo Alto, CA and Electricity Innovation Institute, Palo Alto, CA: 2002. 1012160.)

2. The Smart Grid

According to the IntelliGrid Architecture Report cited above, the Electric Power Research Institute (EPRI) defines the Smart Grid as:

- A power system made up of numerous automated transmission and distribution (T&D) systems, all operating in a coordinated, efficient and reliable manner
- A power system that handles emergency conditions with 'self-healing' actions and is responsive to energy-market and utility needs

- A power system that serves millions of customers and has an intelligent communications infrastructure enabling the timely, secure, and adaptable information flow needed to provide power to the evolving digital economy

From this definition, we can conclude that the Smart Grid must be:

- Predictive (operationally and functionally) to preclude emergencies
- Self-healing to correct/bypass predicted/detected problems
- Interactive with consumers and markets
- Optimizable to make the best use of resources
- Distributed in nature with both assets and information
- Transformational to turn data into information
- Secure from threats and hazards

The Smart Grid must provide robust, reliable, and secure communication as well as intelligent electronic devices (IEDs) and algorithms to make the necessary system assessments when needed. To achieve a Smart Grid, the industry must merge copper and steel (electricity generation and delivery infrastructure) with silicon and glass (computation and communication infrastructure). We are currently at the crossroads in the coming of age of both technology areas.

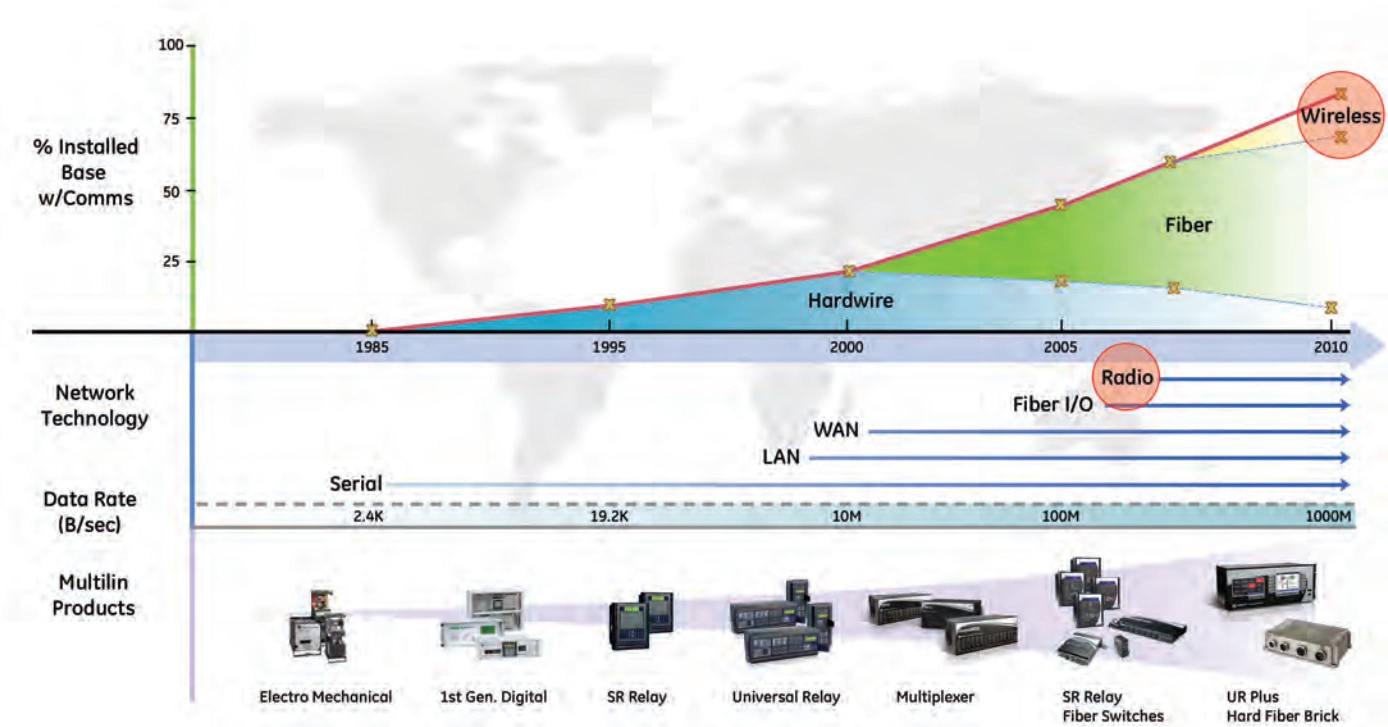


Figure 1.
The Evolution of IED Communications

Over the past 35 years, we have seen communication speeds increase dramatically from 300bps (bits per second) to digital relays that today operate at 100Mbps - an increase of over 300,000 times! (Figure 1) Not only have the communication speeds changed, but the communication protocols have migrated from register-based solutions (e.g. - get the contents of Register 5) to text based data object requests (e.g. - get the Marysville-Kammer Line Voltages) as implemented through the IEC 61850 protocol. In addition, the physical interfaces have transitioned from RS-232 serial over copper to Ethernet over fiber or wireless – both local and wide-area. Interoperability has become a reality and today's devices are self-describing and programmable via a standardized configuration language.

On the device side, the IED and its constituent components have undergone an evolutionary convergence of multiple functions and features into a single device (Figure 2). In the past, protection, control, metering, oscillography, sequence of events (SOE), annunciation, and programmable automation logic were all separate functions. Today's IEDs combine these functions and more into a single platform that provides superior user interfaces allowing visual access to metering, SOE, device diagnostics/solution, and phasor views of data.

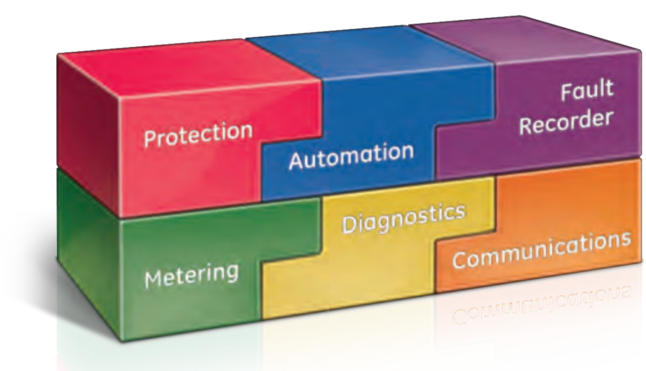


Figure 2.
Convergence of Functionality in Today's IEDs

3. Enterprise Drivers

In migrating towards a Smart Grid, there are three clear enterprise areas that are driving the industry forward: financial performance, customer service, and organizational effectiveness.

3.1 Financial Performance

Financial performance is typically measured in terms of reduced expenditures. In the case of utilities, cost reduction in capital improvement, operations, and maintenance are the primary areas of focus. In the capital improvement arena, advanced communication technologies and global standards, such as IEC 61850, are enabling new architectures and implementations such as Relay-to-Relay communication and Process Bus. These technologies are already demonstrating a reduction in engineering, implementation, and commissioning costs through distributed architecture solutions and soft wiring. Standardized long distance tripping via fiber or wirelessly and analog data communication not only reduce wiring, but also enable new applications such as distributed load shed.

3.2 Customer Service

As described in the introduction, the digital society is demanding higher availability and better quality of electrical energy delivery from utilities. The Smart Grid provides the foundation for addressing these requirements. Detection of incipient problems is facilitated through monitoring and analysis of electrical signatures from the transmission, distribution, and industrial power systems. For example, analysis of electrical signatures from the distribution system can indicate a downed conductor, incipient cable fault, or failed capacitors. On transmission systems, increased communication speeds enable real-time grid control for enhanced stability. In the industrial realm, motor current signature analysis can detect excessive motor vibration, motor turn faults, and broken rotor bars.

In the area of power quality, much of today's electronic equipment demands 100% availability (or at least 99.999%) and preferably clean (minimum harmonic content) power. To meet this demand, the Smart Grid needs to look at new sources of auxiliary power and the means to protect and dispatch power generation in small localized areas. Dynamic filtering of power may be offered as a fee-for-service option. Communication will be key in coordinating this activity throughout the grid.

3.3 Organizational Effectiveness

For an organization to be effective and drive improvement, its people need operational information. Currently, data is gathered through periodic polling of a limited set of measurements and periodic manual inspection of assets.

The Smart Grid view of the substation has changed this paradigm in several ways:

- The IED is monitoring more of the assets in a substation, collecting data, and converting the collected data into information. Timely information about an asset enables optimal use of that asset.
- The IED is able to communicate, on exception, the semantics of the situation. Semantic-based communication provides a standard, unambiguous view of the information and minimizes the documentation and configuration effort.
- The automation aspect provides seamless information aggregation, storage, and dissemination

The overall effect of the Smart Grid in this domain is to improve manpower utilization through automation, and optimized asset utilization through automatic monitoring and operation.

4. Application Domains

As the Smart Grid comes into existence, there are several application domains that promise to drive its development.

4.1 Advanced Metering Infrastructure (AMI) and Smart Home

The first domain, and the area where there is a lot of activity, is advanced metering infrastructure (AMI). AMI represents the next phase of automatic meter reading whereby the meter is responsive to two-way communication, dynamically adjusting for the price of electricity, and interacting with the various loads in the metered facility. The various public utility commissions, who strive to adequately balance the supply and demand aspects of electricity, are driving the implementation of this domain.

The advanced functionality of AMI enables the creation of the Smart Home. The combination of these domains brings to bare functionality such as:

- Real-time pricing/hour ahead emergency pricing /automatic home response
- Direct load control
- Energy usage/optimization display
- Load monitoring/sub-metering
- Remote connect/disconnect
- Outage detection and isolation/customer trouble call management
- Demand profiles
- Security monitoring
- Remote home control
- Remote equipment diagnostics

Home energy optimization will become automatic but the system will also provide user interfaces to foster further energy use optimization (Figure 3).

Figure 3.
Home Energy Dashboard

4.2 Distributed Generation / Microgrids

The second domain driving the Smart Grid's development is Distributed Generation/Microgrids. As the number of Distributed Energy Resources (DER) increases throughout the electronic enterprise, and communication to the various resources becomes more pervasive, the ability to operate segments of the grid as islands or Microgrids becomes reality. The drivers are clear - the desire for high-availability and high-quality power for the digital society. Figure 4 shows a vision of the evolving Microgrid structure.

DER includes not only positive power generation such as solar, wind, and micro-turbines, but also negative power generation through demand response programs, controllable loads, and direct load control. Renewable energy resources are becoming competitive with existing generation resources. Many utility commissions are incentivizing additional renewable generation sources (solar and wind) on the grid. Battery and inverter technology is evolving such that a utility can justify the capital cost of the installation based on the difference in price from buying energy at night at a low price and selling it back during peak daytime rates.

Microgrids do present challenges to the utility from a protection, control, and dispatch perspective. Traditional protection is based on the fact that for a short circuit, significant overcurrents will flow in a direction towards the fault. In a Microgrid environment, a significant portion of the generation will be inverter-based which, through design, is current limited. New protection philosophies will need to be developed to protect these systems.

On the control side, it will be necessary for the Microgrid to be seamlessly islanded and re-synchronized. It may be required that the Microgrid be dispatched as a single load entity. This will mean that a local controller will have to be able to communicate with all of the DERs on the Microgrid, and dispatch both watts and vars, to maintain a constant power flow at the Point of Common Coupling (PCC). The amount of power dispatched will be set either on a contracted value or optimized based on the dynamic price of electricity.

Electric and Plug-in Hybrid Electric Vehicles (PHEVs) provide an additional twist in the operation of the Microgrid because they are mobile. As they connect and disconnect from a Microgrid, the controller will have to be aware of their existence and include their potential effect in the operation of the Microgrid. One of the operational use-cases that evolves from this scenario is the Microgrid controller sending buy/sell messages, that include dynamic pricing information, to the owner of the vehicle.

4.3 Wide Area Measurement and Control

The third major domain area that is rapidly evolving is that of Wide Area Measurement and Control Systems (WAMACS). These systems have the ability to synchronously measure and communicate the instantaneous state of the power system through a measurement known as the Synchrophasor. The ability to dynamically view the state of the power system is similar to being able to view a beating heart. Normal and stressed system states can be assessed in real time and acted upon to affect dynamic control. Today's power system operators take action in the multi-second to multi-minute time frame, but WAMACS can make and execute decisions in the 100 millisecond time frame.

The development of the WAMACS infrastructure entails the installation of measurement and data collection devices in substations, a reliable wide area communication network, and data concentration, visualization, and decision facilities. Work is ongoing in all these areas. As utilities build out their communication infrastructure, they must take notice of the performance requirements dictated by real time synchrophasor communication. Many of the projects will take five or more years to come to fruition.

5. Smart Grid Architecture – Putting the Pieces Together

As the operating scenarios of the above application domains are fleshed out, it soon becomes apparent that there are opportunities and needs for cross-application communication. For example, the WAMACS function detects a system instability and determines that it needs to shed load in the sub-second time frame. It is clear that there needs to be a communication interface between the WAMACS applications and the Smart Home and Microgrid environments. In order to achieve this cross-domain communication, an architecture is needed to define the parts of the communication system as well as to define how they interact.

The architecture process defines a set of plausible scenarios (Enterprise Activities) spanning the entire energy enterprise (utility, industrial, commercial and residential). The scenarios then enable analysis on the data and resulting communication requirements needed to construct a complete, high-level set of functions for the communications infrastructure to enable the envisioned functionality. The requirements can be categorized as:

- Communication configuration requirements, such as one-to-many, mobile, WAN, and LAN
- Quality of service and performance requirements, such as availability, response timing, and data accuracy

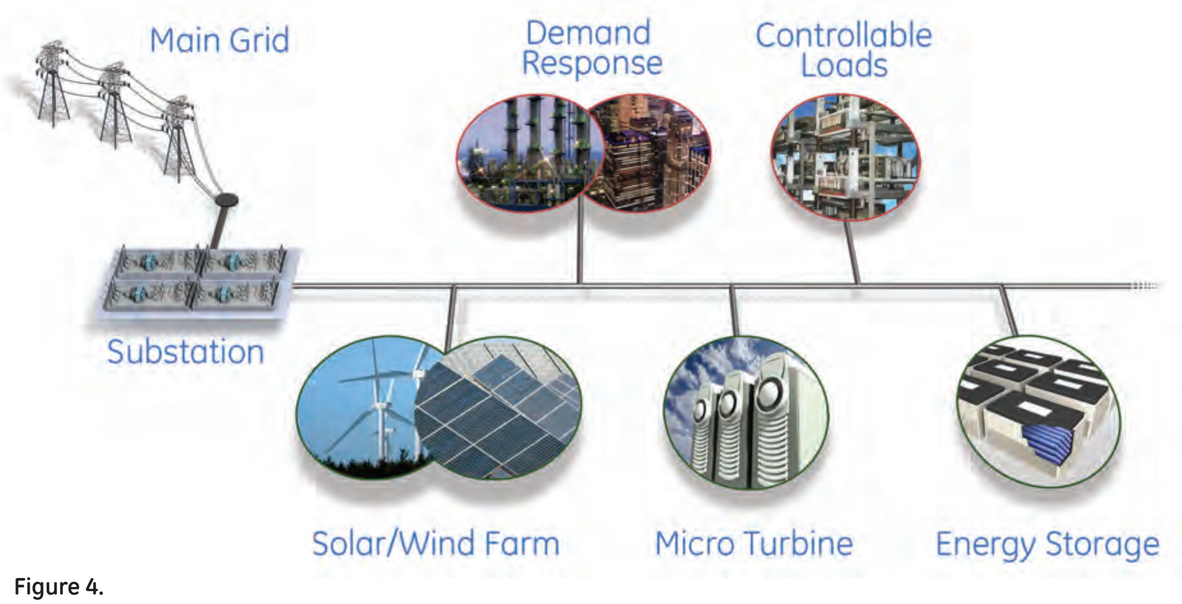


Figure 4.
Microgrid Vision

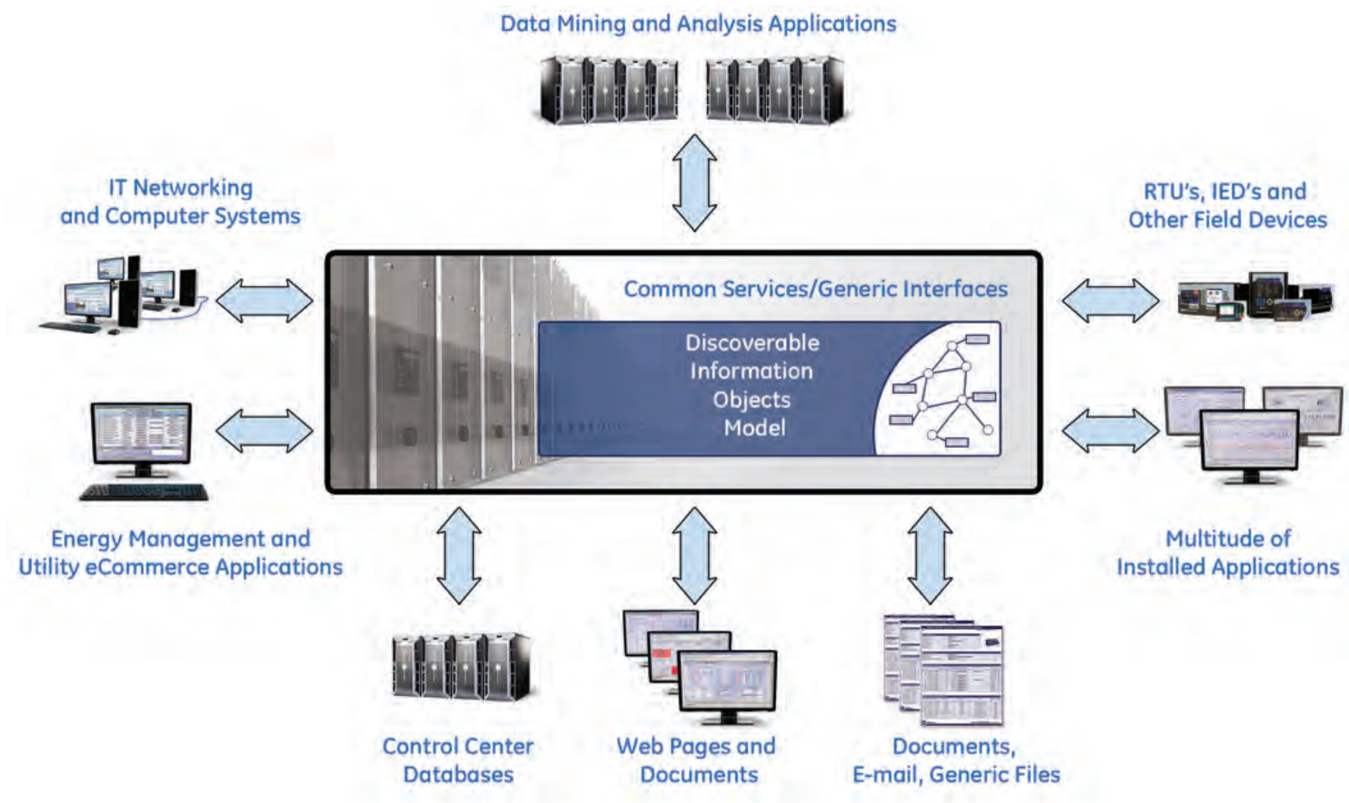


Figure 5.
Smart Grid Architecture

- Security requirements, such as authentication, access control, data integrity, confidentiality, and non-repudiation
- Data management requirements, such as large databases, many databases across organizational boundaries, and frequent updates
- Constraints and concerns related to technologies, such as media bandwidth, address space, system compute constraints, and legacy interface
- Network management requirements, such as health and diagnostics of infrastructure and equipment, remote configuration, monitoring, and control

Putting together the pieces, there are several guiding principles that show the way to an architecture. According to the IntelliGrid Architecture Report cited earlier, an architecture should be technology independent, based on standard common services, a common information model, and generic interfaces to connect it together. Figure 5 is a conceptual view of such an architecture. While adapters can accommodate the above heterogeneity, to achieve interoperability using off the shelf components, we need standards for what data is exchanged and how data is exchanged. Furthermore, these standard information models and interfaces must be applicable to a variety of utility services. A standardized common information model solves what is exchanged. A standardized set of abstract interfaces solves how data is exchanged. A single technology for every environment will never be agreed upon so adapters will still be required to convert between different technologies.

It should be noted that the IEC 61850 communication protocol, "Communication Networks and Systems for Utility Automation," meets these requirements today. This protocol defines internationally standardized models for protection, control, metering, monitoring, and a wide range of other utility objects. In addition, it defines a standard set of abstract services to read and write to these models. Most importantly, it provides a mechanism for self-description of the data models to any requesting client. This feature becomes of paramount importance for auto configuration as the number of devices in a domain becomes large, for example, millions of electric meters.

6. Conclusion

The journey towards establishing a Smart Grid is underway.

The industry is working to meet the demands of the digital society. Progress is being driven forward by demonstrating solid financial performance through reduced expenditures, meeting customers' demand for higher availability and better quality of delivery, and increasing organizational effectiveness through high-quality, timely operational information. Several application domains such as Advanced Metering Infrastructure, Smart Home, Distributed Generation/Microgrids, and Wide Area Measurement and Control are also key in driving the Smart Grid's development.

Traveling down the road to a Smart Grid will take an organized effort to overcome isolated development and unite power system organizations to provide a more capable, secure, and manageable energy provisioning and delivery system.

070209-v2

Leader or Follower

Developing the Smart Grid Business Case

John McDonald
GE Energy

A world of energy developments are coming together right now with consequences that we will all feel for generations to come. World energy consumption is forecast to triple by 2050. Climate change has become more fact than fiction. Our nation's energy security is vulnerable due to our current dependence on finite natural resources for energy generation. We are in a time of fundamental change in the utility industry, and we must make decisions as significant as those wrestled over by Edison and Westinghouse as they debated DC versus AC power distribution. We have the technology, and market forces are converging to fundamentally change the way the grid operates to improve efficiency, reliability, and energy security.

After a decade of expectation that advanced grid and metering technologies will provide a step change in system cost and performance, momentum towards smart-grid implementation is finally building. In practical terms, this means the industry will see larger-scale commitments to not just advanced metering infrastructure (AMI) deployment but investments in new and improved grid technologies vastly expanding the scope of benefits available to a utility and its customers.

A number of forces are aligning to drive momentum, particularly as the industry is entering an era where expectations of what the grid can do are being stretched to activities that include providing instantaneous corrections to outages, enabling customers to make energy consumption decisions, and facilitating the smooth transfer of power flow from large wind farms. Supporting these new expectations is an emerging environment of greater regulatory acceptance and understanding of the real benefits that smart grid can deliver.

Despite the changing environment, there are challenges preventing utilities from fully understanding and developing their smart grid strategies. Continually evolving technologies, silo efforts within utilities, and cautious skepticism of benefits all lead to slowing down decision-making and investment in smart grid technologies. To address these challenges and to quickly move to capture the benefits of smart grid that are accrued over a longer duration, utilities need to get organized and act with urgency. Utilities should develop a comprehensive fact-based assessment of smart grid in the absence of developing the comprehensive assessment of smart grid benefits; however, utilities are missing out on an opportunity to capture significant benefits for customers that are self-funding over the life of the investments.

This column discusses the key driving factors behind smart grid momentum, the challenges facing utilities, and suggests how utilities should think about developing their comprehensive smart grid business cases.

1. Momentum Is Building Towards a Smart Grid Vision

The past two years have been pivotal in the industry for broadening the definition of smart grid from AMI to encompass a larger set of customer facing and grid applications combining communications, digital hardware, and decision making to drive step-change improvements in cost, quality, and reliability of service. This broadening represents a natural evolution of improved technologies combined with expanding needs. In this column, smart grid is defined as the set of advanced, digitally based technologies that can be attached at the boundary of generation and transmission and all the way through the grid across the meter and into the home. This includes phasor measurement, centralized and integrated voltage and VAR controls, grid automation, advanced monitoring and diagnostics as well as AMI. Home area network (HAN) applications based on advanced telecommunications technologies are included in the scope of smart grid.

This myriad of technologies represents an industry entering a new era where the combination of environmental pressures and tremendous investment needs are reshaping traditional fundamentals. Large-scale grid investments are needed to overhaul the U.S. transmission and distribution grids as historical investment has lagged. Pressure on improved grid reliability and power quality is increasing as more regulators think about attaching penalties and rewards against performance. Customer satisfaction ratings are also viewed with greater scrutiny. Grid security has emerged as a serious concern and much attention is being paid to understanding how new investments will improve grid resilience. New telecommunications technologies with advanced encryption as well as remote inspection of assets enable a stronger grid.

Against this backdrop, the environmental push to drive energy efficiency, integrate large amounts of intermittent large-scale renewables as well as distributed generation has stimulated serious interest in ensuring the grid is well equipped to accommodate this need. AMI-enabled demand response has also assumed a critical role in the discussion of finding least-cost alternatives to new build or expensive power purchases. While direct load control without AMI will continue as an important building block for demand response, introducing consumer decisions to reduce usage will provide necessary additional load reduction. Customer awareness will continue to grow if expected rate increases materialize and share-of-wallet for electricity continues to grow as a proportion of total household spending.

In parallel, technology functionality has grown significantly. Basic SCADA systems have matured into advanced applications of distribution management systems (DMSs). Geospatial information systems (GISs) are normally integrated with outage management systems (OMSs). There are opportunities for significant improvement in service when this integration expands to include DMSs and workforce deployment. More advanced sensors are entering the market enabling real-time evaluation of asset performance.

In addition to these factors, the industry has benefitted from a dramatic reduction in technology costs. For example, disconnect relay switch costs have declined from about US$120 to US$40 in just the past three years. While other core hardware prices in the transmission and distribution space have been steady or increasing as demand has outgrown supply, the smart grid technology curve continues to push forward.

These trends are being matched with growing regulatory support for smart grid. At the national level, the U.S. Congress passed the Energy Independence and Security Act at the end of 2007 that provides grants, sets policy direction for smart grid through a national committee, and recommends accelerated depreciation for technology investments. A number of states are also moving to providing direction setting for smart grid investments. California is pushing utilities to provide an integrated vision of smart grid. In Illinois, Commonwealth Edison has filed for a surcharge to rates that represent a broad set of smart grid investments. In Ohio, the regulatory environment is pushing utilities to move beyond AMI filings to broader grid improvements. In Florida and Ontario, regulators have set precedence for faster depreciation of potentially stranded metering assets.

2. The Case for Smart Grid

With the growing momentum for smart grid implementation, the central question to developing the business case is how real is the impact from the smart grid. Smart grids can help utilities deliver significant benefits. Some of these benefits are quantifiable reductions from the current baseline of costs (O&M and capital). Other benefits will accrue by reducing expected future costs, particularly in terms of deferred or cancelled capital investments through peak reduction and advanced asset monitoring and diagnostics. Not all benefits are monetary; reliability and customer service improvements will ultimately result in better rate case outcomes through generating goodwill for utilities, but may not directly translate into monetary benefits.

Significant O&M cost reductions can be achieved through a smart grid. Many of the AMI-related benefits have been discussed across the industry over the last couple of years. Reductions across metering, customer care, billing, and credit and collections have been documented by utilities that have had AMI systems implemented for several years. Additional O&M reductions in field operations in both gas and electric have been more challenging to capture but the opportunities are certainly visible.

Avoided capital spending is also a critical and key benefit supported through demand response and asset optimization driven based on advanced monitoring and diagnostics. For bundled utilities, avoided capital covers both generation and grid investments and for unbundled utilities this typically involves avoided purchases in addition to grid investments.

There are significant reliability benefits driven by smart grid as well. The combination of AMI and fault detection, isolation and restoration (FDIR) creates a powerful driver to reduce SAIFI (System Average Interruption Frequency Index) as well as SAIDI (System Average Interruption Duration Index). On the other hand, more accurate reporting of outages as opposed to traditional estimation methods may actually increase CAIDI (Customer Average Interruption Duration Index) and quicker automatic restoration does result in shifting events from SAIFI into MAIFI (Momentary Average Interruption Frequency Index).

A smart grid will also drive improvements in the customer service experience. By delivering accurate and instantaneous meter reads, bill estimation challenges will be eliminated. The ability to complete the feedback loop to provide customers with up-to-date service information becomes easier. Currently, many utilities struggle with being able to provide accurate information back to the customer on key areas such as billing and outage notification and updates.

Smart grid also delivers significant control to the customer in their ability to influence energy consumption decisions. Demand response is a critical feature in the suite of smart grid capabilities. Peak shifting as well as overall conservation (kilowatt-hour consumption reduction) are both important impacts of a demand response system. While utilities have been administering direct load control programs for many years, the ability to leverage two-way communications with greater control and accuracy, and with customer input, can substantially enhance a utility's demand response capabilities.

In addition, safety on the grid is enhanced through smart grid applications. Integration of mobile workforce applications with advanced geospatial information systems and asset monitoring and diagnostics provides frontline crews with accurate location and state of sensitive equipment. The ability to diagnose outages more comprehensively also helps in crew safety preparation.

In addition, smart grid is critical in preparing our grid infrastructure for renewables and distributed generation. With intermittency of larger-scale renewables (e.g., wind farms) and the technical challenges of flowing power back and forth from distributed generation, grid controls are increasingly important. Future benefits of integrating plug-in hybrid vehicles (PHEVs) and more advanced microgrids will also require smart grid infrastructure to become reality.

Understanding these benefits and their secondary and tertiary impacts is important to establishing the case for the smart grid. Recent research and work in how customer utilities are thinking about smart grid suggests that most utilities are drawing a broad and cautious brush over understanding the full capabilities the smart grid can deliver.

Many of the benefits discussed above have been discussed by utilities in recent filings and industry discussions. Recent filings in California, for example, demonstrate the NPV positive business cases that AMI can deliver. Announcements by Progress Energy on integrated volt/var controls, PG&E's distribution automation program, AEP's GridSmart initiatives and Duke Energy's development of broad smart grid applications are all recent developments that indicate that momentum for a more comprehensive smart grid definition is growing.

3. Typical Challenges

With the breadth of benefits the smart grid can deliver and the improvements in technology capabilities and reduction in technology costs, investing in smart grid technologies should be a serious focus of utilities. Utilities, however, have been slow to respond. A number of all-too-familiar factors contribute to the stationary mode.

Technology obsolescence plays a critical role in utility caution in investment. The fear new technologies will be outdated within a short period results in a wait-and-see approach. This is particularly the situation with communications technologies that form the backbone from the meter end-point typically to the substation. A decade ago, discussions centered around mobile versus fixed AMR. Now the question is more complicated with options spanning powerline, broadband, and radio frequency spectrum-based wireless technologies as well as emerging WiMAX, 3G and 4G or LTE (long-term evolution) applications that are fast maturing. While communication technologies are certainly evolving, utilities should feel encouraged that open standards—often IP based—are fast becoming the expectation for emerging technologies. This means the array of smart equipment required (e.g., meters, sensors, capacitor bank controllers) is designed to be agnostic to alternative communication environments. In addition, hybrid solutions that combine technologies to fit specific terrain characteristics of a utility are also becoming more common and help mitigate the risk of single technology investments. Humayun Tai, a partner with McKinsey who works with utilities on developing their smart grid strategies, commented "Utilities need to work backwards from understanding what specific grid and metering functionalities they need, how this translates into bandwidth, latency and other requirements and then determine what is the optimal communications solutions. AMI and grid applications have distinct needs and can be addressed differently."

Smart grid efforts at utilities also struggle from being structured within departmental silos. A comprehensive and realistic assessment requires a cross-functional perspective merging engineering, field operations, back office, IT, customer operations as well as generation skills and expertise. Many smart grid efforts find their genesis in AMI efforts that have typically been ongoing within customer service organizations across many utilities. Utilities that have had success moving their smart grid vision forward have formed cross-functional groups with strong executive mandates to explore and develop the business case for smart grid. For example, AEP has a cross-functional group driving smart grid development from both the corporate and operating company perspectives.

In addition, there is significant confusion around the extent and sequencing of IT integration and needs. The industry is beginning to get its head around how engineering applications need to be integrated as well as how they link up with back office applications. Systems integration players are at early stages of understanding the full picture and new products and solutions from IT platform vendors are beginning to emerge. Despite this early state of IT development, utilities should recognize smart grid deployments will not happen overnight or within a year. Deployments will take place typically over several years allowing sufficient time for utilities to test and develop their integration plans.

The aggregation of these challenges leads to an environment where utilities are overly cautious. The vision for the smart grid becomes narrow rather than comprehensive. A prolonged period of piloting multiple technologies prevails. While pilots are an important step in confirming both the suitability and the benefits of smart grid technologies, often pilots are designed to test specific rather than a broad set of capabilities.

4. Moving Forward—and Moving with Urgency

As industry conditions, technologies and utility needs mature, there is urgency in understanding and developing a smart grid vision. Utilities need to take advantage of the emerging regulatory environment and the interest PUCs are showing in granting accelerated depreciation or pilot financing costs.

Because benefits from smart grid accrue over time, investments in smart grid need to be paced such that the cumulative benefits correspond with the timing of needs. For example, developing and launching a successful demand response program takes time because it relies on educating and convincing customers. To defer near-term, peak-based generation investments or to avoid expected high-cost power purchases in constrained markets, a utility will need to launch its demand response program several years ahead of when it needs the additional capacity.

This implies utilities need to develop a perspective on smart grid that is both comprehensive and fact-based. Developing what constitutes the business case requires little investment. It requires dedicating a cross-functional team of experts within the utility backed by executive sponsors. The teams' task would be to develop the benefits available across a range of benefit possibilities, and assessing the costs associated with these based on existing and emerging technology options. Many utilities already have an AMI case developed to some degree and in those instances, the smart grid business case would build upon the AMI case.

In assessing the business case NPV values, utilities have significant flexibility to shape payback and return profiles. Pacing deployment quickly or over a longer time provides a trade-off between spreading upfront investment costs and the payback period. Targeting deployment with areas where there are greater benefit opportunities (e.g., higher losses, uncollectibles, lower reliability pockets) can also alter payback periods. The business case can also be developed by evaluating smart grid capabilities individually. For example, AMI, FDIR, Volt/VAR can be assessed as three independent modules and their returns can be measured separately although there will be cost interdependencies.

In addition to the quantifiable benefits, the business case must also ensure reliability, customer satisfaction and environmental and distributed energy benefits are also articulated clearly along side the financial information. The importance of the nonfinancial benefits will depend on a utility's specific performance and regulatory situation.

Assessing costs can be challenging as technology evolves quickly. The business case should be assessed initially with different technology options for communications (e.g., RF, BPL, advanced telecommunications). Different levels of investment also link to corresponding levels of benefits.

Once a business case has been pulled together, the next step is to understand how smart grid fits into the broader utility strategy, especially developing the regulatory case for these investments.

Completing the financial and business regulatory cases helps the utility build a "road map" for deployment which indicates where the value is, what is the right sequencing of decisions and how regulatory actions should progress (and with what step-gates). Vendor assessment and technology selection should follow once the deliverables on the smart grid are established.

4. Leader or Follower?

As momentum towards smart grid grows, utilities need to get organized and systematically develop fact-based perspectives. The gap between leader and follower in the industry will widen as new implementations lead to more utilities establishing precedence and standards for how smart grid deployments should be defined.

An Enterprise Information Architecture Based on SOA Enables a Smarter Grid

Marcel Van Helton
GE Fanuc Intelligent Platforms

As part of President Obama's stimulus program, an estimated $19B will be invested in the Smart Grid to meet the needs of the 21st century—requiring a major overhaul of America's electrical grid. It will allow for better integration of renewable energy sources and flexible trading of energy as well as improved reliability. Providing better demand response, automatic recovery scenarios and improved "pre-warning" systems of potential distribution problems, the Smart Grid will enable the right measures to be taken to avoid potential failures in the grid.

The acronym for SMART with respect to computer technology stands for Self-Monitoring, Analysis, and Reporting Technology, a monitoring system for computer hard disks that detects and reports on various indicators of reliability to help anticipate failures. Although originally developed for computer technology, the description aligns well to one of the goals of the smart grid, which is to enable more reliable operations. In addition, it aims for increased efficiency and sustainability.

To make the smart grid a reality, utilities need to leverage intelligence by ensuring the availability of critical information needed for smarter, faster decision making. So how do you collect, organize, distribute, integrate, secure and interpret the vast sea of information in today's grid environment to deliver this intelligence?

A smart grid requires leveraging multitudes of information flow between different systems. For example, seamless integration of information from a SCADA system on top of a wind farm into a SCADA system of a larger utility may help determine short-term generation capacity while other parts of the information, for example, the transformer temperature profile, can concurrently be leveraged by the maintenance management system.

It is critical to have the ability to leverage both operational data and non-operational data. Operational data captures the "here and now" and keeps power flowing over the grid, while non-operational data spans a broader timeline. It provides insight into why things happened, keeps track of how people fixed what happened and predicts when problems may happen again. This "memory" is a key element of the intelligence in the smart grid.

All this information needs to be tied together to optimize the entire electrical supply chain, which means utilities need a comprehensive overview of the actual status of the suppliers (generators), the warehouses (storage capacity), the trucks (the grid) and the demand (consumers) to make intelligent decisions. And not surprisingly, other industries also share this challenge of developing IT structures that integrate multiple plant structures and suppliers' IT systems to make information available in "real-time."

1. Abandoning the Traditional Information Pyramid

Most utilities have implemented some type of Supervisory Control and Data Acquisition (SCADA) system with a set of Remote Telemetry Units (RTUs) or Intelligent Electronic Devices (IEDs), primarily focused on key operational parameters in the case of an outage or potential overload. Traditional pyramid-based information models bring information up from these various RTUs and IEDs using serial communication methods into a centralized SCADA system, which has propriety interfaces or an integrated means to communicate or provide Load Management System (LMS)/Demand Management System (DMS)/Outage Management System (OMS) functionality.

These information models, even with point-to-point defined communication of different applications, lead to many information streams, resulting in an unmanageable web of information. Furthermore, as more renewable generating assets are added to the grid, the amount of information is expected to grow; some organizations estimate an increase of up to 15 times the amount of information in today's systems.

2. Moving to a Service Oriented Architecture (SOA)

Companies can build intelligence into their systems with an Industrial Service Oriented Architecture (SOA) such as GE Fanuc Intelligent Platforms' Proficy[1] SOA, which improves interoperability and enables composite applications that leverage a cross-system, real-time data and services bus and repository. Used in combination with appropriate industry standards, SOA allows for a "plug and play" architecture for IT systems, whereby functionality can quickly be added, changed or removed to meet market demands.

The cornerstone of the SOA structure is the Enterprise Data and Service Bus, which includes core components such as standards-based data models, security, configuration, event management, and user management. Other software functions can be "plugged" into the SOA using and adding to the information and

[1]Trademark of GE Fanuc Intelligent Platforms, Inc.
All other brands or names are property of their respective holders.

services within the SOA. It is this information and service-enabling architecture that becomes the foundation of the intelligence in the smart grid as more and more value-added applications are plugged into the SOA structure to optimize the different components of the electrical grid.

The Industrial SOA structure with a standards-based data model supports a transition from a "computer friendly" hierarchical model for data flow to a more natural "user-friendly" approach based on putting the data and applications in the context of the real world. As a result, the information hierarchy is based on the actual structure of Energy Enterprises, Operation Centers, Substations, and Equipment—down to consumers' homes.

In the structure of today's smart grid IT solutions, functions like SCADA, LMS, DMS or OMS are all components leveraging the information available in the Enterprise Bus. The benefit is realized when these components have access to the same data (real-time and historical) in the same context of the real-world structure of the grid. This approach avoids common pitfalls of current systems where context is continually added and lost as data flows from one system to the next.

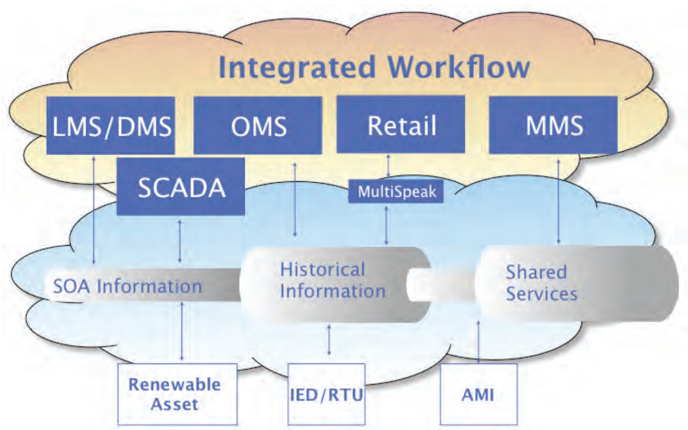


Figure 1.
Industrial SOA Structure.

3. A Structured Approach Toward Information

Traditional SCADA systems are tag-based and when information is transferred to other systems, the information structure has to change, depending on the requirements of each system. However, with an industrial SOA, information is available in a structured manner and all software functions share the same structure, so the data is maintained in a common context.

For example, operational and non-operational information such as the actual primary and secondary power and overview of the actual temperature and dissolved gasses is collected and stored into the SOA. Having operational and nonoperational information in a structured way in the same "repository" allows easier retrieval, interpretation and management of information.

Aside from actual "real-time" information, it is crucial that the system can store historical time series information and collect information in the IED/RTU and store it in the same historical system. As a part of the SOA Enterprise Architecture, a built-in Process Historian stores information in the context provided by the Enterprise Bus. There are two types of information stored: normal time series operational data, and events and alarms.

Delivering a solid backbone for leveraging "real-time" and historical information and providing an infrastructure to distribute the information between different locations, an SOA also provides developers with common architectural services like security, event management and user services. They can design the information structure based on specific industry requirements, adding relevant intelligence to the system.

4. Basic Building Blocks of the Smart Grid

4.1 Connecting to the Grid: The Collection Function

The innovations of today's communication networks are the basis of the smart grid, without which a smart grid would be impossible. We all remember the maximum baud-rate of 1200 bps (bits per second) where the SCADA systems could only poll the most important operational data such as volt, amps and vars. These systems were limited in bandwidth and would often only flow operational data from its source to other systems, which left a wealth of non-operational data islanded—never achieving its full potential.

Today, these bandwidth issues no longer need to constrain the systems and through the strength of a modern LAN/WAN architecture with a modern SOA, non-operational data can be included at all levels, bringing value to a whole new set of users. For example, Marketing and Product Planning can monitor equipment for efficiency in the actual physical environment and plan more efficient product offerings for the future, and substation maintenance can monitor conditions prior to failure and take steps to proactively replace equipment before catastrophic failures occur.

Today's IP-based communication through wireless (UMTS, radio Modems) and fixed or leased lines allows the transfer of more information on a continuous basis. Modern IEDs and RTUs provide a wealth of non-operational data—for example, fault event logs—whereby the more you know about the health of your systems, the better and smarter your decisions can be.

The collection function needs to map the information from the IED/RTU to the SOA structure, either through the traditional DNP 3.0 and the IEC 60870.5.101/103/104 protocols or through the relatively recent IEC 61850 protocol. The key advantage of the IEC 61850 is that it's already modeled to map the most common substation automation equipment.

4.2 Enabling Better Decision Making: The Data Warehouse

Information has a tendency to creep up into personal Excel® files located in different computer systems. To effectively put information to work, data must be up-to-date, easily accessible, and maintained in a common context. In this way, the data is easy to correlate.

For example, the serial historical data of a transformer could be correlated with sequence of event data of that same transformer.

To do this efficiently, a centralized information repository is required. The SOA structure with a built-in historian database allows you to store all information in a single logical location, whereby all the data is in a common context so there is a single version of the "truth."

To satisfy standard and ad-hoc information requirements, the user should have easy access to two types of reports. Standard reports can be used for compliance purposes, for example, a standardized emission report. Ad-hoc reports might be needed to look at the performance of a single asset while troubleshooting a grid problem.

Operators who can combine continuous and ad-hoc-based operational and non- operational information can develop a better understanding of the actual status and behavior of the assets within the grid. Consequently, they can make better and faster decisions in order to optimize performance.

4.3 Providing Operator Decision Support: The Workflow Function

While the additional information collected and generated to run a smart grid more efficiently allows operators and/or systems to make better decisions faster, the vast amount of additional data also requires an increase in the operators' knowledge base. That's where an industrial workflow tool can help—ensuring certain procedures are automatically triggered based on events arising from the information stored in the SOA structures.

The workflow provides the correct procedures to the operator and ensures appropriate sign off of those procedures. For example, if the system detects a potential failure in a breaker based on non-operational information, a workflow gets triggered, and the operator initiates a maintenance order to repair the critical part at the breaker. When the linesmen schedule the work, another workflow gets triggered to ensure that the operator switches off the segment and re-routes the power; once the work is complete, the workflows are closed.

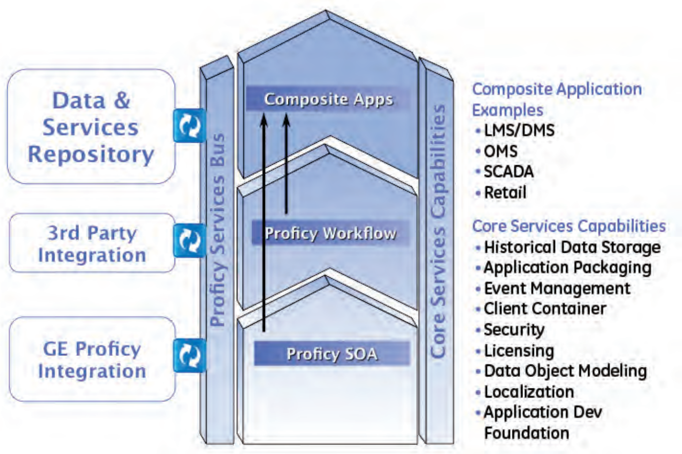


Figure 2.
Proficy SOA Enables Composite Application.

4.4 Functions Build on Workflow

Whereas workflow is an application that uses the SOA structure, other applications are built using the workflow product. For example, an outage management system can use the workflow "foundation" to execute work orders for the linesmen.

5. The Smart SOA Foundation

The Industrial SOA is the basis of the Enterprise Information Architecture, which meets the requirements of the smart grid. It enables a structured information model based on standards that combine "real-time" information with historical data, including events-based and time-series information, and allows other applications to seamlessly access the necessary information to perform certain functions.

Furthermore, an SOA is not limited to a single location or server, but easily spans over multiple locations with advanced search and location capabilities to aggregate information across the grid. For example, if a utility recently experienced an equipment failure, the SOA would enable a quick search across the grid for all similar equipment and collect its current operational and non-operational information to assess the potential for similar failures.

Enabling companies to build intelligence into their systems by leveraging all critical information, an Enterprise Information Architecture powered by SOA can help make the smart grid a reality—delivering improved reliability, efficiency and sustainability.

062909-v1

Key Smart Grid Applications

B. R. Flynn, PE
GE Energy

1. Abstract

The culmination of attention by utilities, regulators, and society for smart grid systems to address operational and electrical efficiencies, improving system reliability, and reducing ecological impacts, has resulted in a significant number of discussions around the requirements and capabilities of a Smart Grid. This session will explore three key Smart Grid functions with the strongest business case justification.

- Delivery Optimization
- Demand Optimization
- Asset Optimization

In addition to technical functionality, the incremental costs and benefits for each example will be presented. This session will include a review of example system architectures and specific functionality to provide improvements to performance metrics, capital and O&M costs and reduction to environmental concerns.

2. Introduction

IMES are changing. More information about the many forces behind these changes is being published every day.

- It is expected that the demand for electric energy will triple by 2050[1].
- Digital-quality power which represents about 10% of the total US electrical load will reach 30% by 2020.
- Rolling power outages in developing countries, previously just an unwelcome fact of life, have escalated to the level of "national emergency".
- Distributed generation including renewable and sustainable power has grown and is expected to double every three years[2].
- The average age of Power Transformer in the US is estimated to be 40 years old.
- Generation of electricity accounts for 40% of the US's CO2 emissions[3].

[1] Source: U.S. Army Corps of Engineers ERDC/CERL TR-05-21
[2] REN21 2007 update + EER
[3] EPRI, "Electric Sector CO2 Impacts, February 2007", Carbon Dioxide Emissions from the Generation of Electric Power in the United States, July 2000, DOE

For several years, electric utilities have been turning to Smart Grid technologies to help deal with these pressures. Currently utilities are focusing their efforts on three major areas.

Delivery Optimization consists of the efforts by the electric utility to improve the efficiency and reliability of the delivery systems.

Demand Optimization focuses on solutions to empower the end consumer and to better manage the evolving demand and supply equation along the distribution feeder

Asset Optimization is the application of monitoring and diagnostic technologies to help manage the health, extend the useful life and to reduce the risk of catastrophic failure of electrical infrastructure.

A Smart Grid drives value with integration of open technologies.

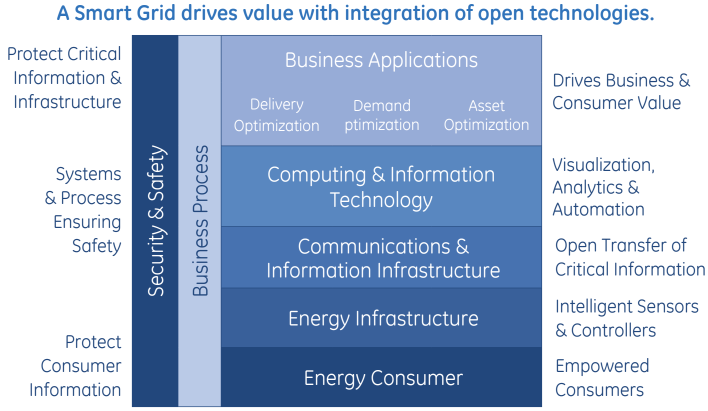


Figure 1.
Smart Grid Technologies

Figure 1 highlights the relationship of the various major functions involved with most Smart Grid solutions. The business applications of Delivery, Demand and Asset Optimization are part of the highest value smart grid business applications. They work on a structure that includes computing and information technology designed to support the applications and help manage the significant amount of data required for each of the applications to function appropriately.

Since the source for much of the data lies outside the utilities data center, an open, secure and powerful communications and information infrastructure is required to access the data. The communications infrastructure touches portions of the entire energy infrastructure from generations to the meter and in many cases into the energy consumer's premise. This system is designed in a way that maintains a high level of safety and security.

3. Smart Grid Solutions

Architectures for solutions that focus on each of the three areas will be presented including a summary of functionality and value.

3.1 Delivery Optimization

Delivery Optimization includes two major areas which will be reviewed separately, Efficiency and Reliability.

Utilities have deployed methods to improve the efficiency of their electrical systems. This discussion will focus on recent efforts to change the methods of controlling voltage and VARs on their distribution systems.

Efficiency

There are two types of losses in electrical systems, restive and reactive. Typically, capacitors are deployed in the station and along the backbone of the feeder to help manage the reactive losses and support the voltage. Distribution capacitors are usually operated by local controllers based on Powerfactor, load current, voltage, VAR flow, temperature, or the time (hour and day of week). Through the use of communications to modern controllers, coordinated VAR Optimization is available. This type of system usually controls the line capacitors based on the Powerfactor measured at the substation. Depending on the feeder's load, quantity of capacitors and existing type of control, the system can reduce the electrical losses.

There are two example architectures for these functions as shown in the following diagrams.

With the addition of communication and smart controllers to various voltage regulators and transformer load tap changers, utilities are taking finer control of their feeder's voltage with a technique called Conservation Voltage Reduction (CVR).

Controlling the regulator and LTC, the utility can reduce feeder voltage levels and depending on the amount of resistive and linear loads along the feeder, will reduce the load at the substation. Utilities have seen a 1% reduction for a 4% reduction in voltage.

The architecture shown above illustrates a system where the communications from the distribution devices communicate with the substation. This system utilizes a station based system which operates the line devices for VAR or voltage control based on the measurements at the station and along the feeder.

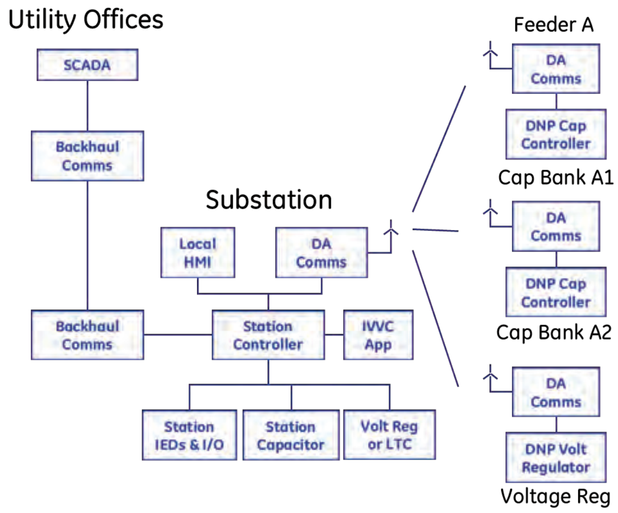


Figure 2.
Station Based IVVC System

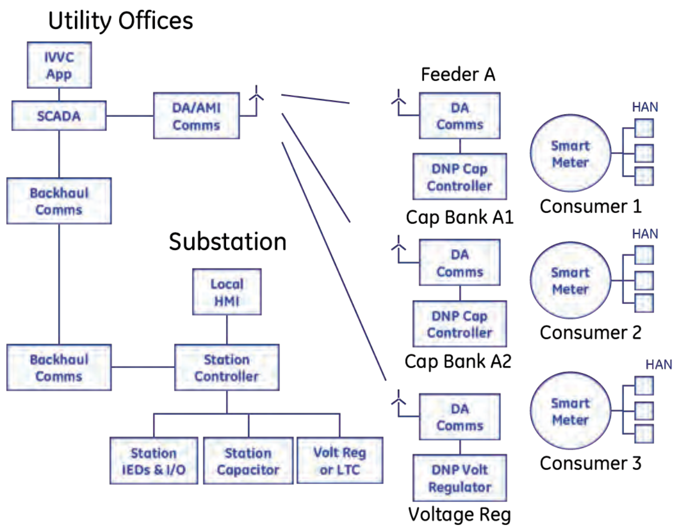


Figure 3.
Centrally Based IVVC System

The next system illustrates a centrally based communications system and a centrally located algorithm. This system adds the ability to monitor the voltage from selected customers' meters. The customers selected for voltage monitoring are those at the end or at low voltage points of various line segments. Depending on the AMI system's latency and bandwidth, selected meter voltage reads are incorporated into the IVVC application to allow for a wider operating range of the CVR application.

The capacitor communications can utilize a separate DA system communications or can share the AMI communications network and backhaul. Both systems require communications with the substation for control and monitoring of station transformers and feeders. Some utilities have estimated the aggregate payback for an integrated volt/VAR control system to be less than two years. These benefits can be significant and are typically shared between the utility and the end consumer depending on the rate structure. Regulating Commissions are becoming more and more receptive to granting a portion of these benefits to the utility to help compensate for the expenses of the systems. The balance of the benefits often flow through to the end consumer in the rate making process. The benefits typically include:

- Improved distribution system efficiency
- Reduced distribution line losses
- Improved voltage profile along feeder
- Improved system stability and capacity
- Defered capital upgrades
- Reduced energy demand
- Reduction of environmentally harmful emissions

Reliability

Many utilities are turning to Smart Grid applications to provide improvements to reliability metrics. Two typical architectures are shown below. The first shows a station based automation system with smart devices installed in the substation and in distribution circuit reclosers, or switches for underground systems. Faults are detected between switches and are isolated under control of the automation system. Unfaulted sections of the feeder are restored from alternate sources depending on available sources and their capacity to carry the additional load.

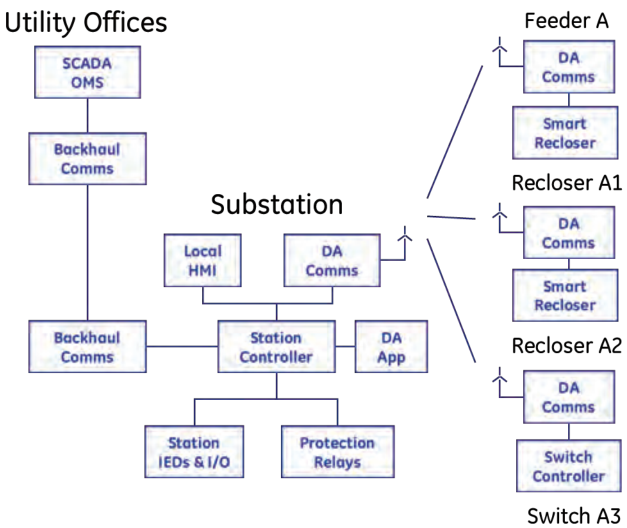


Figure 4.
Station Based Distribution Automation

The architecture shown below uses a centralized distribution automation system with the addition of communication to smart metering. The algorithm can utilize the information from the smart meters to assist in detecting outages outside of the monitored range of the automated devices. This includes fuses or other non-automated fault interrupters. The meters can detect and report an outage and can report successful restoration. Using the restoration detection, the system can determine customers have been properly restored as expected. After restoring customers after a fault, any meters not responding with a restoration can indicate a possible nested outage. This capability can significantly improve the time to respond to these outages.

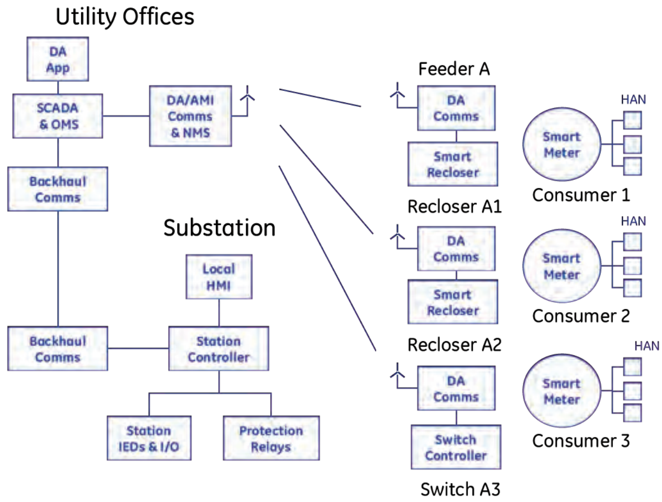


Figure 5.
Centralized Distribution Automation

Many regulators do not provide the utility with direct incentives for investment designed to reduce outages, however rely on the threat of penalties to encourage investments. This makes it prudent for the utility management to apply automaton to the most troublesome circuits first. However, it is also necessary to determine the appropriate level of automation to be applied. The following chart compares the costs per improvement to customer minutes interrupted compared to a typical non-automated base case circuit.

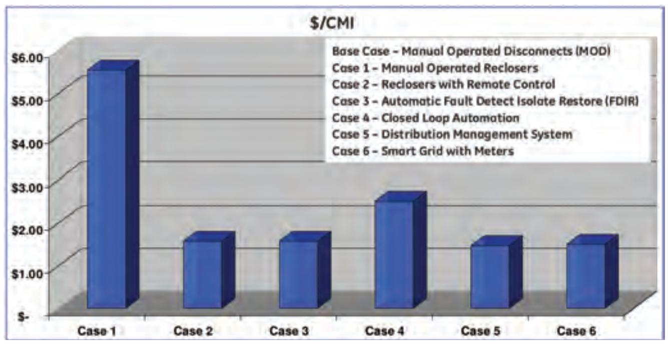


Chart 1.
System Costs by Customer Minutes Interrupted (CMI)[4]

In this study, the Base Case consists of 2 Manual Operated Disconnect Switches (MOD) and a shared tie switch with another feeder. Case 1 changes the MODs to manual operated reclosers on overhead circuits and customers on that circuit experience a corresponding improvement to outage minutes. Case 2 adds communications to the reclosers, allowing the dispatcher remote manual control to of the switches. Cases 2-6 have a significant improvement to reliability metrics from the ability to localize faults and isolate and restore unfaulted segments of the feeder. Case 3 adds the ability for automation software for Fault Detection, Isolation and Restoration (FDIR). Case 4 utilizes an expensive but highly effective automation system where the normally open tie switch is normally closed. This closed loop automation

[4] Justifying Distribution Automation at OG&E, by Cristi Killigan and Byron Flynn, prepared for DistribuTECH 2009

circuit requires expensive dedicated high speed communications between the switches to prevent over-tripping. Case 5 adds the ability to utilize a centralized automation system with the addition more sophisticated electrical network model supporting the automation software. Case 6 adds the ability to detect outages/ restoration from the meters.

3.2 Demand Optimization

In recent years, Demand Optimization has generated a significant amount of interest. This solution has drawn the attention of regulators and the US federal government. Often the benefits from Demand Optimization is what is in mind when regulators installation of smart metering. These are the benefits most directly experienced by the end consumer.

Solutions around Demand Optimization are varied and range from simple advanced metering systems to full home automation. The figure below is designed to highlight the possibilities of a solution.

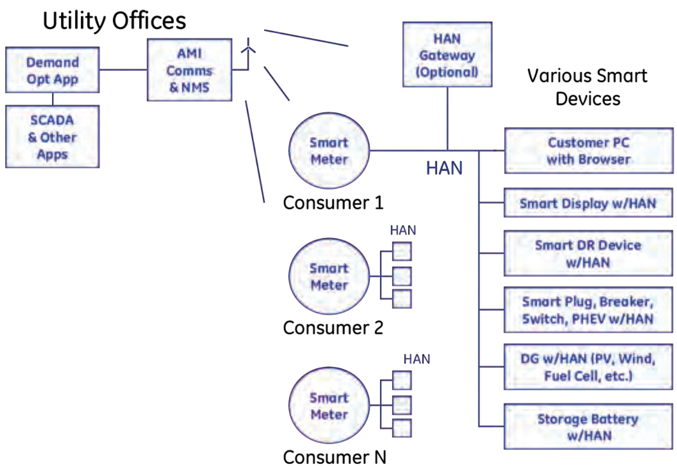


Figure 6.
Demand Optimization System Architecture

This system usually consists of several different devices in the consumer's home, usually at a minimum it includes a smart thermostat connected to a smart meter. Often the consumer connects their PC to a web page containing information about their usage and available programs the consumer can select.

Addition of a Smart Display allows continuous communications between the utility and the end customer. These displays can be simply a light which changes color based on time of use rates or can be a complex full graphic color touch screen connected to a full home automation system. New smart appliances, wall switches and wall sockets are beginning to become available for integration into a Home Automation Network (HAN). Some systems integrate local generation into the home including Photo Voltaic, solar panels, small wind generation, or more exotic systems such as fuel cells.

The architecture above also includes an optional HAN gateway. This gateway is intended to allow secure connection between the utility systems and the consumer's HAN when the communications to the end meter is not robust enough to handle the utility-HAN communications. In this option, the HAN gateway is connected to a customer's broadband Internet connection, providing a higher bandwidth connection than may be possible through some of the legacy slower speed AMI systems.

The following is a partial listing of example choices, programs, and devices which consumers and utilities are electing to deploy around Demand Optimization.

Empowering Customer Choice & Control:

- Critical Peak Pricing
- Time of Use Rate
- Green Power Choices
- CO2 Management Choices
- Prepaid Metering
- Voluntary or Automatic Control of Energy Demand
- Usage Management – by Appliance
- Home Energy Management
- Net Metering, collecting KWH, KVARH, Voltage,
- Power Quality

Providing Security & Safety Management:

- Energy Theft
- Tamper Detection
- Visual inspection during installation
- Monitoring and baselining usage patterns
- Interruptions and usage pattern changes
- Detect load-side voltage with disconnect

Enabling Distributed Generation:

- Photo Voltaic (Solar)
- Wind
- Biomass
- Geothermal

Incorporating Distributed Storage:

- Li-Ion Battery
- Fuel Cells
- Plug in Hybrid Electric Vehicle (PHEV as a storage device)

Facilitating New Programs and Capabilities:

- Load Management Programs
- Demand Response Program
- Distributed Generation
- Storage Management
- Automatic Meter Reading
- New Communications with Customer

- Power Quality Management
- Remote Service Switch
- Cold Load Pickup
- System Cyber Security
- System Management

The value of a TOU and CPP program has been estimated for a 6% peak load reduction as shown below.[5]

- $26 MM/yr O&M and capital expenditure reduction
- 126 GWh generation reduction
- Consumer's savings: up to 10%
- 57K tons of CO2 reduction
- Estimated capital cost of $12MM
- Estimated O&M cost of $11MM/yr

3.3 Asset Optimization

Much of the modern electrical system was installed over 40 years ago. Unfortunately, many devices in the system are frequently being pushed to operate at overload conditions. One of the single most expensive pieces of the distribution system is the station power transformer. Given that the general life expectancy of power transformers is around 40 years; this can result in a risky and expensive challenge.

The architecture shown below illustrates how Asset Optimization solutions can be added to a Smart Grid.

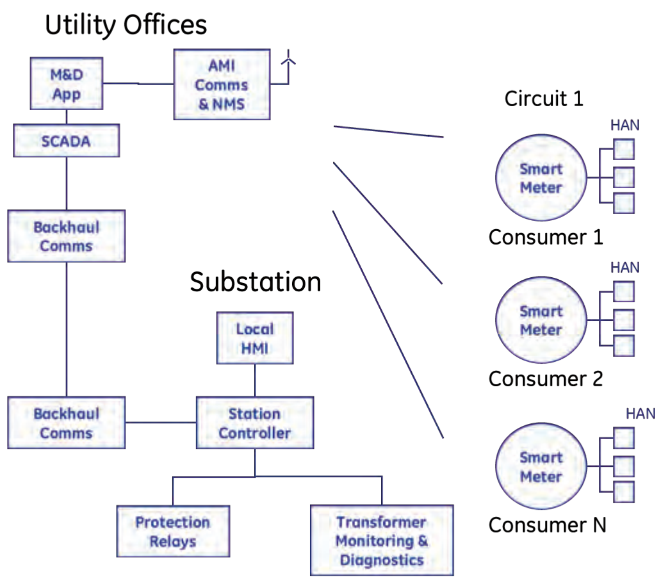


Figure 7.
Monitoring and Diagnostics (M&D) System Architecture

The architecture includes monitoring and diagnostics on the primary station transformer, station breaker, and distribution feeder devices.

The monitoring and diagnostics of the station transformer can include simply monitoring temperatures or continuous monitoring of the oil for combustible gasses and moisture. Advanced monitoring today can calculate internal hot spot temperature, the transformer dynamic load ability and future capacity over time, the insulation aging factors and data from many other models.

Monitoring of the station or line protection relays provides valuable information regarding the health of the breaker including operating times, total interrupted fault current, and operation counts.

Data collected from the meters can help determine near realtime loading on the distribution cables, especially the underground cables, and loading on the local distribution transformers.

This can help distribution engineers improve the distribution planning and design and help rebalance the load along the phases.

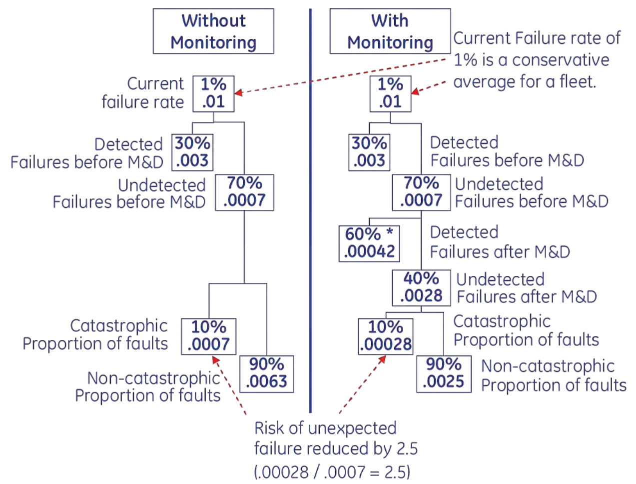


Figure 8.
Transformer reliability comparison[6]

The figure above contains the comparison of the power transformer failure rates with and without monitoring. For transformers without monitoring, the risk of catastrophic failure is approximately .07% and for transformers with on-line monitoring and diagnostics it is .028%, resulting in a reduced risk of failure of 2.5 times.

For example, if an average electric utility with 1 million customers, installed an M&D system which monitored the dissolved gas, temperature and load on their the transformerfleet, rated 20MVA and above, the costs and benefits is determined as follows:

An annual capital expenditure savings of $12MM/yr with an investment of $42MM in capital and $1.2MM/yr in additional maintenance. These numbers would result in a net present value, using 8.7% over a 15 year system life, of over $54MM.

5 Based on avg. 1 MM customer utility, California Statewide Pricing Pilot, June 2006

6 60% is an industry accepted effectiveness number for a quality monitoring system. The failure reduction figure is based partly on a CIGRE study. As an additional reference, a study conducted by one of KEMA's utility client shows that Distribution Automation projects can reduce the costs of repairing substation transformers by 67%.

4. Summary

While each of these solutions can have significant benefits to an electric utility and their consumers, elements of each can be leveraged for uses outside those stated in the previous discussions.

For instance, an IVVC system installed to control the VARs and volts can coordinate with a DA system installed to improve reliability. The rerouting of the distribution system to restore unfaulted sections of a feeder can significantly change the voltage and VAR profile of that feeder. If the IVVC system is operating on the same system network model as the DA system, it can continue to control the VARs and volts in the temporarily reconfigured distribution system.

Coordinating the asset management system to work with the DA system can result in new options to dynamically move load off of overloaded equipment by moving the normally open tie between different feeders to different locations. If the systems are working on the same network model, the DA system can continue to operate to improve reliability on the newly reconfigured network.

Furthermore, the CVR functions in the IVVC system should be coordinated with the Demand Optimization systems to maximize the benefits of improved load management. Depending on the a number of factors such as rates, prices, and system loading, the utilities' operations staff can pick the most cost effective method of reducing load by lowering voltage, issuing an automatic demand response signal and/or changing the consumer's time of use rate.

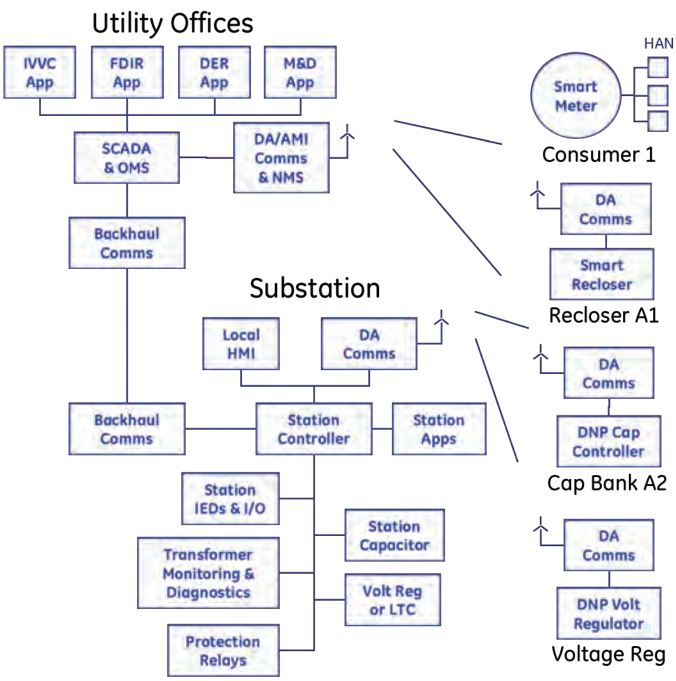


Figure 9.
Smart Grid System Architecture

The architecture of a fully integrated system as shown above is represented in the above figure. Properly designed using open interoperable products and techniques, the various systems can minimize the amount of duplication, can more easily integrate with existing utility infrastructures, can more effectively share communication infrastructure across the system, can share leverage elements of the network model in the office and can share data with other utility systems utilizing standards based methods.

5. References

Papers from Conference Proceedings (Published, or pending publication):

[1] Dalton, Howard, and Flynn, Byron, "SCADA Integrated with Transformer Monitoring Systems over a Secure Wireless Ethernet", 2005 DistribuTECH Conference and Exhibition, San Diego, California January 25-27, 2005.

[2] Flynn, Byron, "Case studies regarding the integration of monitoring & diagnostic equipment on aging transformers with communications for SCADA and maintenance", DistribuTECH 2008, Conference and Exhibition, Tampa Convention Center, Tampa, FL, January 22-24, 2008.

[3] Flynn, Byron, "Secure Substation Automation Architectures for Operations & Maintenance", 2006 DistribuTECH Conference and Exhibition, Tampa, Florida, February 7-9, 2006.

[4] Flynn, Byron, "What is the real potential of the Smart Grid?" Autovation 2007, The AMRA International Symposium, Reno, Nevada, September 30 – October 3, 2007.

[5] Lathrup, Steve, and Flynn, Byron, "Distribution Automation Pilot at PacifiCorp", Western Energy Institute, 2006 Operations Conference, Costa Mesa, CA, April 5-7, 2006.

[6] Stewart, Robert, and Flynn, Byron, "Modeling DA Improvements to Reliability Performance Metrics", 2007 WPDAC, Spokane, Washington, April 3 – 5, 2007.

The Evolution of Distribution

Jiyuan Fan, Stuart Borlase
GE Energy

With smart grids, confidence and expectations are high. To various degrees, utilities are putting smart grid initiatives in place, and many of the technologies that paraded under the smart grid banner are currently implemented in utilities. The smart grid initiative uses these building blocks to work toward a more integrated and long-term infrastructure. If all goes as expected, smart grids will provide tremendous operational benefits to power utilities around the world because they provide a platform for enterprise-wide solutions that deliver far-reaching benefits to both utilities and their end customers.

The development of new technologies and applications in distribution management can help drive optimization of the distribution grid and assets. The seamless integration of smart grid technologies is not the only challenge. Also challenging is the development and implementation of the features and applications required to support the operation of the grid under the new environment introduced by the use of clean energy and distributed generation as well as the smart consumption of electricity by end users. Distribution management systems and distribution automation applications have to meet new challenges, requiring advances in the architecture and functionality of distribution management, i.e., an advanced distribution management system (DMS) for the smart grid.

1. Current Distribution Management Systems

Distribution Management Systems (DMSs) started with simple extensions of supervisory control and data acquisition (SCADA) from the transmission system down to the distribution network. A large proportion of dispatch and system operation systems in service today rely on manual and paper-based systems with little real-time circuit and customer data. Operators have to contend with several systems and interfaces on the control desk ("chair rolls") based on multiple network model representations. The experience of operators is key to safe system operation. With an increase in regulatory influence and the focus on smart grid advanced technologies, there is a renewed interest in increasing the investment in distribution networks to defer infrastructure build-out and to reduce operating and maintenance costs through improving grid efficiency, network reliability, and asset management programs.

Various DMS applications are commonly used today.

- Fault detection, isolation, and service restoration (FDIR) is designed to improve system reliability. FDIR detects a fault on a feeder section based on the remote measurements from the feeder terminal units (FTUs), quickly isolates the faulted feeder section, and then restores service to the unfaulted feeder sections. It can reduce the service restoration time from several hours to a few minutes, considerably improving the distribution system reliability and service quality.
- Integrated voltage/var control (IVVC) has three basic objectives: reducing feeder network losses by energizing or de-energizing the feeder capacitor banks, ensuring that an optimum voltage profile is maintained along the feeder during normal operating conditions, and reducing peak load through feeder voltage reduction by controlling the transformer tap positions in substations and voltage regulators on feeder sections. Advanced algorithms are employed to optimally coordinate the control of capacitor banks, voltage regulators, and transformer tap positions.
- The topology processor (TP) is a background, offline processor that accurately determines the distribution network topology and connectivity for display colorization and to provide accurate network data for other DMS applications. The TP may also provide intelligent alarm processing to suppress unnecessary alarms due to topology changes.
- Distribution power flow (DPF) solves the three-phase unbalanced load flow for both meshed and radial operation scenarios of the distribution network. DPF is one of the core modules in a DMS and the results are used by many other DMS applications, such as FDIR and IVVC, for analyses.
- Load modeling/load estimation (LM/LE) is a very important base module in DMS . Dynamic LM/LE uses all the available information from the distribution network—including transformer capacities and customer monthly billings, if available, combined with the real-time measurements along the feeders—to accurately estimate the distribution network loading for both individual loads and aggregated bulk loads. The effectiveness of the entire DMS relies on the data

accuracy provided by LM/LE. If the load models and load values are not accurate enough, all the solution results from the DMS applications will be useless.

- Optimal network reconfiguration (ONR) is a module that recommends switching operations to reconfigure the distribution network to minimize network energy losses, maintain optimum voltage profiles, and to balance the loading conditions among the substation transformers, the distribution feeders, and the network phases. ONR can also be utilized to develop outage plans for maintenance or service expansion fieldwork.

- Contingency analysis (CA) in the DMS is designed to analyze potential switching and fault scenarios that would adversely affect supply to customers or impact operational safety. With the CA results, proactive or remedial actions can be taken by changing the operating conditions or network configuration to guarantee a minimal number of customer outages and maximum network reliability.

- Switch order management (SOM) is a very important tool for system operators in real-time operation. Several of the DMS applications and the system operators will generate numerous switch plans that have to be well-managed, verified, executed, or rejected. SOM provides advanced analysis and execution features to better manage all switch operations in the system.

- Short-circuit analysis (SCA) is an offline function to calculate the short-circuit current for hypothetical fault conditions in order to evaluate the possible impacts of a fault on the network. SCA then verifies the relay protection settings and operation, and recommends more accurate relay settings or network configuration.

- Relay protection coordination (RPC) manages and verifies the relay settings of the distribution feeders under different operating conditions and network reconfigurations.

- Optimal capacitor placement/optimal voltage regulator placement (OCP /OVP) is an offline function used to determine the optimal locations for capacitor banks and voltage regulators in the distribution network for the most effective control of the feeder vars and voltage profile.

- The dispatcher training simulator (DTS) is employed to simulate the effects of normal and abnormal operating conditions and switching scenarios before they are applied to the real system. In distribution grid operation, DTS is a very important tool that can help operators evaluate the impacts of an operation plan in advance or simulate historical operation scenarios to obtain valuable training on the use of the DMS. DTS is also used to simulate the conditions of system expansions.

2. Transformation of the Grid: Increasing Complexity

Distribution networks have not always been the focus of operational effectiveness. As supply constraints continue, however, there will be more focus on the distribution network for cost reduction and capacity relief. Monitoring and control requirements for the distribution system will increase, and the integrated smart grid architecture will benefit from data exchange between the DMS and other enterprise applications. The emergence of widespread distributed generation and consumer demand response programs also introduces considerable impact to the DMS operation. Smart grid technologies will add a tremendous amount of real-time and operational data with the increase in sensors and the need for more information on the operation of the system. Utility customers will be able to generate and deliver electricity to the grid or consume the electricity from the grid based on determined rules and schedules. This means that the consumers are no longer pure consumers but sellers or buyers, switching back and forth from time to time. It requires that the grid operates with two-way power flows and is able

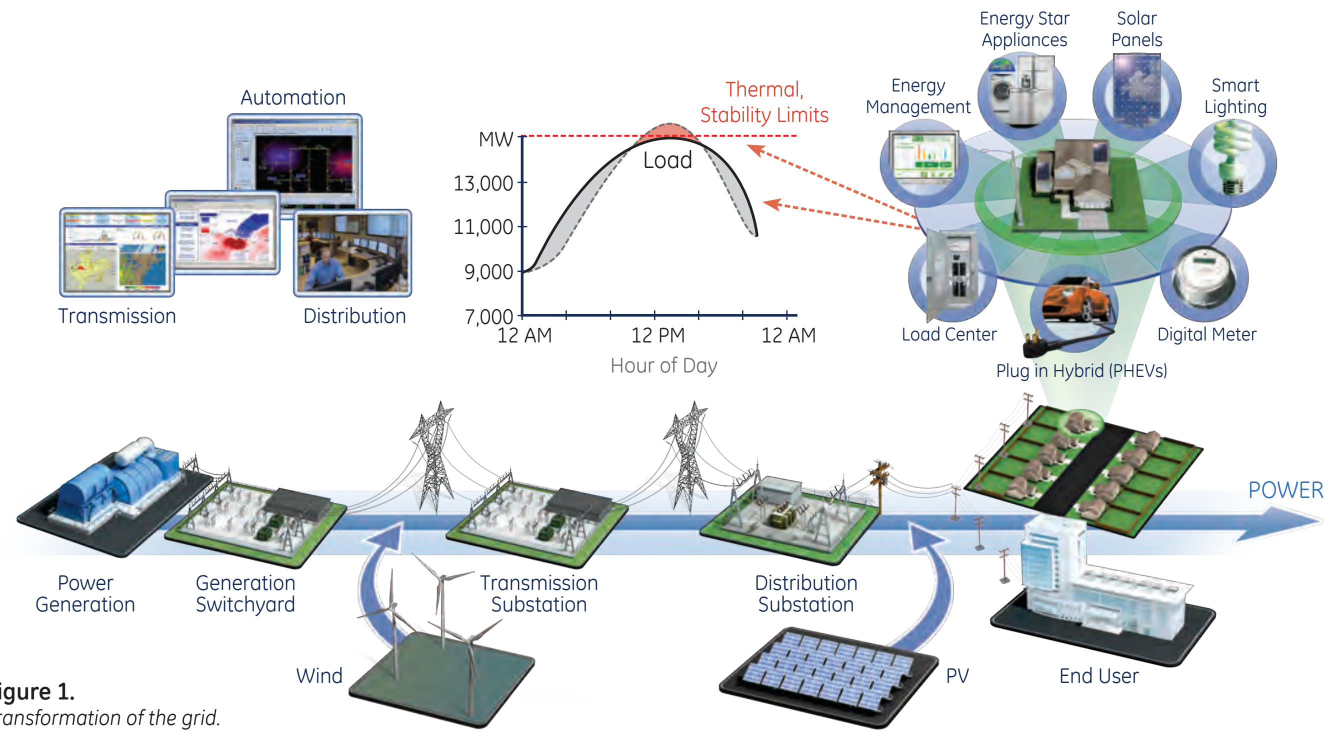


Figure 1.
Transformation of the grid.

to monitor and control the generation and consumption points on the distribution network. Figure 1 illustrates some expected transformation of the grid.

The distributed generation will be from disparate sources and subject to great uncertainty. The electricity consumption of individual consumers is also of great uncertainty when they respond to the real-time pricing and rewarding policies of power utilities for economic benefits. The conventional methods of LM and LE in the traditional DMS are no longer effective, rendering other DMS applications ineffective or altogether useless. The impact of demand response management (DRM) and consumer behaviors may be modeled or predicted from the utility pricing rules and rewarding policies for specified time periods, which can be incorporated into the LM and LE algorithms; this requires a direct link between the DMS and the DRM applications. When the DRM application attempts to accomplish load relief in response to a request from the independent system operator (ISO), it will need to verify from the DMS that the DRM load relief will not result in any distribution network connectivity, operation, or protection violations. The high penetration of distributed generation will require the load flow algorithm to deal with multiple, incremental, and isolated supply sources with limited capacities, as well as a network topology that is no longer radial or is weakly meshed. In a faulted condition, the distributed generation will also contribute to the short-circuit currents, adding to the complexity of the SCA, RPC, and FDIR logic.

3. Advanced Distribution Management Systems

A number of smart grid advances in distribution management are expected, as shown in Figure 2.

- Monitoring, control, and data acquisition will extend further down the network to the distribution pole-top transformer and perhaps even to individual customers by means of an advanced metering infrastructure (AMI) and/or demand response and home energy management systems on the home area network (HAN). More granular field data will help increase operational efficiency and provide more data for other smart grid applications, such as outage management. Higher speed and increased bandwidth communications for data acquisition and control will be needed. Sharing communication networks with an AMI will help achieve systemwide coverage for monitoring and control down the distribution network and to individual consumers.

- Integration, interfaces, standards, and open systems will become a necessity. Ideally, the DMS will support an architecture that allows advanced applications to be easily added and integrated with the system. Open standards databases and data exchange interfaces (such as CIM, SOAP , XML, SOA , and enterprise service buses) will allow flexibility in the implementation of the applications required by the utility, without forcing a monolithic distribution management solution. For example, the open architecture in the databases and the applications could allow incremental distribution management upgrades, starting with a database and a monitoring and control application (SCADA), then later adding an IVVC application with minimal integration effort. As part of the overall smart grid technology solution or roadmap, the architecture could also allow interfacing with other enterprise applications such as a geographic information system (GIS), an outage management system (OMS), or a meter data management system (MDM) via a standard interface. Standardized Web-based user interfaces will support multiplatform architectures and ease of reporting. Data exchange between the advanced DMS and other enterprise applications will increase operational benefits, such as meter data management and outage management.

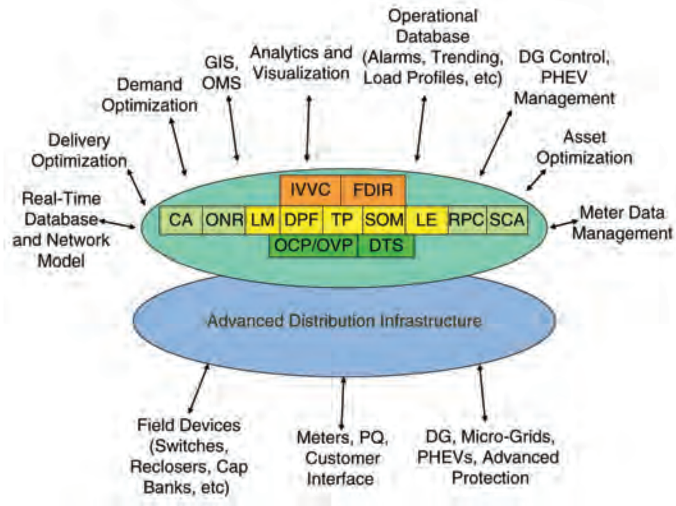


Figure 2.
Advanced distribution management for the smart grid.

- FDIR will require a higher level of optimization and will need to include optimization for closed-loop, parallel circuit, and radial configurations. Multi-level feeder reconfiguration, multi-objective restoration strategies, and forward-looking network loading validation will be additional features with FDIR.

- IVVC will include operational and asset improvements-such as identifying failed capacitor banks and tracking capacitor bank, tap changer, and regulator operation to provide sufficient statistics for opportunities to optimize capacitor bank and regulator placement in the network. Regional IVVC objectives may include operational or cost-based optimization.

- LM/LE will be significantly changed where customer consumption behaviors are no longer predictable but more smartly managed individually and affected by distribution response management.

- TP, DPF, ONR, CA, SCA, and RPC will be used on a more frequent basis. They will need to include single-phase and three-phase models and analysis, and they will have to be extended down the network to individual customers. Distributed generation, microgrids, and customer generation (such as plug-in hybrid electric vehicles (PHEVs) will add many challenges to the protection, operation, and maintenance of the distribution network. Small generation loads at the customer interface will complicate power flow analysis, contingency analysis, and emergency control of the network. Protection and control schemes will need to account for bi-directional power flow and multiple fault sources. Protection settings and fault restoration algorithms may need to be dynamically changed to accommodate changes in the network configuration and supply sources.

- Databases and data exchange will need to facilitate the integration of both geographical and network databases in an advanced DMS. The geographical and network models will need to provide a single-phase and three-phase representation to support the advanced applications. Ideally, any changes to the geographical data (from network changes in the field) will automatically update the network models in the database and user interface diagrams. More work is required in the areas of distributed real-time databases, high-speed data exchange, and data security. Take, for example, the interfaces and applications required to support roving PHEVs on the utility's (or another utility's) distribution network. Point-of-use metering and energy charge or credit must be managed and tracked on the distribution network. This is a challenge in terms of not only the additional load or potential supply (and related protection and control issues), but also the tracking and accounting of energy use or supply at various points on the distribution network or on a neighboring utility's distribution network. This will be a huge challenge for utilities and will lead to a significant change in data management and accounting—away from the once-a-month meter reading and billing of customers. The customer interface challenge is illustrated in Figure 3.

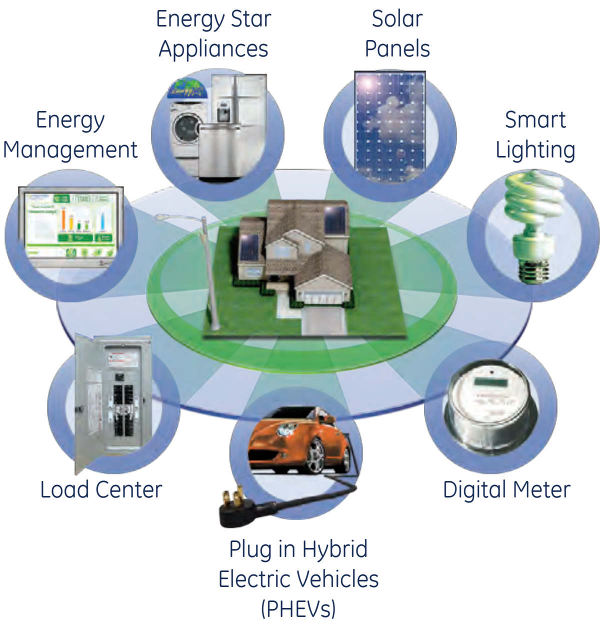


Figure 3.
The customer interface challenge.

- Dashboard metrics, reporting, and historical data will be essential tools for tracking performance of the distribution network and related smart grid initiatives. For example, advanced distribution management will need to measure and report the effectiveness of grid efficiency programs, such as var optimization or the system average interruption duration index (SAIDI), the system average interruption frequency index (SAIFI), and other reliability indices related to delivery optimization smart grid technologies. Historical databases will also allow verification of the capability of the smart grid optimization and efficiency applications over time, and these databases will allow a more accurate estimation of the change in system conditions expected when the applications are called upon to operate. Alarm analysis, disturbance, event replay, and other power-quality metrics will add tremendous value to the utility and improve relationships with customers. Load forecasting and load management data will also help with network planning and the optimization of network operations.

- Analytics and visualization assimilate the tremendous increase in data from the field devices and integration with other applications, and they will necessitate advanced filtering and analysis tools. Visualization of the data provides a detailed but clear overview of the large amounts of data. Data filtering and visualization will help quickly analyze network conditions and improve the decision-making process. Visualization in an advanced DMS would help display accurate, near real-time information on network performance at each geospatially referenced point on a regional or systemwide basis. For example, analytics and visualization could show voltage magnitudes by color contours on the grid, monitor and alarm deviations from nominal voltage levels, or show line loading through a contour display with colors corresponding to line loading relative to capacity. System operators and enterprise users will greatly benefit from analytic and visualization tools in day-to-day operations and planning.

- Enterprise integration is an essential component of the smart grid architecture. To increase the value of an integrated smart grid solution, the advanced DMS will need to interface and share data with numerous other applications. For example, building on the benefits of an AMI with extensive communication coverage across the distribution system and obtaining operational data from the customer point of delivery (such as voltage, power factor, and loss of supply) helps to improve outage management and IVVC implementation.

- Enhanced security will be required for field communications, application interfaces, and user access. The advanced DMS will need to include data security servers to ensure secure communications with field devices and secure data exchange with other applications. The use of IP -based communication protocols will allow utilities to take advantage of commercially available and open-standard solutions for securing network and interface communications.

4. A New Way of Thinking

Smart grids are not really about doing things a lot differently than the way they are done today. Rather, they are about doing more of what we already do—sharing communication infrastructures, filling in product gaps, and leveraging existing technologies to a greater extent while driving a higher level of integration to realize the synergies across enterprise integration. A smart grid is not an off-the-shelf product or something you install and turn on the next day; it is an integrated solution of technologies driving incremental benefits in capital expenditures, operation and maintenance expenses, and customer and societal benefits. A well-thought-out smart grid initiative builds long-term focus. It is not a one-time solution but a change in how utilities look at a set of benefits across applications and remove the barrier created by silos of organizational thinking. While current smart grid initiatives are typically driven by regulatory pressure and tend to focus more on the meters as a direct impact on consumers, we are likely to see more technology-rich initiatives after well-proven smart grid evaluations ("staged deployments"). Expect to see traditional distribution management evolve to include advanced application the smart grid.

070209-v3

A Paradigm Shift in Protection, Control and Substation Automation Strategy

Vahid Madani, Godwin Duru
Pacific Gas and Electric Company

Mark Adamiak
General Electric Co.

Abstract

The electric power industry is experiencing significant changes in protection, control, monitoring, recording and energy management. The requirements for improved efficiency in all phases of engineering, maintenance, and operation are examined. The demand for reliability has placed emphasis on service restoration and has highlighted the need for a more precise exercise of the art and science of protection & control both for local as well as the more complex schemes protecting the integrity of the interconnected grid.

This paper is a transformation journey in substation integration encompassing the components of new technology for a major power company in North America which has resulted in the implementation of tomorrow's technology today. The transformation blueprint is a blend of fundamentals using new technology with the vision of the future. The markers include elements of leadership and technical reasons, process for capturing the scope, harmonization of different plans and disciplines to a united vision, and justification strategies and cost analysis for significant capital investments.

The article then leads to the details of protection and control technology selection and application, design philosophy, implementation strategies, establishment of partnerships for protective relay feature developments. The paper then examines the skill sets needed for a companywide rollout program and lays the groundwork for the future directions. Both transmission and distribution challenges and solutions are presented.

Integration of protection and control functions such as stub bus, breaker failure interlocking, automatic restoration with voltage supervision, loss of voltage during source switching, local / remote access, and fail-safe operation mode are some of the challenges of integration described in this paper. The flexibility of the architecture to adopt the IEC 61850 process bus interface is also described.

Pioneering designs and visions influenced decisions that have propelled the journey from conception to reality are also presented including innovative concepts for "drop-in plug and play" control building that have become the hallmark of future system protection.

The obstacles, struggles, and victories gave rise to a prototype philosophy including the modularization and achievements in new protection and control standards. This groundbreaking work has led to the company's commitment to upgrade over 200

substations companywide by 2014. The progress detailed in this journey has ignited other professionals and companies to follow the lead and to become an advocate of this pioneering path.

1. Introduction

The electrical grids are, in general, amongst the most reliable systems worldwide. These large interconnected systems, however, are subject to a host of challenges – aging infrastructure, need for siting new generation near load centers, transmission expansion to meet growing demand, distributed resources, dynamic reactive compensation, congestion management, grid ownership vs. system operation and reliability coordination, asset management and life cycle planning, etc.

The aging infrastructure is at the center of the challenges facing today's expected grid reliability, availability, and demand for faster restoration. The advancements in microprocessor and network communication are amongst a host of technology enablers that provide the opportunity for engineering a sustainable and reliable infrastructure.

While microprocessor relays have gained full industry acceptance, there is a large number of legacy electromechanical and solid state devices still in operation resulting in increased maintenance and failure costs as well as concerns that those costs will increase. It is not trivial to determine end of life and probability of failure for electromechanical relays. Spare parts availability for older relays is only one issue. Experience shows that in some cases legacy relays have long exceeded their life expectancy and continue to perform reasonably well, particularly if well maintained. Reduction in the skill set and knowledge base familiar with troubleshooting, testing, and repairs of the old technology is across the power industry spectrum from manufacturing to end-users [1], [2].

The probability of failure and replacement needs for equipment can be approximated by the following criteria: age; maintenance practices and records; obsolescence; visual inspection; industry experience with certain devices; in-house knowledge; and criticality of failure. However, it is not easy to economically justify relay upgrades entirely based on probability of failure and replacement needs. Reluctance to upgrade to microprocessor relays is further emphasized by complexity associated with increased functionality (e.g. settings), need for firmware upgrades, short life span of microprocessor technology, and the overall need to change the protection system philosophy and design. In addition, while digital relays provide wealth of data, users may be faced with data overload. It is often the case that even data already available are not used or even collected.

Latest technological advancements in power system protection and control (P&C) are important enablers to meet the challenges of the electrical grid in the 21st century. Evolutions in protection and restoration principles for interconnected power grids are made possible by the wide-area measurement systems [3]. Real-time adjustment of the protection system's security-dependability is within reach given the advancements in technology and investments in communication systems infrastructures.

This paper is a summary overview of initiatives on transmission and distribution substation automation and integration with several different parallel strategies that were harmonized in mid 1990s to a united vision for a major power company in North America. The paper describes the process from the initial stages of identifying the scope to strategies for justification of such major initiatives, details of selection, application; design philosophy, implementation strategies, partnerships and resources, and required skill sets are described. Many of the success and lessons learned along the way are also presented.

2. Background and Reasons for Migration

In the early 1980s, Pacific Gas and Electric Co. (PG&E) started to look at use of numerical devices on its 230kV and below transmission systems. The approach started with replacement of one level of protection with microprocessor based devices and soon expanded to move towards replacement of protective devices on per terminal (panel) basis. Reasons for the step-by-step conversion process are attributed to a number of factors including the need for:

- Field experience with the then new technology
- Development of new standards to identify full range of compatibility with the existing conventional practices
- Determination of the financial merits

It was then identified that replacement by panel only results in protection equipment upgrades yet does little to modernize the overall aspects of power system operation and that a holistic approach was needed. In addition, the relative number of equipment terminals that would need to be upgraded would take several generations to accomplish. Given the rapid developments in technology, it would not be feasible to maintain course both from product manufacturing support of "out dated" equipment and from the utility perspective of not making use of latest technological advancements and the benefits offered to the industry as a whole.

In the early 1990's PG&E was facing difficult economic decisions in its transmission business. Customer unrest over increasing prices, greater demands on limited budgets and increasing new business needs required a new approach to asset management. In addition, device and panel replacements were exceedingly costly. With multiple forces pulling in different directions, and armed with the knowledge from the gradual panel migrations, PG&E started to study a new paradigm for budgeting limited dollars for aging control room equipment.

At the same time the industry was quickly developing new automated systems for control and more modern flexible protection and multifunction capabilities which were being introduced to the market. The possibility of the new automation [1] and protection packages offering greater reliability and customer service led to more focused evaluations. Various options were explored and a new vision and strategy was initiated – the Modular Protection, Automation and Control (MPAC) concept was selected to be studied.

2.1 Vision

The vision was to create integrated systems and automated applications that use data from transmission and distribution facilities to effectively process and act on information to operate and maintain the electric transmission and distribution systems, Figure 1.

Figure 1.
MPAC Vision

[1] Since many functions in today's substations are automated with regards to system faults and restoration response, many believe that substations are already automated. Automation used in this paper is in the larger sense. Substation automation is the use of microprocessor based devices for metering, monitoring, controlling and protection of substation functions. Automation allows for the sharing of data between devices over a local area network and accessing substation information remotely.

Developing a common vision for the substation of the future was an important first step. The vision had three key drivers:

- Safety
- Cost reduction
- Improved reliability

With these drivers in mind, three areas of focus were defined. These areas later became the major initiatives:

- Information technology and management
- Communications with different groups
- Equipment performance; and work practices

The new systems needed to respond faster, remain price-competitive, improve customer reliability, and do it all with fewer resources.

2.2 Strategy

In order to determine the feasibility and to identify road maps a set of basic strategies would be needed. The strategy was based on some fundamental objectives - To improve safety, efficiency, service reliability, and manage the cost of transmission and distribution Operations, Maintenance, Planning and Engineering through the integration and the implementation of automation applications, Figure 2.

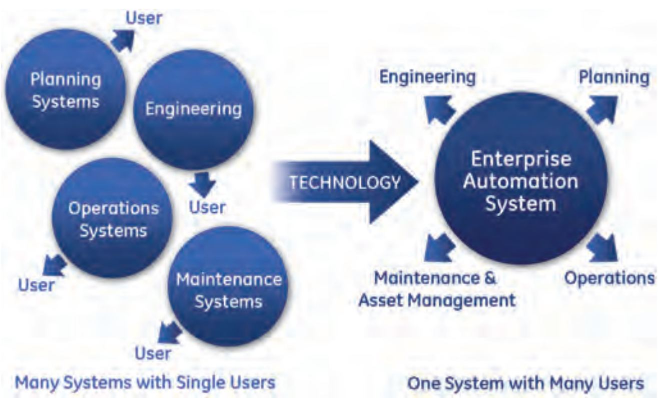


Figure 2.
Integration and Automation Objectives

The initiative would require technical and human factor considerations and many other related aspects for system-wide implementation which are covered later in the paper.

Some of the factors in strategy explored included:

- As equipment wears out, replace with the new generation of devices, systems, or schemes
- Build new substations in the new image
- When opportunity knocks, follow the blueprint

Management of the above three initiative areas was intertwined in order to:

- Continue with incremental migration but proven technologies to achieve gradual benefits and gain practical experience
- Build a specification for the "Substation of the Future" that will be the standard blueprint for all projects by the year 2002

Another key step in the development of the strategy included:

- Site visits to other power companies that had considered or had implemented similar concepts
- Discussions with manufacturers of protective devices and system integrators to identify their offerings of products and systems. Although the team was interested in what the vendors already offered, PG&E was even more interested in where the manufacturers were headed

Armed with better information in terms of manufacturing and technology as well as the direction of others in the industry, PG&E had a clear basis for its own strategy implementation, or migration path. The strategy would be continually updated as time passes and the future business and technology environments reveal themselves.

2.3 Initial Stages of Expenditures on MPAC and Prototypes

Cost justification for comprehensive upgrade programs comes from combination of various benefits. Those benefits do not result only from replacing protective relays, but deploying an integrated system using enterprise Information Technology (IT) architecture to enable collecting required data and processing and distributing information when and where required for use by various applications and users.

The initial MPAC program for PG&E came out of a budget process which focused on single year expenditures for multiple projects of different types competing against each other for funds. With this approach, items like "new business" and distribution lines, and other projects serving the immediate needs of the customer generally received the bulk of the funding, while items like transmission or distribution automation did not attract much funding. While the promise of automation seemed hopeful and was being promoted within the industry, the cost/benefit case could not be made to justify the overall scope. Where power companies and vendors had gone forward, they did so based on other reasons such as aging workforce, equipment obsolescence, or reliability needs. The traditional business cases by themselves were not sufficient.

Taking a longer term prospective and a program approach, a budget plan was prepared for other major capital projects over a five year timeframe; i.e. wood pole replacements. This budget planning approach provided funding opportunity to focus on grid infrastructure revitalization over time.

With funding realignments, multiple efforts had to come together to make the MPAC concept a success. From a strict economic perspective (one of the realities of budgeting in a large corporation with competing priorities), there was not much incentive to replace working electromechanical or solid state devices with newer and more feature enhanced devices. However, with a program approach to the larger needs of the substation, and an aging infrastructure in existing control rooms, the need for determining the overall reliability performance measures, and managing infrastructure assets the idea caught hold. By combining automation, aging equipment, and integration of functions using the new microprocessor capabilities, a case could be made to replace the equipment.

At the same time, many technical details needed to be worked out. Development of the details such as the system architecture, levels of integration, harmonizing PG&E's protective relay selection and application philosophy, automation and SCADA / HMI (Human Machine Interface) hardware and practices, and other requirements led to the concept of pilot projects in the mid 1990s.

The first pilot involved installation in an existing building of new racks, equipped with then latest numerical devices. The cost, however, to put in new racks in an existing control room was extremely high. Again, the economics would not support the approach. Attention was then turned to a more modular approach of replacing the whole control room.

The first pilot project involving a completely new control building showed promise from an economic cost benefit standpoint. In fact, when compared to a more traditional PG&E approach of building a custom building, a savings of 20-25% seemed achievable. This pilot project then became the turning point for justification of future modular buildings (MPAC). However, in order to have a systemwide program, many factors had to be considered and processes established or enhanced. For example, standardization of equipment, levels of integration, establishment of policies for network and information technology (IT) infrastructure expansions, development of engineering standard schematics and setting templates, automation diagrams and standards, and preparation of test programs namely, Factory Acceptance tests (FAT) and Site Acceptance Testing (SAT) for control building. Equally important in the design and engineering development was maintenance testing over the project life cycle that had to be incorporated in the new paradigm.

By design, the first automation pilot project was somewhat limited in functionality. The primary goal was to achieve small advances with complete certainty and learn from the experience, rather than try to solve all automation problems in a single stroke. Thus, attention focused on establishing connectivity through modems and collecting information, as well as to provide means for basic SCADA functions. This project was completed successfully, and has been performing well. The primary concerns were with the accuracy of the data and false signals that were resolved after further equipment calibrations.

Some information provided by the first pilot project demonstrated the capability of new devices to provide information which surpasses the typical data available from traditional SCADA. The new system collected load information from redundant protective devices which allowed for telemetry validity check. In traditional SCADA, one set of transducers collected load information, and if the transducers drifted there was no built-in check to diagnose the problem. The newly installed devices also have the potential to monitor breaker wear for example. Breaker operations, as recorded by the relays, were not being entered directly into the reliability calculations at this stage pending development of databases.

The second pilot project was more ambitious and included building a new control room and installing a completely new integrated information and control system. The plan included building a completely modular control room, built off-site and delivered ready for operation. Traditional RTU (Remote Terminal Unit) systems and numerical multi-function devices were used for SCADA and for Protection & Control respectively. The idea included minimizing, and if possible eliminating, traditional control switches and providing a Human Machine Interface (HMI) for operational needs.

3. Integration and Reliability Considerations

While the modularization concept was being explored, the evaluations in technology associated with numerical devices were being conducted by another group at PG&E. The System Protection and Controls Department was exploring the ideas of integrating many protection functions and automatic reclosing features. The ideas ranged from continuing with gradual migration of features to delivering significant improvements in dependability, security, and greature reduction in hardware. Several factors needed to be examined including:

- **The architecture** of integration.
- **Level of integration** and associated complexities. For example, would it be acceptable to integrate line protection, breaker failure detection, stub bus protection, and automatic reclosing into one device?
- The **capacity and processing speed** of the hardware; e.g. could a device perform its primary protection function while it is also providing SCADA or HMI functions?
- **System reliability**, will it be compromised compared to traditional methods, and to what degree if any?

Since similar discussions were starting to take place in other electric power companies, the approach considered was to discuss the integration ideas and concepts with technical committees at the Regional Council meetings. Exchange of ideas and reaching for common grounds provided further support to PG&E.

4. Protection Reliability, Hidden Failures & Unintended Operations Detection

Several key benefits for migrating to the new paradigm are highlighted in other publications [4], [5]. Technological advancements in modern protective devices, user selectable supervisory elements, and monitoring features in modern devices further supported the justification for proceeding with the development of the blueprint.

4.1 Protection Reliability

The availability for proper operation of protective relays for various system conditions is one of the most important factors in improving system reliability. Detecting hidden failures is a critical task that requires good understanding of the principles of operation of the protective devices, their self-checking functions and their limitations, as well as properly defined methods and procedures.

Security and dependability are two measures of reliability. Dependability is defined as the "Degree of certainty that a relay system will operate correctly", and Security: "Degree of certainty that a relay will not operate incorrectly", Figure 3.

	NO-Operation	Operation
	RELIABLE	
Correct	Secure	Dependable
	UNRELIABLE	
Incorrect	**Undependable**	**Insecure**

Figure 3.
Definition of Protection Reliability [4]

4.2 Monitoring the Protective System - Identification of Hidden Failures

A failure of a protective device may be caused by many different factors, including not only failure of the device itself, but also of components of the overall substation protection, control and monitoring system.

5. Integration of Protection and Control for Improved Asset Management

The key to the asset management concept is three fold:

- Replace the entire control building – replacing components and racks is too costly and operationally disruptive.
- Secure a program approach – develop a long term plan with multi-year funding.
- Standardization – Treat the whole control room like a commodity, not a custom application. Develop a standard design, procurement, and specification for the entire building including the protection, integration, and automation components to be able to bid out the specification to selected venders.

The need to justify the preferred and perceived most cost effective option resulted in preparing a comprehensive listing of benefits for the standardization which included:

- Utilizing the features of new devices and systems to reduce the amount of equipment, floor and panel space, and hardware failures while improving protection performance.
- Reduced installation and maintenance cost for protection and control equipment. The ultimate goal should be to eliminate time-based maintenance while improving availability, security, and dependability. For example, manual relay testing could be significantly reduced.
- Improved dependability and security, while drastically reducing the number of units required, and complying with or exceeding all requirements by the regulators.
- Reduced operating costs. No or minimal human intervention is needed to rapidly determine status, event triggers, event reports, equipment performance, etc. Settings could be securely managed remotely using well-defined procedures.
- Accurate and timely fault location to the dispatch personnel. It could also help with identifying the cause of both permanent and momentary faults, weak spots in the network, and aid in calculating tower footing resistance, and system parameters such as the line impedance [7].
- Equipment condition data that would help in asset maintenance savings and prioritization of capital and O&M investments as a part of the overall asset management strategy.
- Improved network security, as well as replacement energy and congestion savings. The latter two are results of minimizing equipment loss and, consequently, avoiding both a need to replace energy on the spot market and congestion.
- Enhanced system restoration.
- Real-time system prognosis and capability for adaptive protection and control.
- Reduce down time.
- Easily adaptable to advancing technology – Ease of upgrade without impact to wiring.
- Information as opposed to data rapidly available – Helps in information broadcasting, automatic identification of trouble spots, and client / customer satisfaction.
- Cost savings in implementing condition based maintenance - Improved asset management decisions based on solid statistical data.
- Identifying weak spots in the system.
- Reliability improvements resulting from avoided failures due to continuous monitoring and better T&D planning using statistical data.
- Cost savings in crew overtime.
- Productivity improvements through integration of IT systems and databases.
- Better inventory control.

The comprehensive approach to standardization provided yet another key pillar towards integration.

6. Roadmap to the Development of Architecture

The experiences gained from the trial projects provided many insights and the lessons learned could be transferred to other projects. The trial projects also shed light on some of the absolute requirements in order to launch a full scale implementation. Some of the requirements included:

- Large scale strategy for systemwide roll out
- Development of system architecture and roadmaps for testing and training new users
- Development of Engineering design standards and supporting documents such as logic drawings, test procedures, and recommended maintenance steps

Before the system architecture could be developed, however, other requirements had to be met. The equipment needed to be evaluated for flexibility and performance in meeting the majority of PG&E integration and automation applications. Different bus configurations such as breaker and half, (BAAH), Ring, or Double Bus Single Breaker, would have different interlocking, control, and / or automation requirements. Also, automation requirements had to be defined and different substation automation hardware had to be evaluated for best flexibility, performance, and overall cost.

6.1 MPAC Core Team

In order for the vision to come to fruition, a cross section of expertise and interfaces with various departments was formed. The MPAC core group members had to have vision, subject matter expertise, and the dedication needed to make this company initiative a success. These individuals had to think outside the box, foster a paradigm shift, and come up with a plan that was innovative, cost effective, reliable, and practical. The complexity of the task required involvement from many affected departments.

Every group (Department) had to have ownership and contribute in the development of the new plan. Each subject matter expert (SME) was responsible for representing their respective work group and providing the expertise from the respective expertise. Therefore, each core team member was charged with communicating milestones and acting as a conduit for feedback to the MPAC core team.

6.2 Need for Partnership

Initial discussions focused on partnership with protection and control device manufacturers and the possible need for an integrating company, Figure 4.

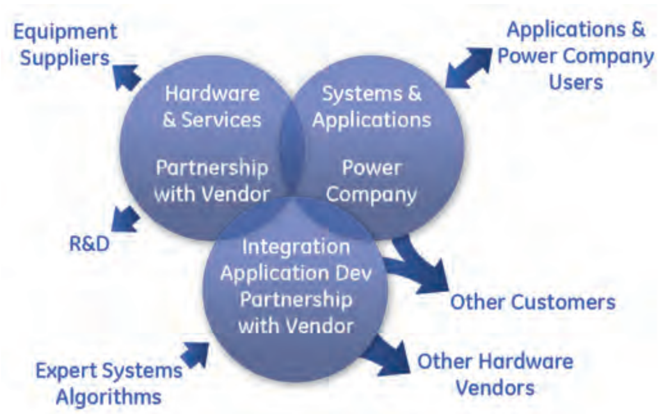


Figure 4.
Partnership Model Considerations

Under this scenario, each component of the model would contribute an equal amount of knowledge, skill sets, processes, and development capability to the project as needed, Figure 4.

Some of the key benefits of the partnership included:

- Cost reduction and revenue sharing
- Product and technology development
- Efficiency and process improvement
- Standardization to reduce costs
- Knowledge sharing - Industry experience sharing
- Quicker turnaround
- Ability to influence suppliers
- Training of partners on each other products or standards
- Better utilization of resources and resource sharing in peak periods
- Project Management support
- Streamlined procurement process namely, request for information (RFI) and request for proposal (RFP)

6.3 RFI Process for System Architecture

In order to avoid the need to obtain completely new and separate bids every time, the PG&E MPAC team wanted to establish standardized pricing as much as possible before projects were initiated or procured. Bidders were required to propose pricing that would remain effective for the respective year subject to certain project defined modifications which may alter the final price of a given project. The team also included an evaluation process as part of the performance of the bidders for the year that a project would be granted. The idea was focused on partnership as opposed to a pre-bid evaluation based on price. To facilitate the concerns and risks associated with initial configurations "targeted price" proposals were accepted from the bidders as to their recommendations and technical requirements for partnership. Also, incentives were put in place for sharing the savings below the "targeted price".

7. Integration and Object Model Development

One of the initial tasks undertaken by the core team was the development of the major requirements such as:

- Should integration be limited to consolidation of protection features and components only? Should stub bus, breaker failure, automatic reclosing with voltage supervision, etc. be all integrated?
- Could PG&E policy in the application of two levels of protection with no potential for common mode failures in products, scheme performance, or associated interlocking with high-speed or slow speed reclosing be maintained, without sacrificing reliability and security?
- Should metering and operational switches be integrated? Would local / remote function be integrated and how?
- Should the auxiliary tripping relays be integrated or maintained? Would the latching function during power loss be available if the function is to be integrated?
- How would the MPAC station interface with remote terminals that would be not be immediately scheduled for conversion to integrated protection and control (IPAC)?
- How to maintain control functions similar to the existing practice in functionality and in "Look and Feel" when the control function is to be exercised from the front of the panel? – e.g.: One control switch location, one switch to control circuit breakers, one switch to control group settings, etc.
- How to maintain visual information on the front of the panel to complement any computerized HMI.

- How to maintain “multi-directionality” of controls and information between local panel information, the HMI at the station, and the SCADA system at the control headquarters.

- How would the MPAC station interface within an existing established substation without significantly increasing the project scope? For example, a two winding transmission transformer bank (i.e.; 230/115kV) with two different MPAC buildings for the respective bus voltages? If the MPAC was to be installed at the 230kV site, and the 115kV control building should not be required to become MPAC.

- Interface with neighboring companies that do not have MPAC substations or may opt to stay with their own standards.

- Would SCADA be incorporated as part of consolidation and integration of protection and control components?

- Would SCADA be a distributed SCADA or a centralized system per station or per control building?

Given the many challenges to face, and armed with the in-depth knowledge of industry and internal practices, the development of an object model was conceived to better visualize the interactions of the various functions, Figure 5.

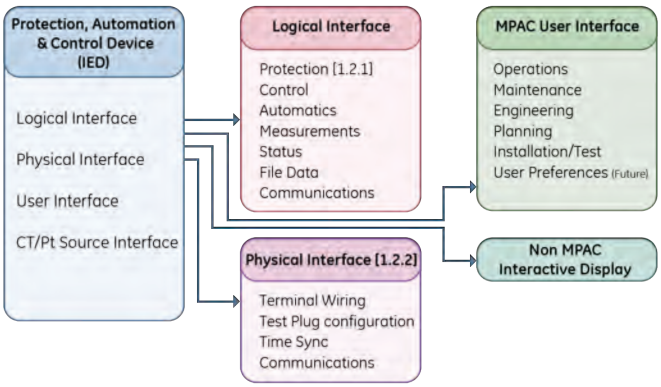


Figure 5.
IED Object Mode

Use of the object model would allow consistency amongst applications, suppliers, and partners. The high level object model included components such as:

- Logical Interface
- Physical Interface
- User Interface
- CT/PT Source interface
- Interface with non-MPAC
- Reclosing – Both raid or high speed and time reclosing

Throughout the development, the standard / core team maintained focus on design safety, reliability performance, internal practices, and the overall cost.

The core team also recognized the human factors such as need for knowledge transfer, training, and other related aspects for systemwide implementation and strategies that needed to be developed in parallel with the technical discussions.

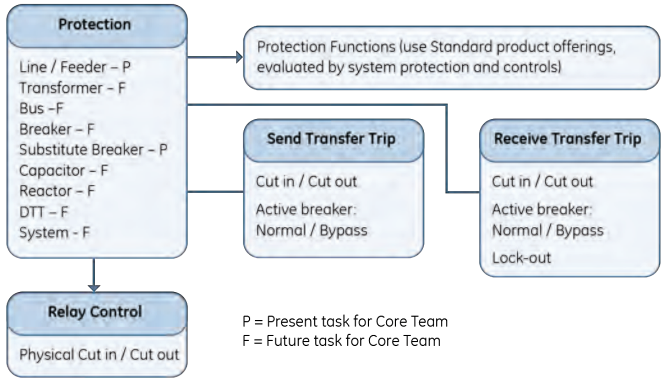


Figure 6.
Protection Object Model

One of the initial tasks was the development of engineering and protection design standards. They also recognized that the best way to succeed would be to implement the development of standards one item at a time while considering the various elements of the object model.

Figure 6 shows a simplified Protection object model for components that may exist in a substation. Figure 6 also shows that the initial task was development of integrated standards for “line Protection”. As a component of the integrated system was developed, it would be rolled out for implementation while other components were being developed [5]. This concept of phased roll out also allowed participation by a larger group of field personnel or engineers as projects would start to be designed and fabricated based on the new standards. Appropriate suggestions would be incorporated both in the components already developed and also for the components that were being developed.

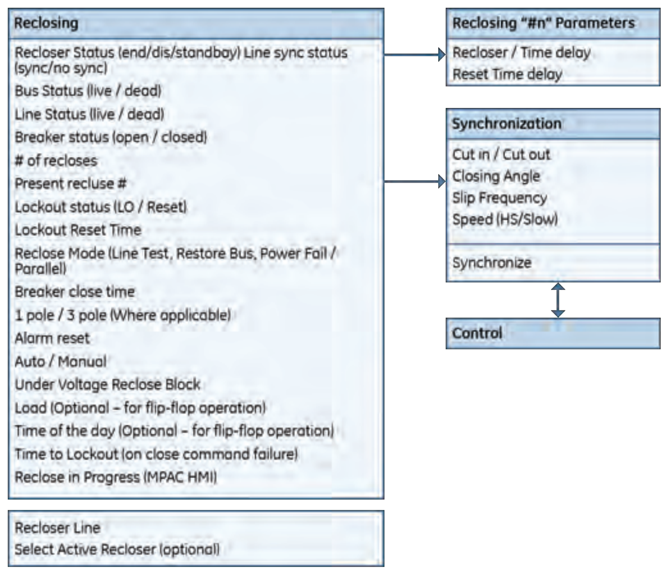


Figure 7.
Simplified Object Model for Reclosing (both rapid and time reclosing)

Details of line protection object model and various types of protection applications including direct transfer trip and third party interconnections were then developed [5]. Other object models such as Automatic reclosing and Human Machine Interface (HMI) were also important in design of standards. Automatic reclosing encompassed rapid reclosing (both with or without synchronization supervision to meet existing practices for different applications) and time reclosing and associated interlocking for situations that required a lockout condition, Figure 7.

For the HMI development, the challenges varied between different environments such as a brand new building (MPAC), or when multiple buildings are needed due to station or bus configuration, transitional projects in existing substations, and interactions with SCADA, Figure 8.

Another key element in the design was maintaining reliability in control functions. In the traditional control, highly reliable control switches were used for controlling protection and also elements. For example, only one setting group selector switch would control the desired setting group for both levels of a line protection. The new integrated design needed to maintain conventional operational control concept to one device (one virtual switch) while maintaining the reliability and operational flexibility ("independence") when the device assigned to perform the group setting switch function was removed or became unavailable. Also, the position of the control switch was visible in the traditional applications, where control was performed locally. These considerations led to the use of LED indications to reflect the position of equivalent "Switch" functions. Also, the requirements for reliability and availability for metering and control functions drove the decision for distributed SCADA / computerized HMI functions. Since in PG&E's practice each piece of equipment has redundant multifunction devices used for protection functions, it would be possible to use the integrated concept for protection and reclosing as well as for traditional physical controls and maintain functional dependability for operational / switching needs. In the new MPAC design, the traditional station metering and station control switch function was assigned to one level of multifunction devices (Set "A" protection and control), and the second level multifunction protection and control device (Set "B") was used as the gateway for HMI / SCADA.

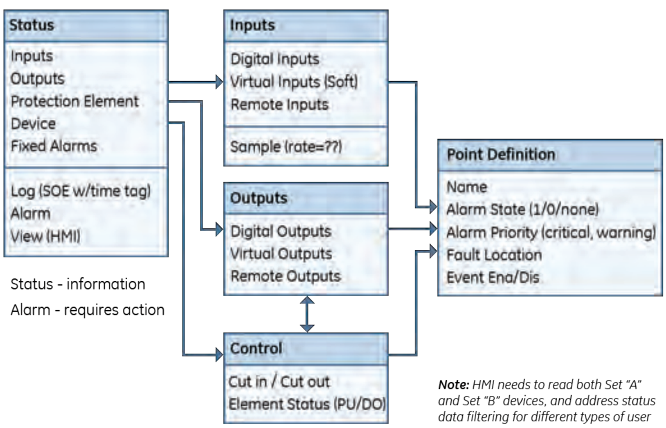


Figure 8.
Simplified Object Model for HMI

Also, all timed based automatic reclosing functions have been programmed into the Set "A" device. Other functions have been designed to be in a combination of both Set "A" and Set "B" devices. For example, a breaker can be manually closed from the front of the panel or via the station HMI. In the case of the front panel, the Set "A" LED indications and the Set "A" device display have been designed (programmed) to inform the operator of the voltage, frequency, angle, and direction of voltages on the two sides of the breaker, as well as a dedicated LED to inform the operator of the closing angle being in the acceptable range for closing the respective breaker. Likewise, the synchroscope display on the HMI is designed to reflect the voltage vectors from each side of a circuit breaker. When the vectors are in the same quadrant and approaching each other, the operator can click on the close command and the device synchronizer function will close the circuit breaker when appropriate.

8. Development Roadmap and Standards

The conventional protection and control schemes used many discrete components and auxiliary devices. With the additional capability of multi-function devices it was be possible to minimize use of auxiliary equipment and include more of the features within the devices. The new microprocessor devices contain more than one protection scheme or feature. For example, backup, breaker failure, reclosing, and stub bus protection.

Another major factor to improve overall performance and system reliability was the goal to standardize on the design, while reducing overall project cost over the life cycle. This concept required standardizing on the size and type of building, type of equipment installed within the building, and the various schemes.

The success of the concept would depend on standardizing on many key factors such as:

- The buildings
- Protective schemes
- Switchboard layout
- Engineering
- Training
- Procurement process
- Test and commissioning

Standardization would also lead to cost stabilization and reduction while improving system and service reliability. This concept led to forming partnerships with some manufacturers. At the same time it was very important that the performance and functionalities would not significantly change. Many of the traditional functionalities have been enhanced based on many years of practical experience and lessons learned and have been reflected as part of fundamental practices.

Development of such new standards required resources with knowledge of internal standards, understanding the reasons for previous practices, expertise in industry best practices, and vision to develop a new generation of standards.

Process improvement was incorporated as part of the initial phases of the vision development and roll-outs which allowed the core team along with the respective building manufacturer to critique the project and go over the successes and failures [9]. From the discussions, the processes could be improved and further cost reductions could be captured by both the builder and the company without sacrificing performance, safety, or reliability. Then, the core team's job was to discuss the various issues and find ways to improve the process itself. For example, the period from 2001 to 2003 was used to firm up the design and the supporting standards for the MPAC buildings and systems. While the development of the interlocking logics between various elements of power system equipment moved forward, some elements such as the interface with the devices and the HMI architecture needed more time to be reviewed and options examined.

The Remote Terminal Unit (RTU) was initially replaced with a Data Concentrator that would offer the following:

- A secure network interface for remote access by engineers and others
- Survive a rugged substation environment
- An embedded processor and no hard disk
- Communicate with one device using the device native protocol (serial)
- Communicate with the second level device using Modbus TCP/IP protocol (LAN)
- Communicate with the Substation HMI using in-house (PG&E) protocol

After 2003, the Substation HMI software was converted from the third party supplier to the software being used at the switching centers. This approach offered consistency between the displays used for operating the systems, and would eliminate the need to develop and maintain two different databases. The database and displays developed for the substation could be loaded directly into the switching center systems. In this architecture, the substation HMI would poll the Data Concentrator using DNP3 protocol and would communicate to the switching center using a TCP/IP protocol with three levels of security.

A system architectural redesign was later implemented to have the substation HMI server communicate directly to the multifunction devices. This alternative became available due to following two changes in the system architecture.

- First the SCADA program used for the HMI and at the switching station was revised to provide the capability of DNP master protocol. This change provided the capability to the SCADA software to poll the IED devices directly.
- The second change was the development of a secure isolated wide area network with dedicated routers. This new WAN is used solely for SCADA and operational data and the new routers were selected to provide security and user authentication. The additional new security features provided by the new WAN routers eliminated the requirement for providing access and security functions within the Data concentrator.

The SCADA system direct IED poll concept was successfully tested in the Engineering Laboratory. A second full scale test was also run on a large MPAC building that was in a PG&E substation but not connected to the power grid equipment at the time of the tests. This test was also successful so the future designs will no longer needed the data concentrator. Furthermore, the new architecture reduced the site acceptance time from three weeks to less than one week.

8.1 Integrated Data Management

Figure 9 shows a hierarchical information routing architecture where the devices (redundant or non-redundant) are using different protocols and communication at the substation level. For example, Set "A" and Set "B" protection and integration devices are using different communication cables and protocols. Likewise, redundant System Integrity Protection (SIPS) devices "A" and "B" have different topology in network connection.

This concept includes significant use of messaging (IEC 61850 for protection and control) that have been applied to both transmission and distribution switchgear. At the substation level today, the IEC 61850 is used for protection, control and interlocking [10]. A next step at the Enterprise level would be implementation of IEC 61850 to migrate from the DNP protocol.

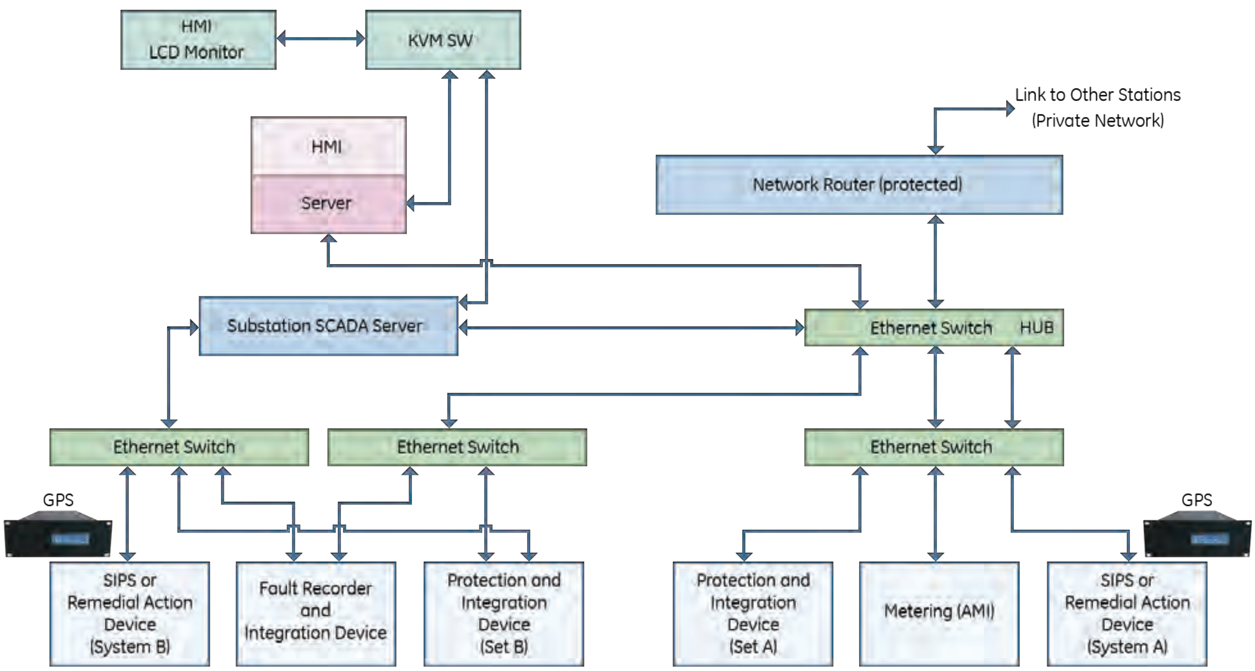


Figure 9.
Substation Network Showing Different Types of Equipment with Different Network Protocol

Similar to the protection and integration standardization efforts, the next steps include development of standards for use of IEC 61850 for Automation and identification of migration path to a complete communication based systems between the substation and the Grid Control both at the transmission level for real-time applications at transmission (i.e., link to EMS) or distribution system. Synchronized measured values are also available at the substation level and are part of the architecture of the future for real-time measurements (as opposed to state estimation).

The Ethernet switch selection and standardization is also important. In the era of rapidly advancing technology, clear roadmaps should be developed to allow migration and gradual transition while operating the grid over the life cycle. Equipment tracking mechanisms should be applied for ease of identifying brand, equipment location (substation), technology applied (i.e: 10 mbps vs. 100 mbps Ethernet switch).

9. Application of IEC 61850 for Protection

One of the elements of the object model included the development of standard applications for protection and control using UCA / IEC 61850. Development of this object model requires listing of benefits, identifying adverse functional impacts, training of resources, and cost to name a few of the considerations.

Furthermore, deployment of this object model would also require comprehensive and fully developed setting templates, logic drawings, and tools that would allow protection and automation engineers to assist technicians and control building contractors during commission testing, FAT and SAT.

9.1 Benefits of IEC 61850 for Protection Application

Benefits of the IEC 61850 for protection applications are described in [5]. Highlights include Design, Monitoring, Application, Asset management, etc. Below are some of the benefits in using IEC 61850 for protection interlocking and automation:

- Self Monitoring and Alarm – Continuous real-time status of control point communications from the source device to the implementing / receiving device for failure anywhere in the circuitry.
- Improved flexibility in design
- Ease of applications when I/Os are limited - Minimizes use of auxiliary devices – Less hardware, less components, less monitoring, more reliability.
- Prevents potential for mixing DC circuits, for example, when inputs or outputs are limited.
- Reduced implementation and testing time and cost
- Programmable timing and loss rate monitoring

Data sharing benefits for automation, asset tracking, and maintenance include:

- Remote system monitoring
- For SCADA Data
  - Superior Asset Management options
  - Condition monitoring of primary equipment
  - Power Quality Information

Other large scale benefits include:

- Exchange of Synchronized phasors data between PMU devices via GOOSE which would better enable applications such as wide-area out-of-step.
- Potential for bringing synchronized phasor data via GOOSE to phasor data concentrator (PDC)
- Ease of use with optical sensor and merging unit technology

9.2 Challenges of Application IEC 61850 for Protection

Below is a listing of some of the challenges in implementing the IEC 61850 GOOSE for protection and control:

- Adequate training of the protection engineers
- Adoption to existing substation automation concepts and changes in the specification and design process
- Conformance Certification of Devices to IEC 61850
- Tool for variety of purposes, for example:
  - Advance application development
  - Documentation of engineering design – Substitutes for Wiring and Schematics
  - Mapping
  - Performance tracking
  - Configuration and testing
  - Troubleshooting and Maintenance
- The protection engineer will need to develop some basic understanding of the:
  - Engineering approach with the use of the configuration language
  - Concepts of the object models and the basic communication services
  - Ethernet technology with switches and priority tagging

9.3 Practical Examples of IEC 61850 GOOSE for Protection and Control Interlocking

Figure 10 shows a simple interlocking example used for automatic reclosing in a breaker and half bus configuration. In this example, each breaker has a multi-function breaker control and reclosing device. Each breaker can be independently selected in advance, by the operator, to be the designated breaker for line reclosing, or automatic transformer restoration, when power system conditions would allow the breaker to close [5]. Other examples include breaker failure interlocking, breaker maintenance interlocking with bus differential and middle breaker in the respective bay, etc.

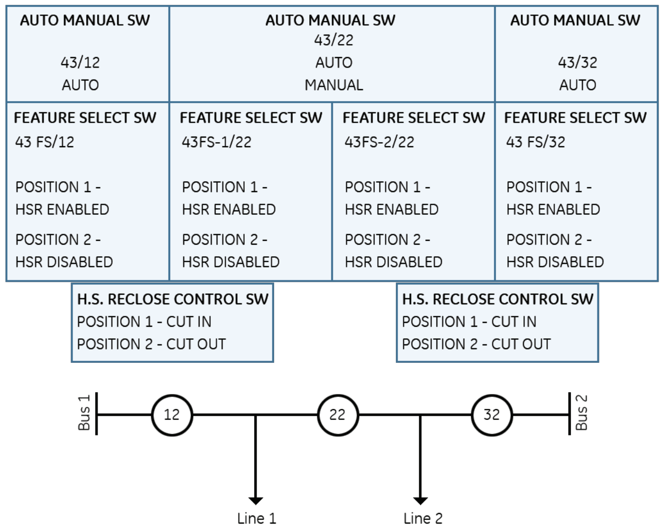


Figure 10.
Interlocking Example using IEC-61850

Transformer protection interlocking between the high and low side windings is another example where the devices on the high side winding maybe in a different control building than the low side winding devices. The buildings may, in some cases, be at considerable distances (hundreds of feet) away from one another. Application of the IEC 61850 makes the task of designing the interlocking simple. It is important to properly address allocation of network switches in multi-building stations where GOOSE messaging is communicated between buildings. For example, when protective devices for the high and low voltage windings of a power transformer are in two different buildings and IEC 61850 GOOSE messaging is used for interlocking functions between the two buildings. A simple solution is a fiber connection between the network switches in the two protection and control buildings. Other options include use of custom programmed network routers to pass V-LAN Multicast traffic if the two buildings for some reason (e.g: Cyber Asset allocations in each building) cannot be on the same network.

Another key advantage of the IEC 61850 application for transformer protection interlocking is minimizing use of DC circuits and running DC circuits between buildings when battery sources between the high and low side windings are not the same and protection DC sources cannot be mixed.

Other examples include breaker failure interlocking, breaker maintenance interlocking with bus differential and middle breaker in the respective bay, etc.

9.4 Design Considerations

In all of the above examples, it is recommended that the user applications have a "fail-safe" mode of operation. In each case, the use should consider factors such as:

- Loss of source (i.e.: DC circuit) to the devices that are communicating GOOSE messages?
- Need for redundancy in communication equipment
- Logic design and considerations – Example, upon DC source loss, scheme performance should not be any different than the conventional scheme.

9.5 Architecture Adaptability to IEC 61850 Process Bus and Merging Unit

The modularity of the MPAC provides for opportunities to enhance the architecture through the adoption of new technology. Similar to other aspects of MPAC, the adoption of process bus is evaluated to determine measurable and quantifiable overall benefits. Many of the benefits are covered in earlier sections in this paper. Areas for improvement in using the process bus include:

- Reduced engineering
- Simplification of electrical drawings – Some cabling diagrams will need to be incorporated into the new design concepts
- Minimization of copper wiring
- Turn around time of installation and commissioning
- Reduced maintenance cost
- Overall improvement in availability

The IEC 61850 Process Bus communication architecture and a "fit for purpose" physical architecture can be advantaged to achieve these goals.

The IEC 61850 Process Bus communication architecture provides a standard configuration for communication messages from a "Merging Unit (MU)" located in the field to a numerical relay located in the MPAC building. The MU can be locally connected to monitor CT, PT, Status Inputs, and Transducer Inputs. The MU can be connected to operate process equipment (breakers, switches, tap changers) in the field. From a physical architecture perspective, the use of fiber optic cabling between the MU and the relays in the MPAC building is the logical choice. A Relay-to-MU architecture further simplifies the installation from several perspectives:

- Cabling follows the existing wiring troughs
- Precise MU Synchronization can be achieved through the communication channel – eliminating the need for master clock synchronization
- Elimination of Ethernet switches in the path of this critical cyber asset
- Minimization of wiring connections and the associated engineering, drawings, installation, and testing
- Ease of implementation of redundant MUs

The Process Bus architecture allows connection of the MU to process equipment as early as the factory manufacturing stage. Implementation at this early stage allows for controlled, repeatable, and factory-tested installations. Connection of the MU to a relay in the control house requires the addition of a single fiber jumper between the MU data source and the relay input data card. A connection table now replaces wiring diagrams. For those measurements where field installation of the MU is required, the MU can be located anywhere in the yard and wiring is simplified to a point-to-point exercise.

The choice of modular relays in the MPAC building has made the adaptation to process bus straightforward. One Process Bus interface card in each of the MPAC devices (system "A" or "B" devices) replaces the respective analog, status input, the transducer and output control cards.

In terms of device set points and already established object models, all functions remain unchanged in the MPAC building. For example, the pushbutton operation, LED mapping, interlocking functions, and logic settings remain unchanged. The only additional settings are those that map the data from the MU into the appropriate locations in the relay (process bus interface card). Note that the functions defined in the IED Object Model remain the same – the only difference being that the data acquisition function in the MPAC devices is transferred to the MUs in the field.

9.6 Training Philosophy

With the new paradigm shift, training the employees has taken added importance, Figures 11-13. Training is a key component in a major initiative as every aspect of design, engineering, construction, maintenance and operation is affected.

While the basic control room appeared totally different, the operating principles remained the same as the older control rooms. Many of the functionalities from the conventional control room were incorporated into the multi-function devices thus, giving the new control rooms a different visual appeal. The challenge was how to train all the employees so they felt comfortable operating the new technology.

Figure 11.
MPAC Building in Route to Station

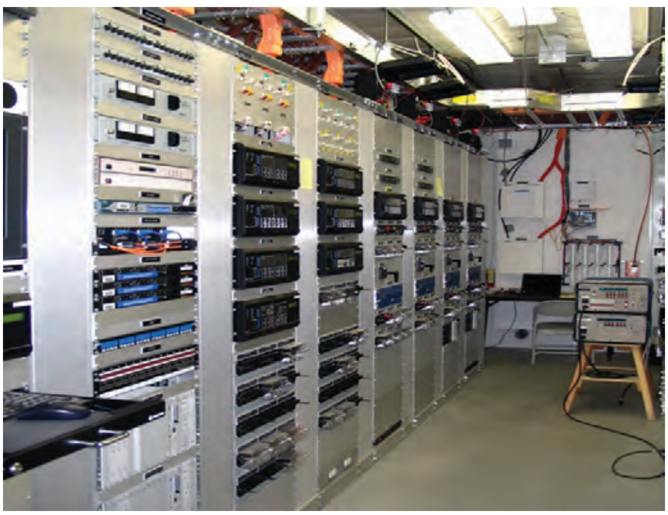


Figure 12.
MPAC Building with Integrated Protection and Control

Figure 13.
MPAC Building – Minimized Wiring

The initial series of trainings sessions were conducted on-site and consisted of hands-on training, just before the new buildings went into service. The training manual contained the description of operation, interaction with the HMI, Figure 14, and the multi-function devices [5].

9.7 Training Development and Technology Lab

The next step in the development of training involved a more systematic approach for a centralized training facility with formal classes and certified instructors that would provide training for different types and classifications such as engineers, technicians, and operating personnel. This facility would also be designed such that further technology advancements could be evaluated for systemwide roll out subject to successful testing. For example, the synchronized phasor functionality was recently implemented in the technology lab both for advance application studies and also for training and education of resources. The training and technology lab concept was studied and recommended to the management along with the justification for such a facility.

Figure 14.
Typical MPAC Building Showing the HMI

In parallel with the building of the simulator, a training matrix was developed in order to deliver specific training modules to specific groups based on the needs. Table 1, shows a simplified version of the training modules for different functions. The intent was to develop content such that each stand alone training module could be presented as an individual class or given to certain groups of employees that required the training. With the training modules in place, types of tools and course contents were developed. For example, the "troubleshooting logic" module required both hands on and classroom type material. It was also anticipated that as more MPAC buildings are constructed, the level of training for different groups or individuals may vary and therefore the training modules would need to be flexible to be enhanced as required.

One of the main differences and challenges with the use of multifunction devices has been the scheme design, functionalities, and interlocking embedded in the form of logic. Since the standards and associated logic developments have been with the core standards team, many aspects of training and troubleshooting have been considered and developed during the initial design phases. For training purposes, the logic related modules concentrated on the new style of prints, logic symbols, and how the logic interacted between the various discreet components. This was a significant change compared with the conventional standard drawings which normally contained device contacts and auxiliary devices. The new designs incorporated many of the functionalities of the inputs and outputs so the logic diagrams were required to show the logic flow and the relationship between the contacts and logic.

Another training module, the HMI module, was developed with input from operating personnel, electricians, and first responders. This module, as all the modules, contained situational problems that had actual problems to solve during the training session.

The training modules also include examples of conventional and the parallel functionalities based on the integrated schemes for the respective disciplines. These training modules, along with the other modules, provided the students with various hands-on scenarios, training text books, and job aids. The various modules would provide the company course flexibility when training the employees. The development of the training modules utilized a subject matter expert along with the training group. Standardized designs implemented in the field allowed the company to standardize on the training thus, capturing training costs and efficiencies.

10. Testing and Scheduled Maintenance

With the development of a partnership with the manufacturers, one of the cost savings involved testing the components within the buildings, including the multi-function devices. The core team worked with the respective manufactures of the multi-function devices and agreed to standard sets of tests based on the agreed set points. The set points were developed based on the function of the device. For example, a transformer device had a series of set points which are by function different than a line current differential device. While testing conventional protective relays was a normal procedure at PG&E, having the manufacturers of the respective devices test their various discreet components within the MPAC building was a new concept.

Previously, the company would receive a new protective relay from the manufacturer and spend the time to test every element within the relay, proving the manufacturer specifications. Today, the company's practice is to accept the manufacturer's testing specifications and then only perform a functional test once the microprocessor devices are installed in the scheme. One way to capture efficiencies with the MPAC building was to have the manufacturer perform some testing before shipping the building on-site. Standardized testing was part of the requirement to save costs and efficiencies.

10.1 Factory Acceptance Testing

The Factory Acceptance Testing has improved over a period of time to capture efficiencies. During construction of the initial MPAC buildings, representatives from PG&E participated in the Factory Acceptance Testing (FAT) to assist and witness testing. FAT is a series of step-by-step tests developed in advance and intended to verify wiring, interlocking, the logic and functionality at the time of building construction. The main purpose is to ensure the wiring is correct between the discrete components and that the devices operate as designed. A representative from the manufacturer would communicate any problems or needed enhancements with the company representative.

After the initial 3-4 projects, the PG&E core team did not attend the FAT. Only the PG&E local inspectors participate in the building inspection. The FAT results are submitted at the time of building delivery on site.

Module	Maintenance	Operations	Automation	Electrical Technicians	Engineering
Logic Diagrams				X	X
Building overview	X	X	X	X	
Building Systems	X	X			
Controls	X	X	X	X	
Safety	X	X	X	X	
Testing	X		X	X	
Data & Communications	X		X	X	X
HMI	X	X	X	X	X

Table 1.
Sample Training Matrix

10.2 Site Acceptance Testing

The FAT also led to another standardized test procedure for when the building was delivered and installed on site. Site Acceptance Test (SAT) are intended to prove the functionality of the schemes and the interaction among all the discrete components prior to release of the building to operations. This procedure proved all the relay logic without having the electrical technician follow the actual logic diagrams. The SAT is preformed by company technicians and start-up engineers.

The standardization of hardware, factory configuration of equipment, direct interface HMI server to the multi-function devices, and standardized test methods also reduce the SAT duration by nearly 60%.

10.3 Routine Maintenance and Troubleshooting

Another consideration in the MPAC development roadmap was the maintenance testing and troubleshooting. The SAT process is designed and developed based on this particular need when maintenance testing would be needed or required due to regulatory requirements for example. Troubleshooting tools and product training have been incorporated as part of the alliance and procurement. Also, the use of the new standard test procedures will also help the company capture labor costs and efficiencies.

The next step for the company in multi-function device testing is to move towards a more condition based maintenance system. Advances in technology, uses of a common database between departments, and the information collected from the various components within the new buildings allows this next step to take place. These future steps will further assist in improving maintenance effectiveness and efficiency.

11. Additional Considerations - System Security at Corporate Level

The initial plan included one general agreement and requirement. If the system could not be secure, the plan cannot move forward. It was paramount that the system could not be hacked or compromised or not be accessed by unauthorized personnel. The architecture, by virtue of the design approach, had many security levels and devices had multiple levels of alarms and password controls. However, there was still the remote possibility for someone knowledgeable to gain access into the system. The design team looked to the Corporate Computer Systems Department for direction, but few existing answers were available. Up to that point it was primarily security through obscurity. Even existing communications to the substations had security issues. A totally new approach had to be developed. The team focus shifted to the information technology and communications department for developing a physically separate LAN / WAN system for Substation Operations. This added to the complexity of the overall approach, but with Homeland Security issues on the forefront, greater support for the overall design was forthcoming. Both physical and electronic security would be required for future control buildings. Could we make the new control buildings more secure through card swipe locks and video monitoring? This also added to the specifications, communication capabilities and space requirements putting pressure on valuable real estate within the building. Finally a physically separate LAN / WAN architecture was developed and implemented meeting both corporate requirements and new emerging national requirements.

12. Cycle Time and Measured Savings

To date, there are nearly 35 MPAC buildings in service and cycle time and costs are continually measured and compared to the conventional approaches. Project cycle time and the cost of the few initial projects as anticipated were near the cost of conventional projects until the complete process leading to product levels were put in place and various functional groups and team members became familiar with developments and implementation process. The cost for the learning curve (including acceptance of the concept) is measured and for the most part seems evenly distributed across the various organizational teams.

The costs for developing the standards, setting guidelines, and templates, and engineering / maintenance tools, is a one time cost and can be distributed amongst the many projects. The overall project costs beyond the few initial projects has been steadily declining – The "targeted" vs. "budgeted" costs of the projects completed to date show a steady reduction in the 20% range. The contingency funding allows for addressing complexities. For example, if a station involves design and implementation of System Integrity Protection Scheme (SIPS) or Remedial Action scheme.

13. Conclusion

This paper is the roadmap of the success and lessons learned toward a systemwide revitalization of the assets and grid infrastructure for a major power company. The paper concludes with some measured savings based on installed systems. The initiative started with a clear vision of the future and putting a long term strategy in place. A set of trial migration sites were used as the initial steps followed by the formation of a core team and alliances with some protective relay and automation equipment suppliers. With the core team in place and the development of the object models, a "proof of concept" lab facility was established at the engineering headquarters to refine the objectives, develop the details for the architecture, troubleshoot the concepts, evaluate overall performance, and to identify the requirements and challenges. At the heart of the project was the commitment to develop a comprehensive set of standards, tools such as setting templates and logic drawings for various control features and associated interlocking with protection elements, comprehensive training program, establishment of asset maintenance process, and the description of operations for various components of modular building that led to the ground breaking concept for building a technology and state-of-the-art training facilities. The project success is credited to many hours of dedicated teamwork and commitments by the partners to develop the required features for implementation. The savings are approaching the original vision and the anticipated cost reductions when the concepts for MPAC were being developed. The vision has also laid the ground work for the future direction once all substations are digitized. The vision is now well accepted companywide and many companies from around the world have come for information exchange and site visits.

14. References

[1] V. Madani R. King, S. S. Venkata, W. Reder, The Challenges and Opportunities to Meet the Workforce Demand in the Electric Power and Energy Profession, IEEE PES, Munich, Germany: November, 2007

[2] S. S. Venkata, V. Madani, et al - The Education and Training of Future Protection Engineers: Challenges, Opportunities and Solutions, IEEE Power System Relaying Committee, May 2006

[3] M. Adamiak, V. Madani, et al. – "Wide Area Protection and Control, Today and Tomorrow", Proceedings of IEEE T&D, May 2006

[4] V. Madani , D. Novosel, P. Zhang, S. Meliopoulos, R. King, "Vision in Protection and Control Area Meeting the Challenges of 21st Century", IEEE PSCE, October 2006

[5] V. Madani, G. Duru, B. Tatera, M. Jones, B. Pace, A Paradigm Shift to Meet the Protection and Control Challenges of the 21st Century, Georgia tech Conference, Atlanta, May 2006

[6] V. Madani "IEC 61850 Applications and Challenges for Protection Engineers", Pre-conference Day -Western Protective Relay Conference, - October 2006

[7] V. Madani, D. Novosel, et al. "Taming the Power Grid", IEEE Spectrum Web. February 2005

[8] W. Peterson, D. Novosel, D. Hart, T.W. Cease, and J. Schneider, "Tapping IED Data to Find Transmission Faults," IEEE Computer Applications in Power, April 1999

[9] B. Tatera "Setting a Strategic Direction for Substation Automation at Pacific Gas & Electric Co - Western Power Delivery Automation Conference, Spokane, Washington April 2003

[10] P. Myrda, D. Tates, E. Udren, and D. Novosel: "Optimal Strategies for System-Wide Protection and Control Replacement Programs" CIGRE, Paris, August 2006

Implementing Smart Grid Communications

Managing Mountains of Data Opens Up New Challenges for Electric Utilities

James G. Cupp, PE, and Mike E. Beehler, PE
Burns & McDonnell

Electric utilities faced with the prospect of increasing customer rates are seeking solutions to challenges presented by rising global energy demand, aging infrastructure, increasing fuel costs and renewable portfolio standards in light of climate change. Many consider Smart Grid to be one such solution.

If we define the Smart Grid as "the convergence of information and operational technology applied to the electric grid, allowing sustainable options to customers and improved security, reliability and efficiency to utilities," then we must focus on deployment in ways that address rate and bill impacts. Here, we will outline the technical implementation of technologies that enable Smart Grid practices.

1. Communications for Data Transport

Electric utilities continue to be among the largest users of privately owned and operated wide-area networks (WANs) for communications. These networks include a hybrid mix of technologies including fiber optics, power line carrier systems, copper-wire line, and a variety of licensed and unlicensed wireless technologies. The utility WAN is designed to support applications vital to the safe and reliable operation of the electric utility mission-critical infrastructure: protective relaying for high voltage lines, SCADA/EMS, mobile fleet voice and data dispatch, generating plant automation, distribution feeder automation and physical security. Rather than relying on public communication carriers (AT&T, Sprint, Verizon, et al), utilities justify the costs of building and operating their own private WANs because of the highly critical nature of these applications for maintaining a reliable and secure power grid. Less-critical business applications such as corporate voice and data networks are also supported, but are not normally the driver for private WAN deployment.

A typical electric utility WAN consists of a high-bandwidth transport backbone network that backhauls large numbers of channels and applications from the utility service territory to the control center(s). Lower-bandwidth segments, or spurs, connect individual or small groups of facilities to the backbone. Fiber optics and/or digital microwave radio are usually the technologies of choice for backbone transport, whereas the spurs may combine these technologies with less robust alternatives such as copper twisted-pair wire lines, power line carrier, VHF and UHF radio links, and unlicensed wireless systems. Common carrier leased services are used only sparingly in most cases, for low-criticality applications in locations where privately owned alternatives are cost-prohibitive.

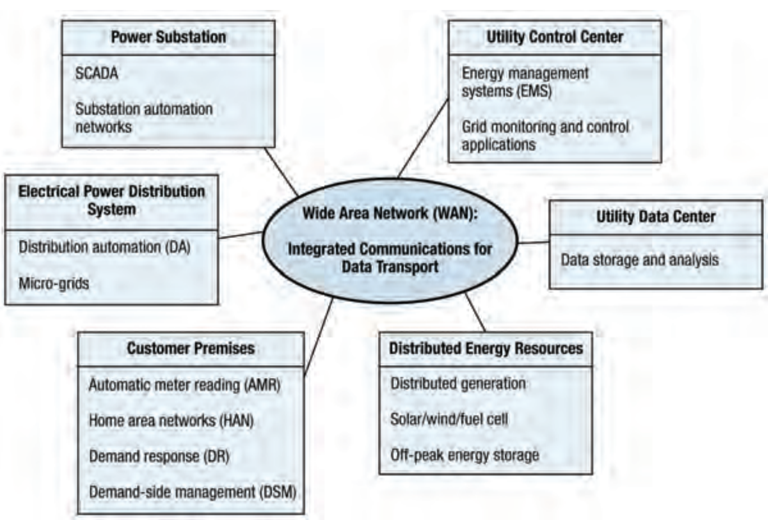


Figure 1.
A utility WAN under Smart Grid applications is required to handle more robust data transport.

These utility WANs have served traditional applications like SCADA/EMS, distribution automation (DA)/demand-side management (DSM) and automatic meter reading (AMR), now popularly encompassed as part of the Smart Grid (see Figure 1). The number of locations requiring communications service increases and the criticality of each location to the integrity of the overall grid decreases as these applications are pushed deeper into the distribution system (i.e., farther out from the primary substation and closer to the customer). Historically, this combination of increasing costs and decreasing benefits has been the primary obstacle to deployment of more feeder-level and customer-level applications such as DA/DSM and AMR/advanced meter infrastructure (AMI). When such applications were deployed, costs were controlled by limiting communications to one-way systems like broadcast radio signals or narrowband, highlatency systems such as power line carriers or dial-up phone lines.

What is needed is a nearly ubiquitous IP transport network operating at bandwidths robust enough to handle traditional utility power delivery applications along with vast amounts of new data from the Smart Grid.

2. Networks for the Future

Today, the political and regulatory impetus for wider deployment of Smart Grid applications, especially their deployment all the way to the customer premises, has resulted in pressure on utility engineers to solve the problem of establishing robust data transport WANs to the distribution feeder and customer level. The proliferation of information technology utilizing Internet protocol (IP) transport over Ethernet has made IP the de facto standard for data transport. What is needed is a nearly ubiquitous IP transport network operating at bandwidths robust enough to handle traditional utility power delivery applications along with vast amounts of new data from the Smart Grid. These networks need to be scalable enough to handle future applications as they come.

Communications for Smart Grid data transport require that utilities address both the backbone and the spur segments. Most electric utility communications backbones today are based largely on traditional time-division multiplexing (TDM) digital architectures. TDM technology, while highly reliable, was originally developed for the transport of point-to-point constant-bit-rate voice communications and is not necessarily suited to cost-effective transport of point-to-multipoint "bursty" data traffic required in an IP environment. The Smart Grid will require that these backbones be upgraded to backhaul Ethernet/IP data traffic at speeds ranging from one to 10 gigabits per second in a highly reliable manner. Rather than replacing their legacy TDM networks, many utilities will opt initially to overlay these existing networks by overbuilding gigabit Ethernets on unused fiber, and licensed or unlicensed broadband wireless networks over existing microwave paths.

3. Last-Mile Challenges

The deployment of spur or last-mile communications for the Smart Grid, typically from a backbone node to the customer premises, offers additional challenges: First, the network must cover a large area, especially if coverage of residential customers is to be provided. This has prompted some utilities to take a phased approach, deploying the Smart Grid to large-load industrial and commercial customers initially, since the bulk of the benefits of Smart Grid follow the bulk of the electrical load, while residential applications may remain on the back burner, waiting for a clearer quantification of benefits. This balanced approach may make sense economically but may have broad ramifications politically as rates rise and residential customers (voters) demand relief.

Second, the proper balancing of performance and cost is less clear for these last-mile applications. Losing communications with a small percentage of the DA or AMI for a time, while undesirable, would pose no real threat to the safe and reliable operation of the overall power grid. Communications with a single customer or residence do not require the bandwidth and performance needed in the backbone, so low-speed communication devices with marginal signal strength that may require multiple retransmissions to complete a message can be tolerated. These issues raise questions like, "How reliable is reliable enough?" "How fast is fast enough?" and "At what cost?"

The relaxed performance and reliability constraints in the last mile also mean that the number of technology options available for this portion of the WAN are more plentiful. Technologies like meshed Wi-Fi, packet-based store and forward radio networks, and broadband-over-power line (BPL), not considered reliable or robust enough for the mission-critical infrastructure backbone, are viable options for the last mile. Likewise, public carrier and CATV-based services like broadband cable modem, digital subscriber line (DSL) and cellular-based wireless data networks may also make sense where utilities can negotiate bulk service rates.

4. Data Integration and Management

Once the DA or AMI data is efficiently transported, a completely new set of data integration and management issues will challenge utilities technically and culturally. The Smart Grid will generate billions of data points from thousands of system devices and hundreds of thousands of customers. Data must be converted to information through a knowledge-management life cycle in which the data from meters and appliances or substations and distribution systems are analyzed and integrated in a manner that leads to action. A data-to-information-to-action plan will develop as a better understanding of load factors, energy usage patterns, equipment condition, voltage levels, etc. emerges through analysis and is integrated as functional information into usable customer programs and/or operation and maintenance algorithms that identify, trend and alert operators to incipient failure.

The first phase of the knowledge management effort and a key component in the system of information ecology is data conservation in a data warehouse. Data storage needs will explode. Data security will be important, but some of the best system or customer programs may result by allowing engineers and operators the opportunity to freely analyze some or all of the data. IBM, Oracle and Microsoft recognize the huge growth potential and are visibly promoting their solution concepts.

The Smart Grid is expected to be fully functional by 2030. Data collected, analyzed, visualized and warehoused from the Smart Grid will contribute to many new ideas and inventions that can improve lives.

Dennis M. Klinger, vice president of information management services for Florida Power & Light, calls this "moving at the speed of value." In an era of serial rate increases, customers will demand value, and utilities must deliver that value. This will be the future of electricity.

5. Customer Programs

The future of electricity begins with the customer. Integration and management of system and customer data can lead to the ability to analyze warehoused information in a manner that improves operational efficiency and reliability, but most importantly, provides sustainable options for customers. Sustainable options will include demand response and demand-side management programs for all customer classes that include a home area network (HAN) plan for residential customers, allowing prices to devices supported by ultra-simple rate plans. Data will become information used for action.

6. Scheduling Savings

The HAN is a computer automation system for the home (or small commercial business) that integrates devices through the Internet and with the electric utility to allow the user to be proactive in the use or generation of energy. The HAN will play a major role in making the grid more efficient and in moderating rate impact for the customer. The HAN begins on the customer side of the meter and will be made up of plug-in hybrid electric vehicles, renewable and/or distributed generation, HVAC systems, pool pumps, intelligent appliances and consumer devices like MP3 players, cell phones and iPods authenticated to the electric utility on a secure network owned by the owner. The owner will have the ability to control the operation of devices on the HAN from a computer to maximize the advantages for demand response (DR) or DSM rate structures offered by the electric utility.

7. Improving Load Factors

DR is a voluntary rate structure that typically lowers a customer's general rate per kilowatthour in return for the utility's option to curtail power as needed during system peak loading events. DSM is the effort to incentivize customer use through simple time-of-use rates that generally correspond to the cost of producing electricity. DR and DSM shift electric load and improve the electric utility's load factor and should not be confused with energy efficiency programs that reduce load and, therefore, sales. The current regulatory construct allows utilities a reasonable rate of return, or profits, on prudent investments and the cost to operate and maintain those investments. Some utilities seek to decouple their sales from profits since energy-efficiency programs lower sales as less electricity is consumed. Decoupled sales and profits theoretically make the electric utility indifferent to energy efficiency programs and distributed generation but remain a controversial issue in the industry. Cyber security, ownership of customer data, standardization of device protocols for low-power personal networks, customer acceptance of DR and DSM programs and other issues are also sources of controversy in HAN build-out.

> Allowing customers to make sustainable decisions on the use of electricity and, ultimately, satisfying regulators will provide for full rate recovery and return on investment.

8. Where Next?

Regulators and lawmakers are not passively waiting for utilities to offer solutions to the serial rate increases that are coming. Regulatory action is being taken and the desired result is clear. The Smart Grid must provide sustainable options to customers. Allowing customers to make sustainable decisions on the use of electricity and, ultimately, satisfy regulators will provide for full rate recovery and return on investment. That done, utilities can move at the speed of value to confidently use the Smart Grid to achieve other security, reliability and efficiency objectives. These other objectives may include more efficient meter reads and billing, better customer service, theft/tamper detection, turn-on/turn-off service, advanced pay services, load forecasting, asset management, transformer sizing, power quality improvements, and a myriad of other efficiencies and services that will be developed in the years to come, when today's electric grid becomes the Smart Grid.

➲ *Originally published in TECH Briefs, 2008, No. 4*

070209-v2

HardFiber™ System

IEC 61850

Process Bus Solution

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.

Faster Installation...

Better Reliability...

Lower Costs...

HardFiber™ Brick

Hardened Switchyard Interface

Universal Relay Family

IEC 61850 Compliant P&C Family

Digital Energy
Multilin

GE Multilin
www.GEMultilin.com/HardFiber
gemultilin@ge.com

Worldwide
Tel: 905-294-6222

North America
Tel: 1-800-547-8629

Europe/MiddleEast/Africa
Tel: +34 94 485 88 00

IEC 61850 Communication Networks and Systems In Substations:

An Overview for Users

Mark Adamiak , Drew Baigent
GE Digital Energy

Ralph Mackiewicz
SISCO

1. Abstract

Over the last decade, the "digitization" of the electron enterprise has grown at exponential rates. Utility, industrial, commercial, and even residential consumers are transforming all aspects of their lives into the digital domain. Moving forward, it is expected that every piece of equipment, every receptacle, every switch, and even every light bulb will possess some type of setting, monitoring and/or control. In order to be able to manage the large number of devices and to enable the various devices to communicate with one another, a new communication model was needed. That model has been developed and standardized as IEC 61850 – Communication Networks and Systems in Substations [1]. This paper looks at the needs of next generation communication systems and provides an overview of the IEC 61850 protocol and how it meets these needs.

2. Communication System Needs

Communication has always played a critical role in the real-time operation of the power system. In the beginning, the telephone was used to communicate line loadings back to the control center as well as to dispatch operators to perform switching operations at substations. Telephone-switching based remote control units were available as early as the 1930's and were able to provide status and control for a few points. As digital communications became a viable option in the 1960's, data acquisition systems (DAS) were installed to automatically collect measurement data from the substations. Since bandwidth was limited, DAS communication protocols were optimized to operate over low-bandwidth communication channels. The "cost" of this optimization was the time it took to configure, map, and document the location of the various data bits received by the protocol.

As we move into the digital age, literally thousands of analog and digital data points are available in a single Intelligent Electronic Device (IED) and communication bandwidth is no longer a limiting factor. Substation to master communication data paths operating at 64,000 bits per second are becoming common-place with an obvious migration path to much high rates. With this migration in technology, the "cost" component of a data acquisition system has now become the configuration and documentation component. Consequently, a key component of a communication system is the ability to describe themselves from both a data and services (communication functions that an IED performs) perspective. Other "key" requirements include:

- High-speed IED to IED communication
- Networkable throughout the utility enterprise
- High-availability
- Guaranteed delivery times
- Standards based
- Multi-vendor interoperability
- Support for Voltage and Current samples data
- Support for File Transfer
- Auto-configurable / configuration support
- Support for security

Given these requirements, work on a "next generation" communication architecture began with the development of the Utility Communication Architecture (UCA) in 1988. The result of this work was a profile of "recommended" protocols for the various layers of the International Standards Organization (ISO) Open System Interconnect (OSI) communication system model. This architecture resulted in the definition of a "profile" of protocols, data models, and abstract service definitions that became known as UCA. The concepts and fundamental work done in UCA became the foundation for the work done in the IEC TC57 Working Groups 10, 11, and 12 which resulted in the International Standard – IEC 61850 – Communication Networks and Systems in Substations [1].

3. Scope and Outline of IEC 61850

The stated scope of IEC 61850 was communications within the substation. The document defines the various aspects of the substation communication network in 10 major sections as shown in Table 1 below.

Part #	Title
1	Introduction and Overview
2	Glossary of terms
3	General Requirements
4	System and Project Management
5	Communication Requirements for Functions and Device Models
6	Configuration Description Language for Communication in Electrical Substations Related to IEDs
7	Basic Communication Structure for Substation and Feeder Equipment
7.1	- Principles and Models
7.2	- Abstract Communication Service Interface (ACSI)
7.3	- Common Data Classes (CDC)
7.4	- Compatible logical node classes and data classes
8	Specific Communication Service Mapping (SCSM)
8.1	- Mappings to MMS (ISO/IEC 9506 – Part 1 and Part 2) and to ISO/IEC 8802-3
9	Specific Communication Service Mapping (SCSM)
9.1	- Sampled Values over Serial Unidirectional Multidrop Point-to-Point Link
9.2	- Sampled Values over ISO/IEC 8802-3
10	Conformance Testing

Table 1.

Parts 3, 4, and 5 of the standard start by identifying the general and specific functional requirements for communications in a substation (key requirements stated above). These requirements are then used as forcing functions to aid in the identification of the services and data models needed, application protocol required, and the underlying transport, network, data link, and physical layers that will meet the overall requirements.

The major architectural construct that 61850 adopts is that of "abstracting" the definition of the data items and the services, that is, creating data items/objects and services that are independent of any underlying protocols. The abstract definitions then allow "mapping" of the data objects and services to any other protocol that can meet the data and service requirements. The definition of the abstract services is found in part 7.2 of the standard and the abstraction of the data objects (referred to as Logical Nodes) is found in part 7.4. In as much as many of the data objects are made up of common pieces (such as Status, Control, Measurement, Substitution), the concept of "Common Data Classes" or "CDC" was developed which defined common building blocks for creating the larger data objects. The CDC elements are defined in part 7.3.

Given the data and services abstract definitions, the final step was one of "mapping" the abstract services into an actual protocol. Section 8.1 defines the mapping of the abstract data object and services onto the Manufacturing Messaging Specification – MMS2 and sections 9.1 and 9.2 define the mapping of the Sample Measured Values (unidirectional point-to-point and bi-directional multipoint accordingly) onto an Ethernet data frame. The 9.2 document defines what has become known as the Process Bus.

From a system perspective, there is a significant amount of configuration that is required in order to put all the pieces together and have them work. In order to facilitate this process and to eliminate much of the human error component, an XML based Substation Configuration Language (SCL) was defined in part 6. It allows the formal description of the relations between the substation automation system and the substation (switchyard). At the application level, the switchyard topology itself and the relation of the switchyard structure to the SAS functions (logical nodes) configured on the IEDs can be described. Each device must provide an SCL file that describes the configuration of itself.

Although the scope of IEC 61850 was originally focused "inside" the substation, discussions are underway to look at defining IEC 61850 for the Substation to Master communication protocol (already in service in several installations). In addition, applications are in service that uses various components of IEC 61850 for wide area substation-to-substation communication.

Finally, part 10 of the document defines a testing methodology in order to determine "conformance" with the numerous protocol definitions and constraints defined in the document.

The rest of this paper goes into some focused details of the various parts of the IEC 61850 standard.

4. Modeling Approach

Legacy protocols have typically defined how bytes are transmitted on the wire. However, they did not specify how data should be organized in devices in terms of the application. This approach requires power system engineers to manually configure objects and map them to power system variables and low-level register numbers, index numbers, I/O modules, etc. IEC 61850 is unique. In addition to the specification of the protocol elements (how bytes are transmitted on the wire), IEC 61850 provides a comprehensive model for how power system devices should organize data in a manner that is consistent across all types and brands of devices. This eliminates much of the tedious non-power system configuration effort because the devices can configure themselves. For instance, if you put a CT/VT input into an IEC 61850 relay, the relay can detect this module and automatically assign it to a measurement unit without user interaction. Some devices use an SCL file to configure the objects and the engineer need only import the SCL file into the device to configure it. Then, the IEC 61850 client application can extract the object definitions from the device over the network. The result is a very large savings in the cost and effort to configure an IEC 61850 device.

The IEC 61850 device model begins with a physical device. A physical device is the device that connects to the network. The physical device is typically defined by its network address. Within each physical device, there may be one or more logical devices. The IEC 61850 logical device model allows a single physical device to act as a proxy or gateway for multiple devices thus providing a standard representation of a data concentrator.

Each logical device contains one or more logical nodes. A logical node (see Figure 1) is a named grouping of data and associated services that is logically related to some power system function.

XCBR Class				
DATA NAME	COMMON DATA CLASS	DESCRIPTION	T	MANDATORY/ OPTIONAL
LNName	Secure	Shall be inherited from Logical-Node Class (see IEC 61850-7-2)		
DATA				
Common Logical Node Information				
		LN shell inherit all Mandatory Data from Common Logical Node Class		Mandatory
Loc	SPS	Local operation (local means without substation automation communication, hardwired direct control)		Mandatory
EE Health	INS	External equipment health		Optional
EE Name	DPL	External equipment name plate		Optional
OpCnt	INS	Operation counter		Mandatory
Controls				
Pos	DPC	Switch position		Mandatory
BlkOpn	SPC	Block opening		Mandatory
BlkCls	SPC	Block closing		Mandatory
ChaMotEna	SPC	Charger motor enabled		Optional
Metered Values				
SumSwARs	BCR	Sum o Switched Amperes, resetable		Optional
Status Information				
CBOpCap	INS	Circuit breaker operating capability		Mandatory
POWCap	INS	Point on Wave switching capability		Optional
MaxOpCap	INS	Circuit breaker operating capability when fully charged		Optional

Figure 1.
Anatomy of Circuit Breaker (XCBR) Logical Node in IEC 61850-7-4

There are logical nodes for automatic control the names of which all begin with the letter "A". There are logical nodes for metering and measurement the names of which all begin with the letter "M". Likewise there are logical nodes for Supervisory Control (C), Generic Functions (G), Interfacing/Archiving (I), System logical nodes (L), Protection (P), Protection Related (R), Sensors (S), Instrument Transformers (T), Switchgear (X), Power Transformers (Y), and Other Equipment (Z). Each logical node has an LN-Instance-ID as a suffix to the logical node name. For instance, suppose there were two measurement inputs in a device to measure two 3-phase feeders. The standard name of the logical node for a Measurement Unit for 3-phase power is MMXU. To delineate between the measurements for these 2 feeders the IEC 61850 logical node names of MMXU1 and MMXU2 would be used. Each logical node may also use an optional application specific LN-prefix to provide further identification of the purpose of a logical node.

Each logical node contains one or more elements of Data. Each element of data has a unique name. These Data Names are determined by the standard and are functionally related to the power system purpose. For instance, a circuit breaker is modeled as an XCBR logical node. It contains a variety of Data including Loc for determining if operation is remote or local, OpCnt for an operations count, Pos for the position, BlkOpn block breaker open commands, BlkCls block breaker close commands, and CBOpCap for the circuit breaker operating capability.

Each element of data within the logical node conforms to the specification of a common data class (CDC) per IEC 61850-7-3. Each CDC describes the type and structure of the data within the logical node. For instance, there are CDCs for status information, measured information, controllable status information, controllable analog set point information, status settings, and analog settings. Each CDC has a defined name and a set of CDC attributes each with a defined name, defined type, and specific purpose. Each individual attribute of a CDC belongs to a set of functional constraints (FC) that groups the attributes into categories. For instance, in the Single Point Status (SPS) CDC described in Figure 2, there are functional constraints for status (ST) attributes, substituted value (SV) attributes, description (DC) attributes, and extended definition (EX) attributes. In this example the status attributes of the SPS class consists of a status value (stVal), a quality flag (q), and a time stamp (t).

SPS Class					
ATTRIBUTE NAME	ATTRIBUTE TYPE	FUNCTIONAL CONSTRAINT	TRGOP	VALUE / VALUE RANGE	MANDATORY/ OPTIONAL
DataName	Inherited from Data Class (see IEC 61850-7-2)				
DATA ATTRIBUTE					
Status					
stVal	BOOLEN	ST	dchg	TRUE|FALSE	Mandatory
q	Quality	ST	qchg		Mandatory
t	TimeStamp	ST			Mandatory
Substitution					
subEna	BOOLEN	SV			PICS_SUBST
subVal	BOOLEN	SV		TRUE|FALSE	PICS_SUBST
subQ	Quality	SV			PICS_SUBST
subID	VISIBLE STRING64	SV			PICS_SUBST
Configuration, description and extension					
d	VISIBLE STRING255	DC		Text	Optional
dU	UNICODE STRING255	DC			Optional
cdcNs	VISIBLE STRING255	EX			AC_DLNDA_M
cdcName	VISIBLE STRING255	EX			AC_DLNDA_M
dataNs	VISIBLE STRING255	EX			AC_DLN_M

Figure 2.
Anatomy of the Single Point Status (SPS) Common Data Class in IEC 61850-7-3

The IEC 61850 model of a device is a virtualized model that begins with an abstract view of the device and its objects and is defined in IEC 61850 part 7. Then, this abstract model is mapped to a specific protocol stack in section IEC 61850-8-1 based on MMS (ISO9506), TCP/IP, and Ethernet. In the process of mapping the IEC 61850 objects to MMS, IEC 61850-8-1 specifies a method of transforming the model information into a named MMS variable object that results in a unique and unambiguous reference for each element of data in the model. For instance, suppose that you have a logical device named "Relay1" consisting of a single circuit breaker logical node XCBR1 for which you want to determine if the breaker is in the remote or local mode of operation. To determine this you would read the object shown in Figure 3.

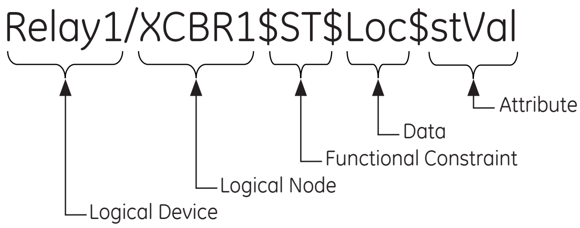


Figure 3.
Anatomy of an IEC 61850-8-1 Object Name

5. Mapping to Real Protocols

The abstract data and object models of IEC 61850 define a standardized method of describing power system devices that enables all IEDs to present data using identical structures that are directly related to their power system function. The Abstract Communication Service Interface (ACSI) models of IEC 61850 define a set of services and the responses to those services that enables all IEDs to behave in an identical manner from the network behavior perspective. While the abstract model is critical to achieving this level of interoperability, these models need to be operated over a real set of protocols that are practical to implement and that can operate within the computing environments commonly found in the power industry. IEC 61850-8-1 maps the abstract objects and services to the Manufacturing Message Specification (MMS) protocols of ISO9506. Why was a protocol originally designed for manufacturing used? Because MMS is the only public (ISO standard) protocol that has a proven implementation track record that can easily support the complex naming and service models of IEC 61850. While you can theoretically map IEC 61850 to any protocol, this mapping can get very complex and cumbersome when trying to map IEC 61850 objects and services to a protocol that only provides read/write/report services for simple variables that are accessed by register numbers or index numbers. This was the reason that MMS was chosen for UCA in 1991 and is the reason that it was kept for IEC 61850. MMS is a very good choice because it supports complex named objects and a rich set of flexible services that supports the mapping to IEC 61850 in a straightforward manner.

The mapping of IEC 61850 object and service models to MMS is based on a service mapping where a specific MMS service/services are chosen as the means to implement the various services of ACSI. For instance, the control model of ACSI is mapped to MMS read and write services. Then the various object models of IEC 61850 are mapped to specific MMS objects. For instance, the IEC 61850 logical device object is mapped to an MMS domain. Table 2 summarizes the mapping of IEC 61850 objects and Table 3 the ACSI mapping to MMS.

In addition to the mapping to the application layer, Part 8.1 defines profiles for the "other" layers of the communication stack that are dependent on the service provided (as shown in Figure 4). Of note on the various profiles: the Sampled Values and GOOSE applications map directly into the Ethernet data frame thereby eliminating processing of any middle layers; the MMS Connection

IEC61850 Objects	MMS Object
SERVER class	Virtual Manufacturing Device (VMD)
LOGICAL DEVICE class	Domain
LOGICAL NODE class	Named Variable
DATA class	Named Variable
DATA-SET class	Named Variable List
SETTING-GROUP-CONTROL-BLOCK class	Named Variable
REPORT-CONTROL-BLOCK class	Named Variable
LOG class	Journal
LOG-CONTROL-BLOCK class	Named Variable
GOOSE-CONTROL-BLOCK class	Named Variable
GSSE-CONTROL-BLOCK class	Named Variable
CONTROL class	Named Variable
Files	Files

Table 2.
IEC 61850 to MMS object mapping

IEC 61850 Services	MMS Services
LogicalDeviceDirectory	GetNameList
GetAllDataValues	Read
GetDataValues	Read
SetDataValues	Write
GetDataDirectory	GetNameList
GetDataDefinition	GetVariableAccessAttributes
GetDataSetValues	Read
SetDataSetValues	Write
CreateDataSet	CreateNamedVariableList
DeleteDataSet	DeleteNamedVariableList
GetDataSetDirectory	GetNameList
Report (Buffered and Unbuffered)	InformationReport
GetBRCBValues/GetURCBValues	Read
SetBRCBValues/SetURCBValues	Write
GetLCBValues	Read
SetLCBValues	Write
QueryLogByTime	ReadJournal
QueryLogAfter	ReadJournal
GetLogStatusValues	GetJournalStatus
Select	Read/Write
SelectWithValue	Read/Write
Cancel	Write
Operate	Write
Command-Termination	Write
TimeActivated-Operate	Write
GetFile	FileOpen/FileRead/FileClose
SetFile	ObtainFile
DeleteFile	FileDelete
GetFileAttributeValues	FileDirectory

Table 3.
IEC 61850 services mapping (partial)

Oriented layer can operate over TCP/IP or ISO; the Generic Substation Status Event (GSSE) is the identical implementation as the UCA GOOSE and operates over connectionless ISO services; all data maps onto an Ethernet data frame using either the data type "Ethertype" in the case of Sampled Values, GOOSE, TimeSync, and TCP/IP or "802.3" data type for the ISO and GSSE messages.

6. Process Bus

As technology migrates to "next generation" low-energy voltage and current sensors, the ability to digitize the base quantities at the source and transmit the resulting sample values back to the substation becomes a need. In addition to Sampled Values, the ability to remotely acquire status information as well as set output controls is very desirable. IEC 61850 addresses this need through the definition of Sampled Measured Values services and the implementation of a Process Bus. The Process layer of the substation is related to gathering information, such as Voltage, Current, and status information, from the transformers and transducers connected to the primary power system process – the transmission of electricity. IEC 61850 defines the collection of this data via two different protocol definitions, namely, Part 9.1 which defines a Unidirectional Multidrop Point-to-Point fixed link carrying a fixed dataset and Part 9.2 which defines a "configurable" dataset that can be transmitted on a multi-cast basis from one publisher to multiple subscribers.

Figure 5, above, shows the basic concept of the Process Bus. Signals from voltage and current sources (low or high energy) as well as status information are input into a "Merging Unit" (MU).

The Merging Units in a station sample the signals at an agreed, synchronized rate. In this manner, any IED can input data from multiple MUs and automatically align and process the data. At this time, there is an implementation agreement that defines a base sample rate of 80 samples per power system cycle for basic protection and monitoring and a "high" rate of 256 samples per power system cycle for high-frequency applications such as power quality and high-resolution oscillography.

Part 9.1 specifies a pre-configured or "universal" dataset as defined in IEC 60044-8. This dataset includes 3-phase voltage, bus voltage, neutral voltage, 3-phase currents for protection, 3-phase currents for measurement and two 16-bit status words. Note that the analog data values are mapped into 16-bit registers in this mapping.

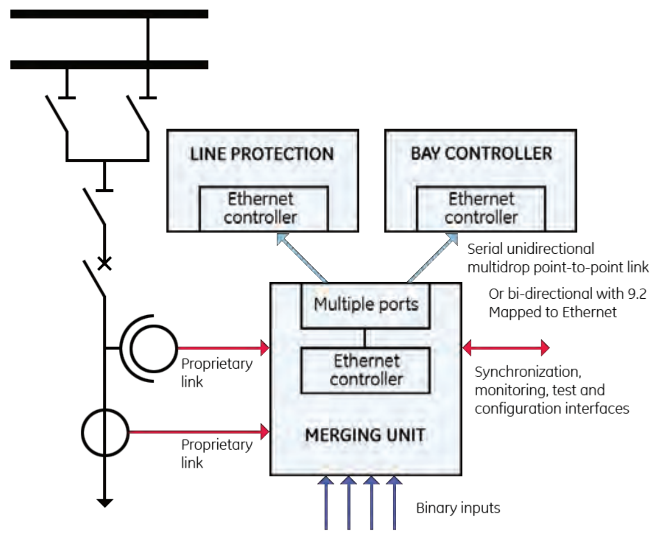


Figure 5.
Sample Measured Value Concept

Part 9.2 is a more generalized implementation of Sampled Measured Values (SMV) data transfer. In 9.2, the dataset or "payload" is user-defined using the SCL. As a dataset, data values of various sizes and types can be integrated together. Note that the existing implementation agreement proposed a data value size of 32 bits with a scale factor of 1 count = 1ma.

Both 9.1 and 9.2 specify mapping directly onto an Ethernet transport (see Figure 4). Depending on the sample data rate, anywhere from 1 to 5 devices can be mapped onto a single 100MB Ethernet link. Multiple 100MB Ethernet data streams can then be

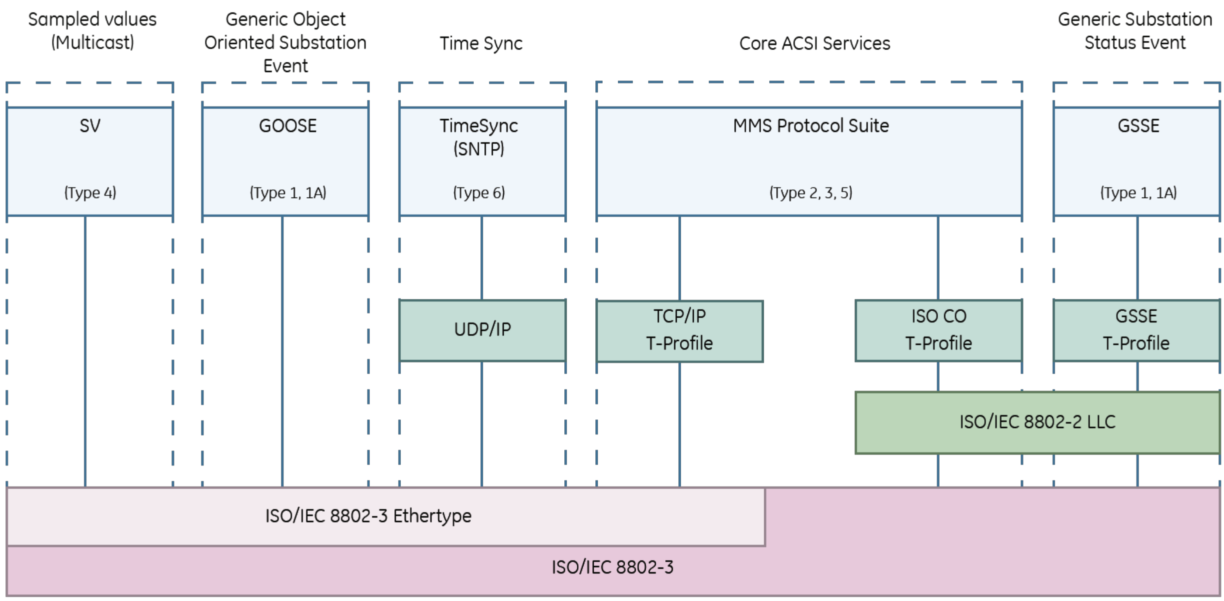


Figure 4.
Overview of IEC 61850 Functionality and Associated Communication Profiles

combined into a single Ethernet switch with a 1GB backbone. In this configuration, 50 or more datasets can be published to multiple subscribers.

7. Substation Configuration Language

IEC 61850-6-1 specifies a Substation Configuration Language (SCL) that is based on the eXtensible Markup Language (XML) to describe the configuration of IEC 61850 based systems. SCL specifies a hierarchy of configuration files that enable multiple levels of the system to be described in unambiguous and standardized XML files. The various SCL files include system specification description (SSD), IED capability description (ICD), substation configuration description (SCD), and configured IED description (CID) files. All these files are constructed in the same methods and format but have different scopes depending on the need.

Even though an IEC 61850 client can extract an IED's configuration from the IED when it is connected to that IED over a network, there are several scenarios where the availability of a formal off-line description language can bring very large benefits to users outside of configuring IEC 61850 client applications. These benefits include:

- SCL enables off-line system development tools to generate the files needed for IED configuration automatically from the power system design significantly reducing the cost and effort of IED configuration by eliminating most, if not all, manual configuration tasks.
- SCL enables the sharing of IED configuration among users and suppliers to reduce or eliminate inconsistencies and misunderstandings in system configuration and system requirements. Users can provide their own SCL files to ensure that IEDs are delivered to them properly configured.
- SCL allows IEC 61850 applications to be configured off-line without requiring a network connection to the IED for client configuration.

SCL can be used as best fits each user's requirements. A user can decide to use CID files to provide help in IED configuration using its existing system design processes. Or SCL can be used to restructure the entire power system design process to eliminate manual configuration, eliminate manual data entry errors, reduce misunderstanding between system capabilities and requirements, enhance the interoperability of the end system, and greatly increase the productivity and effectiveness of power system engineers.

8. IEC Substation Model

Putting the pieces together results in the substation architecture shown in Figure 6.

At the "process" layer, data from Optical/Electronic Voltage and Current sensors as well as status information will be collected and digitized by the Merging Units (MUs). MUs could be physically located either in the field or in the control house. Data from the MUs will be collected through redundant 100MB fiber optic Ethernet connections. The collection points will be redundant Ethernet switches with 1GB internal data buses and 1GB uplinks that support Ethernet priority and Ethernet Virtual LAN (VLAN). VLAN allows the Ethernet switch to deliver datasets to only those switch ports/IEDs that have subscribed to the data. In migrating to Process Bus implementations, manufacturers will need to provide the ability to integrate data from existing CTs and PTs with the data from the newer Optical/Electronic sensors. A redundant synchronization clock architecture will also have to be addressed. In this architecture, upon detection of failure of Clock 1, Clock 2 will have to automatically come on line and continue providing sampling synchronization.

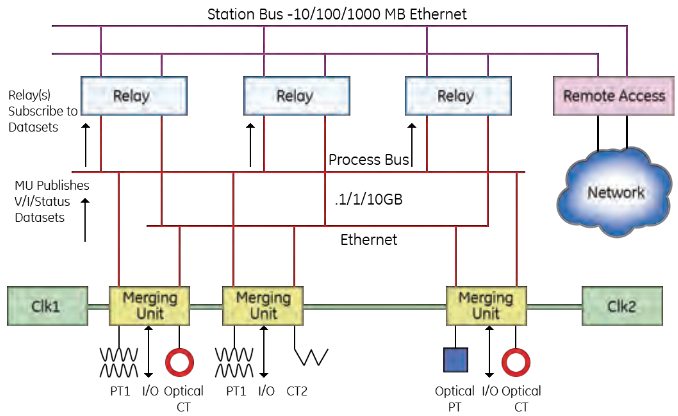


Figure 6.
IEC 61850 Substation Model

At the substation level, a Station Bus will exist. Again, this bus will be based today on 10MB Ethernet with a clear migration path to 100MB Ethernet. The Station Bus will provide primary communications between the various Logical Nodes, which provide the various station protection, control, monitoring, and logging functions. Communications will operate on either a connection oriented basis (e.g. – request of information, configuration, etc.) or a connection-less basis (IEC Generic Object Oriented Substation Event - GOOSE). Again, a redundant communication architecture is recommended as application of IED to IED data transmission puts the communication system on the critical path in case of a failure.

Finally, this architecture supports remote network access for all types of data reads and writes. As all communication is network enabled, multiple remote "clients" will desire access the wide variety of available information. Typical clients would include local HMI, operations, maintenance, engineering, and planning. The remote access point is one logical location to implement security functions such as encryption and authentication. This implementation un-burdens the individual IEDs from performing encryption on internal data transfers but still provide security on all external transactions.

9. Application Software

A variety of commercial products supporting IEC 61850 are already available and the future holds promise for many new innovations that will greatly benefit users. Of particular significance are products that support both the IEC 61850 communications standard and the OLE for Process Control (OPC see http://www.opcfoundation.org) application program interface (API) standard of the OPC Foundation. The combination of a standardized protocol and a standardized API is a powerful tool that allows users to dramatically lower their costs to build substation automation systems by enabling products from different vendors to plug together into a complete solution.

The OPC Data Access (DA) specification is an API that enables an OPC Client application, such as a SCADA or Human Machine Interface (HMI) application, to provide a generic interface to outside data that is independent of any specific protocol (Figure 7). This enables third parties to develop OPC Servers to interface with a wide variety of protocols, including IEC 61850, Modbus, DNP3, and hundreds of other protocols. There is a wide availability of both client and server applications that provide users choice and flexibility. For instance, interfaces to many different applications like relational data base management systems (RDBMS), spreadsheets, data historians, trending systems, etc. are available that support OPC and provide a large choice of options to implement complex systems at a low cost (see Figure 8).

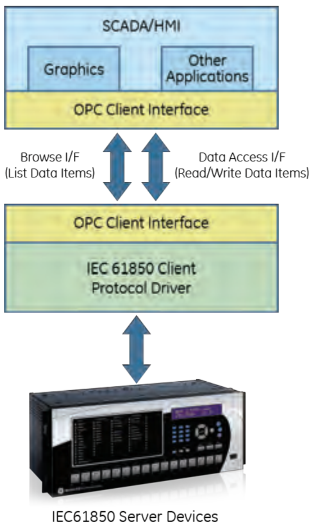


Figure 7.
Using IEC 61850 with OPC

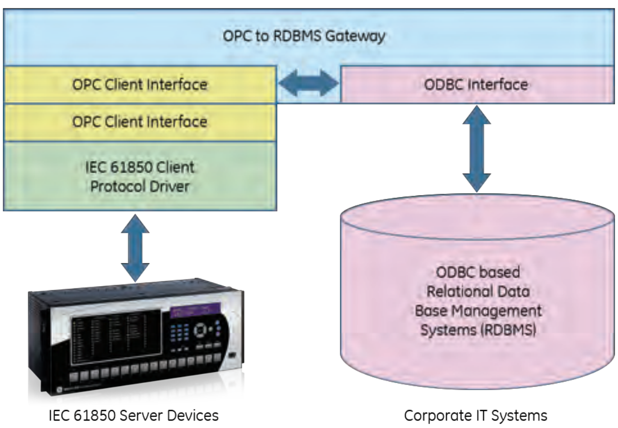


Figure 8.
OPC Enables IEC 61850 Interface to IT

In addition to providing access to data in IEDs, OPC interfaces support an important feature called browsing. The OPC browse interface enables the client to retrieve the list of data items defined in a server instead of having to be pre-configured. This works especially well with IEC 61850 devices because of built-in support for object discovery. By combining OPC with IEC 61850 the substation engineer avoids many hours of configuration and is able to install and commission systems quicker with less effort and fewer errors resulting in lower costs.

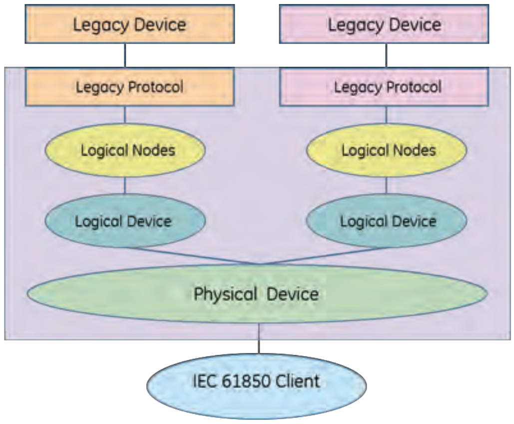


Figure 9.
IEC 61850 Data centrator Architecture

9.1 Interface with Legacy Protocols

Electric power systems are designed to last for many years. For any new technology to be successfully applied into a modern power system, there must be some way to accommodate the use of legacy IEDs and protocols from the past. IEC 61850 is no different and there are several methods for accommodating legacy protocols in an IEC 61850 system. IEC 61850 itself is well suited to accommodate legacy protocols with its logical device model. The ability to support multiple logical devices within a single physical device allows IEC 61850 to directly support the modeling of a data concentrator or multi-device gateway inherently without resorting to techniques outside the scope of the standard. Data concentrator devices (Figure 9) supporting the IEC 61850 logical device model are available with new products under development. In addition to the use of separate data concentrators, OPC technology also offers a way to incorporate simple gateway functionality into a substation SCADA system (Figure 10). In this case, the roles of OPC client and server are reversed from the previous example illustrating a substation SCADA application by building an OPC client application on top of an IEC 61850 server. The OPC client is then mapped to an OPC server supporting any legacy or proprietary protocol. This enables data from legacy devices to be accessed as IEC 61850 data simplifying the client application development by providing a consistent standardized mechanism for data access across the entire substation.

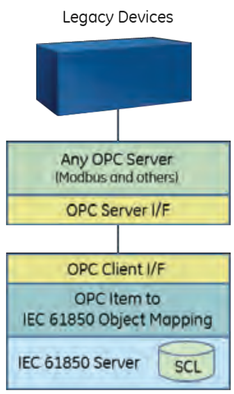


Figure 10.
IEC 61850 Data Gateways using OPC

10. Conclusions

IEC 61850 is now released to the industry. Nine out of ten parts of the standard are now International Standards (part 10 on testing is in the CDV stage). This standard addresses most of the issues that migration to the digital world entails, especially, standardization of data names, creation of a comprehensive set of services, implementation over standard protocols and hardware, and definition of a process bus. Multi-vendor interoperability has been demonstrated and compliance certification processes are being established. Discussions are underway to utilize IEC 61850 as the substation to control center communication protocol. IEC 61850 will become the protocol of choice as utilities migrate to network solutions for the substations and beyond.

11. References

[1] IEC 61850 - Communication Networks and Systems in Substations; http://domino.iec.ch/webstore/webstore.nsf/searchview/?SearchView=&SearchOrder=4&SearchWV=TRUE&SearchMax=1000&Query=61850&submit=OK

[2] Manufacturing Messaging Specification; ISO 9506-1&2:2003; Part 1 – Service Definition: Part 2 – Protocol Specification

070209-v3

Enhanced Security and Dependability in Process Bus Protection Systems

David McGinn, Vijay Muthukrishnan, Wei Wang
GE Digital Energy

1. Introduction

Power system protection is a mission-critical application with demanding requirements in terms of security, dependability and availability.

This paper reports on a new generation protection and control platform designed for enhanced security, dependability and availability. This system is based on traditionally defined protective relays with data acquisition through fully duplicated remote I/O devices (merging units). The I/O devices are deployed directly on or in close proximity to the primary equipment. They communicate their input signals including ac sampled values, contact statuses, and a variety of transducer inputs and execute the trip and control commands using process bus. Message formats are as defined in IEC 61850 [1]. To improve overall system reliability, availability and performance for the task of protection and control, the system does not include any active (switched) communication networks, but is based on simple, dedicated point-to-point Ethernet connections with extensive self-monitoring and inherent security. In particular, by not having active Ethernet infrastructure, the system is not vulnerable to cyber security threats through its process bus.

This paper reviews requirements and practical design solutions for electronics acting as an I/O structure of a protection system when installed in a high voltage switchyard environment, using the above mentioned new protection platform to illustrate the design challenges and solutions. These challenges include temperature requirements, weather proofing, electrical and magnetic fields, conducted and radiated interference, mechanical shock and vibration, and similar conditions. These requirements are applied to mechanical packaging, fiber connectivity, copper wiring connectivity, printed circuit boards, electronic components, internal data buses, and software architecture.

Traditionally, microprocessor-based relays incorporate a certain degree of internal self-diagnostics and checking to guard against internal problems that could potentially result in a false operation or a failure to trip. Extra dependability is achieved in applications using multiple relays in parallel redundancy, while additional security may be implemented by using multiple relays in a voting scheme. The paper describes the implementation of self-testing and redundancy in the presented system, which makes it secure and dependable well beyond the realm of traditional protection and control devices.

In summary, the system reported on features greatly improved immunity to failures of its components, considerably reducing the danger of false tripping while enhancing dependability. The subject of this paper is not just a concept but also a new technical solution now available commercially, and backed up by significant development and testing efforts [2].

2. System Aspects for Reliability, Security and Dependability

In general, the function of a protection system is to limit the severity and extent of system disturbances and possible damage to system equipment. These objectives can be met only if protection systems have a high degree of dependability and security. In this context dependability relates to the degree of certainty that a protection system will operate correctly when required to operate. Security relates to the degree of certainty that a protection system will not operate when not required to operate. The relative effect on the bulk power system of a failure of a protection system to operate when desired versus an unintended operation should be weighed carefully in selecting protection system design parameters. Often increased dependability (fewer failures to operate) results in decreased security (more unintended operations), and vice versa [3].

Another important reliability index for protection and control systems is the attendance rate, the expectation of the number of instances where the system needs to be repaired, re-verified, upgraded, etc. per unit time. With each such instance, in addition to the cost of labour to schedule, prepare for and perform the work, and the cost of any required power element outage, there is a finite probability that an error will occur resulting in an undesired trip operation during restoration to service or afterward. Trips are of special concern where generation is tripped or load curtailed. Infrequent but still of concern is the possibility that a widespread blackout can result, such as occurred on February 26 2007 in Florida [4]. Increased redundancy means an increased number of components, and as each component failure requires a repair attendance, the failure rate of each component contributes to the total attendance rate.

Dependability and security can be obtained through the appropriate use of redundancy. For instance, a voting scheme may be proposed wherein tripping occurs only when at least two of three independent protection systems indicate that tripping is required. However, voting schemes complicate the application in terms of engineering, implementation, commissioning and testing, potentially increasing the risk of unexpected operations due to procedural or site crew mistakes. The extra hardware alone yields a higher attendance rate. Care must also be taken that the vote counting system does not compromise the reliability of the system or the independence of the protection systems.

Previous studies on the impact of IEC 61850 [5], in particular of so-called process bus systems, on protection and control reliability have shown that a generic system architecture based on merging units explicitly synchronized via an external stand-alone source and communicating via Ethernet networks would drastically reduce overall protection system reliability by an order of magnitude compared with today's microprocessor-based relays. This is because of substantial increase in the total part count and complexity of such a distributed system as compared with today's integrated microprocessor-based relays.

A successful process bus system architecture, where individual copper wires are replaced with fiber optic communications, must be driven by the needs of the underlying application – in other words the architecture must be fit for purpose of protection and control. The system architecture would therefore have to keep the total part count and complexity at the level of today's relays in order to maintain the current expectation for overall system reliability.

3. A Protection and Control System with Enhanced Security and Dependability

3.1 Overview

HardFiber™, the protection and control system presented in this paper, is based on an architecture that incorporates application-driven requirements for performance, maintainability, expandability and reliability. This is achieved through the use of remote I/O devices to collect CT/VT and status signals, and to output CB/process control signals [2,5]. In the presented system, these remote I/O devices (Bricks), fulfill the role of IEC 61850

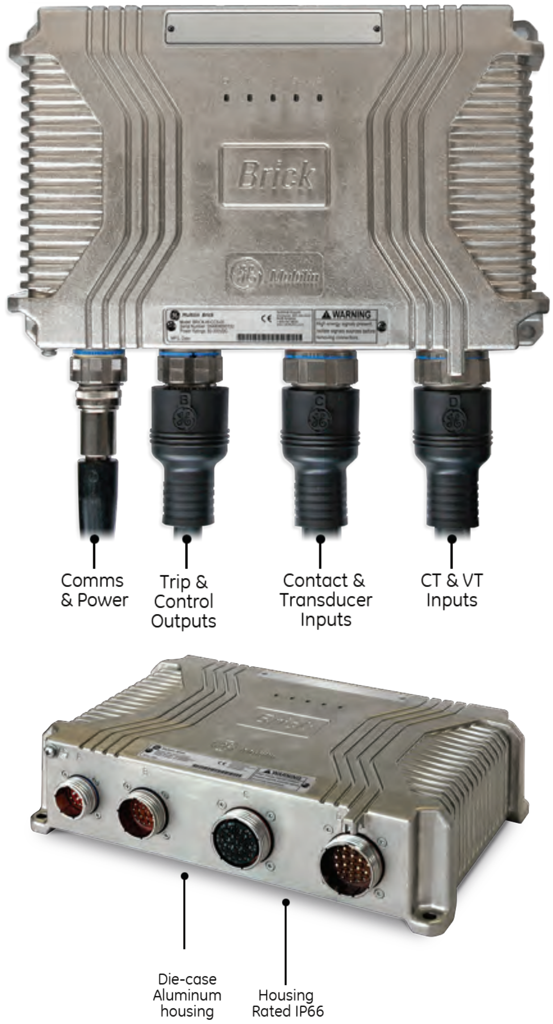


Figure 2.
Brick - rugged outdoor merging unit

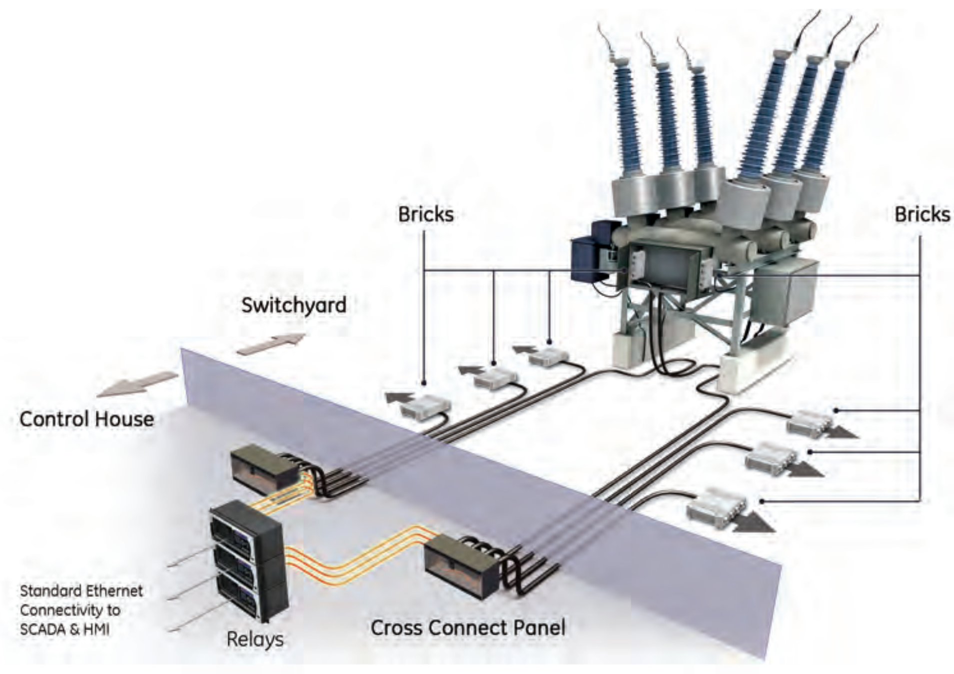


Figure 1.
HardFiber process bus architecture

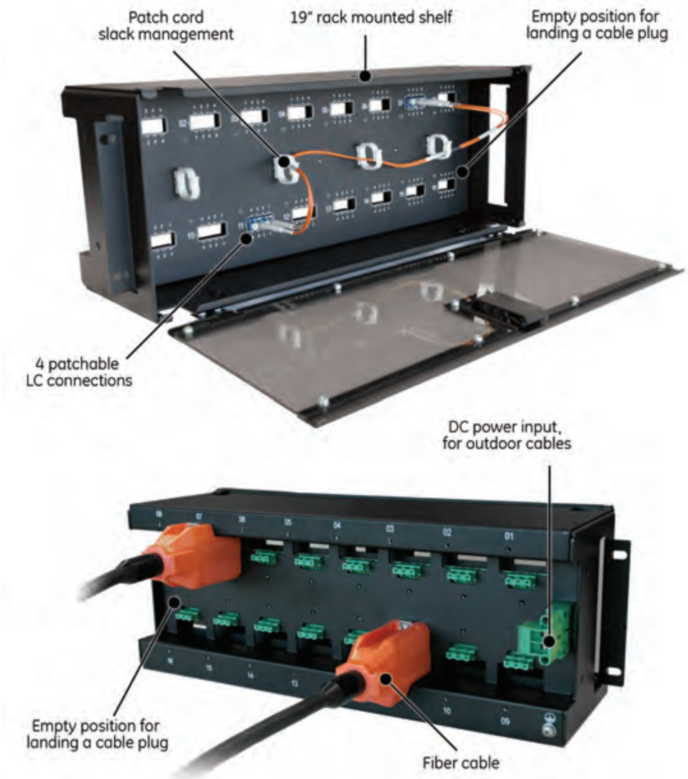


Figure 3.
Fiber communication cross connect panel

merging units [1]. The IEC 61850-9-2 sampled value output of each Brick and the IEC 61850-8-1 control for each Brick are communicated via pre-terminated fiber cables to a cross connect panel that connects the Bricks to the appropriate relays.

Readers already familiar with the HardFiber system may wish to advance over this overview and the following architecture section, to the Design Considerations for Process Bus Device Reliability section.

In reference to Figure 1, the system includes Bricks mounted at the primary apparatus, relays mounted in the control house, pre-terminated cables, and fiber cross connect panels for patching fiber connections from Bricks to relays.

The Bricks are designed to interface 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 trip/close control, disconnect switch status and control, temperature and pressure readings, and so on. The Bricks are designed for the harsh environments encountered there, including temperature extremes, shock and vibration, electromagnetic compatibility, sun exposure, pressure washing and exposure to salt and other harsh chemicals (Figure 2).

Each Brick contains four independent digital cores, each composed of a microcontroller with individual bi-directional (bi-di) fiber links. Each core provides dedicated point-to-point communications with a single relay using messages conforming to IEC 61850-8-1 (GOOSE) and IEC 61850-9-2 (Sampled Values). These digital cores share the analog core's common input/output hardware, implementing a fail-safe hardware design strategy that ensures total signal isolation and independence of the digital cores.

Cross connect panels are used to land and organize the fiber cables to the relays and Bricks, and to distribute and individually fuse the DC power to the Bricks (Figure 3). Standard patch cords are used to accomplish "hard-fibering", making on a one-to-one basis all the necessary connections between the relay ports and Brick cores as dictated by the station's physical configuration, without the use of switched network communications (Figure 3).

The system is currently implemented on the existing GE Multilin Universal Relay platform, which supports all typically required applications. An option module provides each relay with eight optical fiber ports so the relay can directly communicate with up to eight Bricks (Figure 4). These maximum connectivity numbers have been selected upon careful analysis of substation topologies and required data traffic patterns [6]. As such, the 8/4 connectivity (each relay can communicate with up to 8 Bricks, and each Brick can communicate with up to 4 relays) covers most typical applications. Each relay provides protection for one zone, conforming to established protection philosophies. It receives the signals to perform its function over secure and dedicated direct hard-fibered links to each of the associated Bricks. The completely deterministic data traffic on these dedicated links allows the use of a simple and robust method for sampling synchronization whereby each relay controls the sampling of the connected Brick digital cores over the link without relying on an external clock or time distribution network.

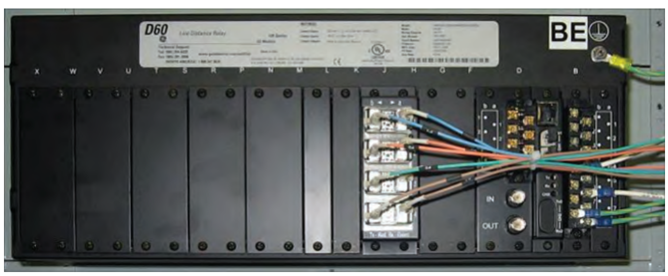


Figure 4.
Connections on a UR-series relay

Brick order code	Brick inputs and outputs							
	CONNECTOR D			CONNECTOR C		CONNECTOR B		
	AC CURRENTS		AC VOLTAGES	CONTACT INPUTS	RTD/TDR INPUTS	CONTACT OUTPUTS		
	1A	5A				SSR	Latching	Form-C
BRICK-4-HI-CC11	8	---	---	3	18	4	1	2
BRICK-4-HI-CC55	---	8	---	3	18	4	1	2
BRICK-4-HI-CV10	4	---	4	3	18	4	1	2
BRICK-4-HI-CV50	---	4	4	3	18	4	1	2

Table 1.
Brick process I/O capacity

To improve reliability and to facilitate design, construction, testing and maintenance, the system is designed to be as simple and modular as possible. Bricks are designed such that they have no stand-alone firmware, individual configuration files, or data processing algorithms; their sole function is to be a high-speed robust IEC 61850 interface to the switchyard, a media and protocol converter. The system "configuration", in this case the specific mapping of relays to their associated Brick digital cores, is handled purely in the physical domain through the provisioning of individual dedicated fiber optic connections.

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 Brick is negligible compared with the gain of simplicity and independency of relays in the system. Similarly, the cost of point-to-point connectivity is acceptable given the gain of avoiding active network devices and ability to perform system maintenance and isolation. [7]

The point-to-point communications architecture provides a major dependability and security advantage over packet switched network architectures. The lack of switches, and their associated failure mechanisms provides the dependability advantage. Although the system dependability problems associated with switches may be largely overcome through switch redundancy, the redundancy adds problems in terms of system testing, and increases the number of failures that do not impair dependability but must be attended to nonetheless. It is important to note that the total number of transceivers in the presented and in a switched architecture is comparable due to the limited number of Bricks a relay needs to interface to in a practical switchgear topology. The direct relay to Brick communications architecture, without intermediate switches, makes this process bus architecture essentially immune to cyber security threats as there is neither need nor mechanism for external access.

The configuration for individual protection applications is relay-centric, exactly as it is today. All process inputs are always sent from each Brick to all of the connected relays, and all valid commands are accepted from the connected relays. The relays themselves determine which subset of the received collection of signals will be consumed internally for protection algorithms and logic schemes. Similarly the relays determine which specific commands are sent to which Bricks. Firmware management is exactly the same as with relays today; the Brick digital cores inherit whatever firmware is required from the connected relay.

3.2 Architecture

The example in Figure 5 illustrates the architecture of the system. A second system not shown provides a completely redundant protection system, and may or may not use a different technology.

In this example, duplicate Bricks are employed on each circuit breaker and on each bank of voltage transformers. Each circuit breaker Brick (numbers 1, 2, 5, 6, 9 and 10 in the figure) acquires the three-phase bushing CT signals on each side of the breaker, breaker position and alarm contacts, as well as outputting breaker trip and close contacts. The Voltage Transformer Bricks (numbers 3, 4, 7 and 8 in the figure) acquire the three phase VT signals and line disconnect positions, as well as outputting line disconnect open and close contacts.

As is apparent from this figure that to perform their protection function, the relays need to interface with several Bricks installed at different locations within the switchyard. For instance, the D60 line distance protection relays need to communicate with Bricks on two breakers and on one VT. For this reason, the relay has eight optical fiber ports, allowing each to connect to up to eight Bricks. Conversely, Bricks will need to interface with several different relays. For instance Brick 5 on the center breaker needs to communicate with the zone protection relay on each side of the breaker and the breaker failure relay. Thus Bricks have four digital cores, each of which can communicate exclusively with one relay. Fiber connections to all the process bus ports of all the relays and all the digital cores of all the Bricks are brought by indoor and

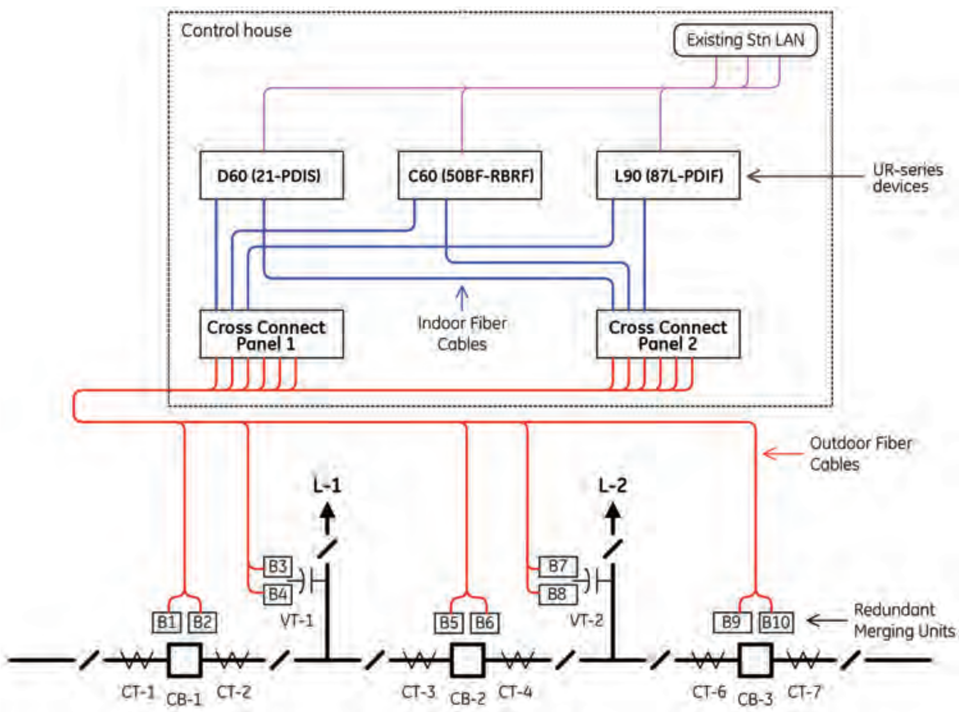


Figure 5.
Example system illustrating the architecture

outdoor multi-fiber cables to cross connect panels. At the cross connect panels, each fiber of each cable is broken out to an LC type optical coupler. Patch cords then interconnect Brick digital cores to relay ports according to the functional requirements and physical configuration of the station's power apparatus. Thus continuous and dedicated point-to-point optical paths are created between relays and Bricks, without switches or other active components. This patching or "hard fibering" is what gives the HardFiber system its name. This hard fibering approach takes advantage of the fact that a relay needs to talk to only the few Bricks that have input or outputs related to that relay's function, that only a few relays need the I/O of any given Brick, and that the necessary relay-Brick connections change rarely, only when the station one-line changes. For those few instances where more than four Brick digital cores are required, for instance for VTs on a large bus, additional Bricks can be installed sharing the same copper interface to the primary apparatus.

Figure 6 provides an expanded view of a portion of the example system. In this example, digital cores from Bricks 1, 3, and 5 are connected to the D60. A single digital core in Brick 5 is connected to the C60, and digital cores from Bricks 5 and 9 are connected to the L90. Note that the choice of specific cores and specific relay ports is arbitrary – Brick cores are functionally identical, as are the relay HardFiber ports.

The various relay protection and measuring elements that use AC data from multiple Bricks must have the currents and voltages at various locations sampled at the same instant. The existing method for determining the time of the samples is maintained. Each relay contains a sampling clock that determines when it needs samples to be taken. In the case of the UR this clock is phase and frequency locked to the power system quantities measured by that relay, although other sampling schemes are possible by other relays. At each tick of the sample clock, a GOOSE Ethernet frame is sent by the relay to each Brick digital core connected to that relay. Digital cores sample the measured quantities on receipt of each frame. As the digital cores are fully independent, different relays may sample at different rates or with different phase, but as each is connected to different and independent digital cores, there is no conflict. Thus each relay is able to sample in a fashion optimal for its application, independently from other relays, and no external clocks are required.

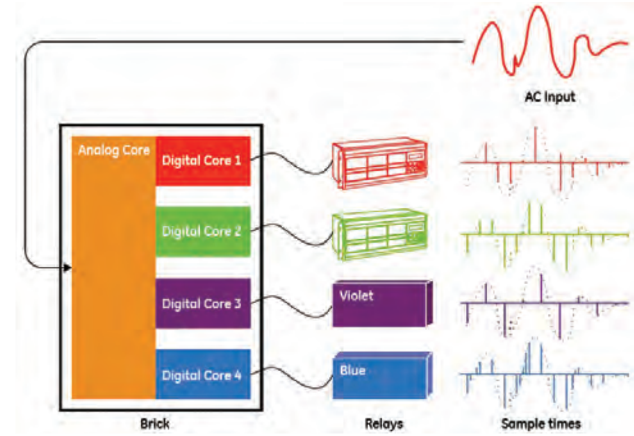


Figure 7.
Brick digital cores sampling asynchronously

4. Design Considerations for Reliability of Process Bus Devices

4.1 Component Quality and Environmental Compatibility

As in the case of any device, proven design rules, tempered with practical in-service experience, should be followed when designing protection devices and systems. This includes component selection, circuit synthesis and analysis, thermal modeling, mechanical design and so on. In this respect, designers are bounded by the commercially available components and tools. Reliance on special components or tools is not recommended – such solutions are typically cost-prohibitive, have limited selection and number of suppliers, and face availability and life cycle management issues.

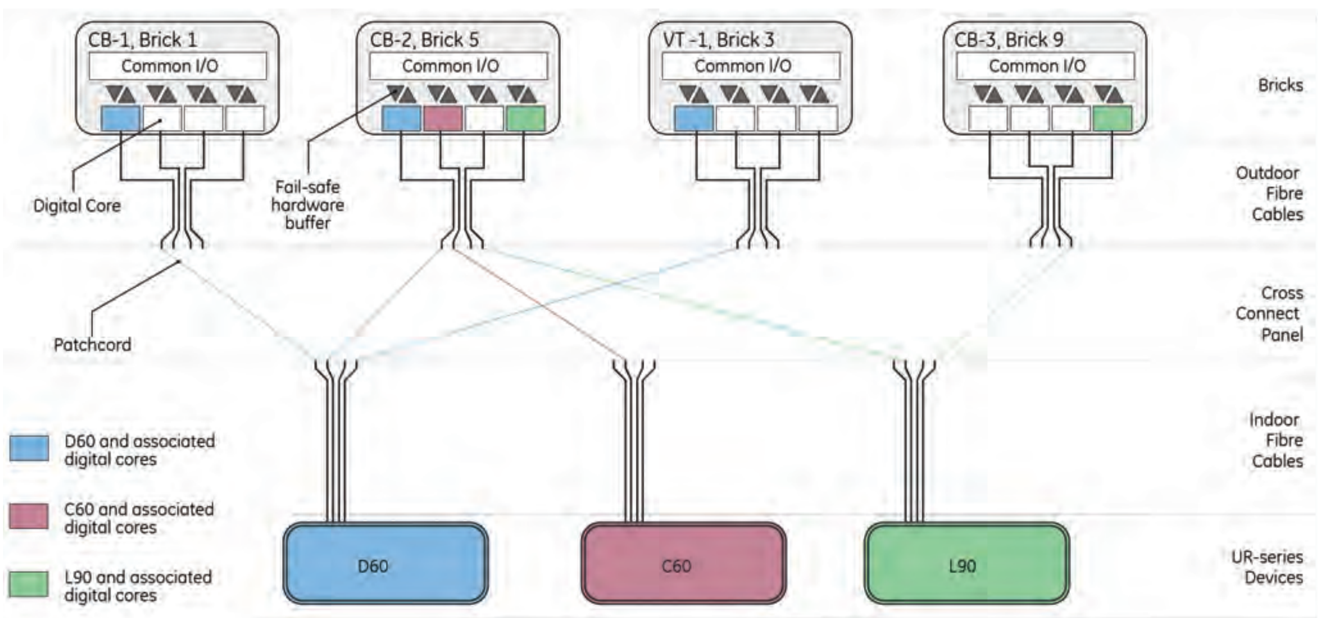


Figure 6.
Hard-fibered cross-connection of Bricks and relays

4.2 Fail-Safe Design

One important aspect of the security of protection is a fail-safe response to internal or external relay problems. With respect to internal problems the ideal outcome is that a single component failure should not cause the protection to issue a spurious command. Moreover, such a failure should be detected by internal diagnostics and alarmed so that corrective actions can be taken. With respect to external factors, protection systems are expected to withstand certain environmental conditions from electromagnetic compatibility requirements, through weather conditions, to mechanical stresses. Furthermore, if a protection system fails due to external factors, it is expected to fail-safe: not to issue spurious commands, or to report false values or status.

From the technical point of view, the fail-safe response of protection systems to avoid unwanted outcomes is arguably the most important factor in the design of such systems. The task is not to attempt to design electronics that will never fail, as all electronics will eventually fail – rather the task is to design a system with good overall reliability meeting established reliability targets that will be able to detect component failures and fail in a safe way.

The fail-safe aspect of protection security is achieved by building internal monitoring and redundancy. Internal relay parameters are measured and compared against their expected values. Monitoring a supply voltage to operational amplifiers comprising analog filters in a relay is a good example. Similarly, some subsystems can be duplicated or some operations performed multiple times in order to detect discrepancies and respond to internal failures. Using two duplicated AC measurement chains within a single relay as a good example of internal redundancy.

Care must be taken when adding monitoring circuits or duplicated subsystems, not to complicate the device and impair other aspects of its performance. Simply adding more monitoring circuits will in fact adversely impact the reliability of the device and the availability of the overall protection. The monitoring systems introduce additional components and therefore new failure modes, while driving up the attendance rate. The adverse impact of extra hardware to provide for monitoring or redundancy can be avoided by designing systems that are inherently simple. Keeping the design simple with minimum number of components and using good engineering design fundamentals optimizes performance for dependability and security, the initial design is better, manufacturing is less prone to errors and quality issues, and reliability is higher due to lower component count.

One important observation with respect to fail-safe design is the distinctly different response of analog versus digital systems to internal failures. Digital systems tend to fail gracefully in that they yield a solution that either works or it stops functioning in a self-evident way. Monitoring is based on a finite set of cases that can be explicitly tested through such mechanisms as watchdogs and data integrity checks where pass/fail criteria are very clear and testing can be built into the system itself.

Analog circuits on the other hand are prone to malfunction in ways that are not explicitly clear. A change in an analog to digital converter (ADC) reference supply for example will appear as a change in the signal being sampled. If this signal is used by a sensitive protection element such as current differential, this may result in an unwarranted protection operation. It is therefore necessary to provide additional monitoring for such analog systems.

It is important to note that at the lowest level, all circuits are analog. For example, if the supply voltage to a microcontroller drops for a short period, the microcontroller may enter a state where it will not behave as designed. Therefore, it is prudent to monitor parameters of digital circuits to make sure they behave as digital circuits, and count on inherent properties of digital circuits to ensure fail-safe operation.

Yet another aspect of design for reliability and fail-safe operation is the proper identification of working conditions: temperature, EMC levels, mechanical factors, humidity, and so on. With respect to protective relays, well-established standards exist and are followed. These standards are verified by the significant installed base and performance history of microprocessor-based protective relays. However, with respect to devices mounted in close proximity to the primary apparatus the industry experience and installed base is limited, so environmental standards for these types of systems will likely need to evolve to take into account new in-service experience.

The following sections will explain how the above principles have been applied to the new protection and control system described in this paper.

5. Design Implementation for Component Reliability

5.1 Outdoor Communications Cable

Mechanical Design

The optical fiber is packaged in a rugged cable to ensure mechanical survival. The cable is designed to meet United States Department of Defence (DoD) standard MIL-PRF-85045 for ground tactical cable, and is suitable for indoor and outdoor installation in direct burial trenches, common use cable pans/raceways/ducts, and when exposed to direct sun and weather. Figure 8 shows the cable cross section, with its multiple layers of protection. Figure 9 shows an actual direct burial installation in progress.

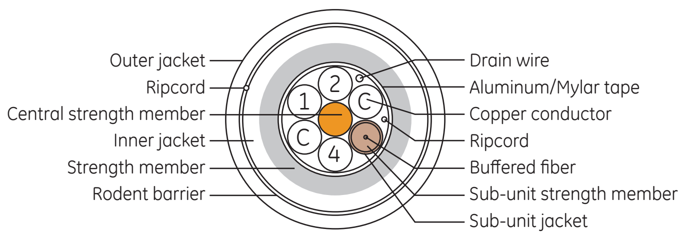


Figure 8.
Cross section of outdoor communications cable

To ensure dependability of the connections and reduce the Mean Time to Replace (MTTR), standard military MIL DTL 38999 [8] type connectors are employed. This particular technology has a long history of dependable performance in challenging environments such as aerospace and naval applications. As such, they are an ideal fit to be deployed in the intended installation environment for the Bricks.

Optical Fiber

To achieve high dependability of the digital communications between the Bricks in the electrically noisy switchyard and the relays in the control house, optical fiber media is employed. The immunity of optical signals to electrical and magnetic interference is well known. The integrity of the data, and thus system security, is further protected by the 32-bit cyclic redundancy check code (CRC) that is a standard part of Ethernet communications. The same relay-Brick link is used for process data acquisition, time synchronization, control (i.e. trip and close), and diagnostic reporting.

Figure 9.
Outdoor communications cable in direct burial application

To further increase system reliability, a single bi-directional (bi-di) fiber is used for each link, as one fiber using a single transceiver at each end will be more dependable than two fibers and two transmitters and two receivers. Course Wavelength Division Multiplexing (CWDM) is used for full duplex communications on a single fiber, such that the signals in one direction use a different wavelength (frequency) from that of the signals travelling in the opposite direction, so that they may be discriminated from each other. As shown in Figure 10, wavelength selective mirrors in each transceiver reflect the incoming light to the receiver, while allowing the outgoing light to pass straight through and out. The physical Ethernet interface is implemented according to standard IEEE 802.3 2005 100Base BX bi-directional fiber optic communications [9].

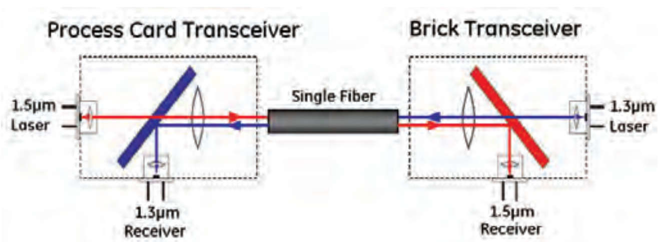


Figure 10.
CWDM bi-di optical link

This bi-directional fiber technology has had substantial successful experience in FTTX (fiber to the premises) applications, particularly in Japan, so the technology is well established and designed for high reliability in potentially harsh environments. The transceivers used to implement the bi-di links have passed all the shock, vibration, temperature cycling and accelerated aging tests described elsewhere, and are thus expected have a negligible contribution to failure rates. On the other hand, each link has half as may optical fibers and transceivers as an equivalent dual fiber Ethernet link, so overall higher reliability can be expected.

Multimode fiber with a 50μm diameter core rather than single mode 9μm fiber is used in the fiber cables. This large core makes the connectors much more tolerant to contamination and misalignment problems. A misalignment a minor impact on a 50μm core could totally obscure a 9μm core.

The optical fiber cables are fully pre-terminated within a factory environment using special purpose jigs, automated testing, and personnel particularly trained with the necessary skills, so that consistent, highly dependable fiber terminations are obtained. Conversely, fiber splicing/termination performed on-site in the field would be done in an environment that may be non-ideal in many respects, leading to instances of poor fiber dependability.

Embedded Copper

The outdoor communications cable also embeds a pair of copper wires along with the fiber optic cables. These copper wires are individually fused at the control building end and are used to provide a reliable power supply to each Brick. From a reliability standpoint, each cable becomes a single unit connection for each Brick rather than relying on two separate connections to independently provide power and communications access. The end result is improved reliability of the overall system. In other words, if the Brick is powered, it will be able to communicate and conversely if the Brick communications are connected, the Brick will be powered.

There is an additional rationale to include the power connection for the Brick along with the communication cable, in that there may not be a convenient uninterruptible supply where a Brick is to be installed. For example, a Brick located on a VT structure will have no local DC station battery supply. Self-powering a Brick from the connected AC signals is not advisable, as outage or fault conditions will render the Brick, and potentially the upstream protection application, unavailable.

5.2 Brick

Bricks are intended for direct installation on or in proximity to primary equipment without requiring additional environmental protection. The solution is to provide a common chassis to clad the electronics, provide EMC shielding, provide weatherproofing, and act as an overall heat sink for the heat-generating electronics. This opens new design opportunities in terms of mechanical and thermal design.

Mechanical Design

Shock and vibration requirements for installation on breaker structures and in close proximity to power transformers call for a sturdy and heavy chassis. Cast aluminium is a rational choice for both mechanical and thermal reasons. EMC and environmental requirements call for a cage-like design with minimum number of openings with overall aperture areas minimized. The openings need to be hermetically sealed to guarantee performance at IP66 (dust tight, pressure washing), and limit the air gap for better EMC immunity.

Heavy components, such as the AC input isolating transformers and the integrated power supply need to be mechanically secured by encasing them as separate integrated components and mounting them directly to the Brick chassis.

Thermal design considerations for critical heat-generating components are accounted for by mounting these components such that they use the chassis itself as a heat sink. At the same time, Bricks mounted outdoors are exposed to so-called insolation or "sunloading" effects – heating due to absorbed solar energy. This calls for striking a balance between the ability to transport the heat out of the chassis from the hot components inside, and minimizing the absorption of the radiated solar energy and heating effect on the components inside the chassis. A black matte finish maximizes heat radiation out of the Brick, but also maximizes absorption of solar radiation. A bright reflective finish minimizes absorption, but also minimizes radiation. This effect is not new and in fact standards such as IEC 60068-2-9 [10] and MIL-STD-810F [11] exist to address these issues. These standards call for over 1,000 W/m2 of solar radiation under an ambient air temperature of 50 degrees C. A relatively small amount of heat needs to be to dissipated, so a reflective finish is used. In order to ensure adequate sunload immunity under worst-case scenarios where the Brick chassis is dirty or otherwise non-reflective, solar testing was also performed with the specimen Brick painted matte black.

The Brick needs to be designed for both hot and cold temperatures. Under cold temperatures mechanical properties of fiber and cold temperature start-up sequencing of the electronics become a concern. Necessary design considerations include avoiding fiber connections by using pigtails embedded in transceivers, securing the fiber mechanically and testing under combined temperature and mechanical conditions.

The tests shown in Figures 11, 12 and 13 show environmental tests for dust ingress, water ingress and sunload effect.

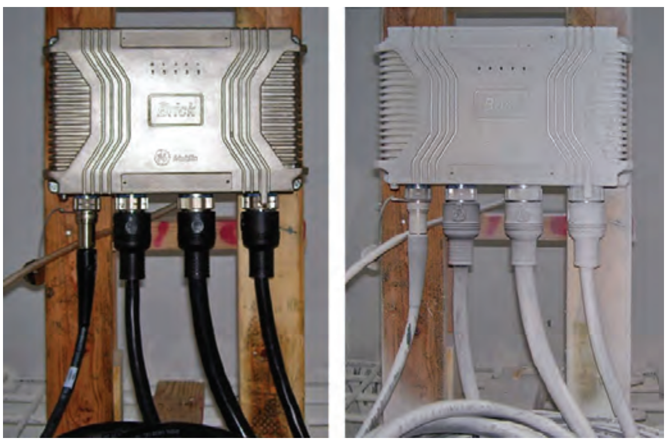


Figure 11.
Dust ingress testing for IP6x: pre-test (left) and post-test (right)

Figure 12.
Water ingress testing for IPx6: pre-inspection (left) and post-inspection (right)

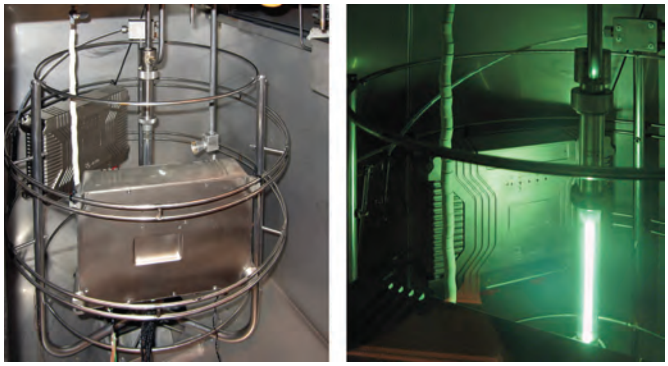


Figure 13.
Solar loading tests at the solar laboratory: Bricks mounted next to light source (left), solar radiation test in progress (right)

Connectorized Interfaces

Terminations of the remote I/O device (Brick) are pre-connectorized using standard off-the-shelf MIL-DTL-38999 connectors. These connectors are available from multiple vendors and are used in naval, military, avionics and industrial applications because of their high performance and reliability including shock and vibration, IP rating, proper electrical parameters and extremes of temperature.

By selecting an extremely rugged and reliable connector technology, a number of design challenges for implementing reliable remote I/O devices are solved simply with a widely accepted hardware solution. The Mean Time to Replace (MTTR) is reduced by reducing Brick replacement time without the need to re-commission physical connections. Adoption of standard, reliable and proven connectors benefits from millions of unit years of field experience, lessons learned, independent verification tests and other aspects relevant to the overall reliability of the system.

An AC input connector brings the secondary currents into the Brick. A danger exists of opening the connector with the CTs live. Development of a self-shorting mechanism embedded in the connector would prevent the use of standard connectors, and would jeopardize reliability of the connector by adding moving parts. Following the principle of a simple design, the presented system uses a simple mechanical feature to prevent accidental disconnection of a live CT cable: the yellow collar shown in Figure 14 below. This is a good example of a design to avoid adverse impact on reliability of the system.

Figure 14.
Safety device protecting against accidental opening of a live CT secondary circuit

Electronics

The Brick power supply is a good example of how a simple design can improve reliability by eliminating the need for electronics that have an adverse impact on reliability. A common source of failures in microprocessor relays is their power supply, in particular electrolytic capacitors used in the power supply to provide "hold-up" so a momentary interruption of the DC station battery does not force the relay to have to restart, a process that may take many seconds. Regardless of the grade of component selected (automotive, industrial), electrolytic capacitors have been repeatedly shown to be a reliability concern.

The simplicity of the Brick allows it to be fully functional within milliseconds of being energized as opposed to several seconds as with relays. By having the Brick start so quickly, the availability of protection from being momentarily powered down is virtually unchanged so there is no need to provide hold up in the power supply. This eliminates the electrolytic capacitors from the power supply, and reliability issues that they introduce.

Contact Inputs

The Brick contact inputs use dry contacts, with a 24 VDC sensing voltage provided by an internal isolated wetting supply generated by the Brick. The low wetting voltage allows a low sensing circuit impedance and a high wetting current. Low input impedance makes the Bricks highly immune to incorrect status indication due to induced transients or insulation degradation in the external contact wiring. High wetting current assists contact "wipe" action in obtaining a clean contact by burning off contact surface contamination. Having wetting supplies isolated independently for each Brick prevents station battery grounds and grounds in other Brick's contact input circuits from causing incorrect status indication. The Brick contact input supplies are also designed so that two Bricks may be paralleled across a single dry contact, buffered such that the failure of one Brick will not adversely impact the operation of the remaining Brick.

Control Outputs

The Brick contains four solid-state relay (SSR) outputs, based on an existing highly tested and field-proven design, to directly interrupt typical breaker trip and close circuit currents. The SSR outputs were chosen with no moving parts so that mechanical vibrations caused by a breaker mechanically operating could not cause a spurious or undesirable contact closure. The SSR outputs themselves are thermally bonded to the cast aluminium shell of the Brick, so the entire chassis acts as a heat sink improving the life expectation for the SSR outputs.

Analog Inputs

The self-testing involved with AC and transducer inputs is worth further discussion.

Two ADCs are employed on each AC input, as shown in Figure 15. The input to the high range ADC is scaled to accept high currents without saturating. The input to the low range ADC is scaled for accuracy at low currents, but clips for currents much above nominal. At each sample instant, the programmable logic device (PLD) starts a conversion on both ADCs, and coordinates sending both conversion results to the digital cores. Microcontrollers in the digital cores use the low range ADC value if not saturated, otherwise they use the high range ADC value. Part of the reason this is done is that available monolithic analog to digital converters (ADCs) with sufficient speed to sample at the rates demanded by today's relays cannot provide the necessary metering accuracy without saturating at high fault currents.

The other reason for dual ADCs on each input is that it provides a unique opportunity for continuous self-testing of the AC input hardware.

Phase CT current inputs are at most times at a level where the waveforms are continuously in the low range. However, except near zero crossings the high level ADC retains sufficient accuracy that there ought to be no significant difference between the high and low range values after accounting for the design scaling differences. Any significant difference indicates a failure in one range or the other. The comparison is made on a sample-by-sample basis, so protection can be disabled before the invalid data is consumed. Disabling protection on detection of invalid AC input data is an immediate security benefit. It also has a positive impact on dependability, as it alarms triggering rapid corrective action.

In addition to dual ADCs, dual anti-alias filters and dual input conditioning and gain stages are provided so that problems in these areas are also detected by the same comparison. The

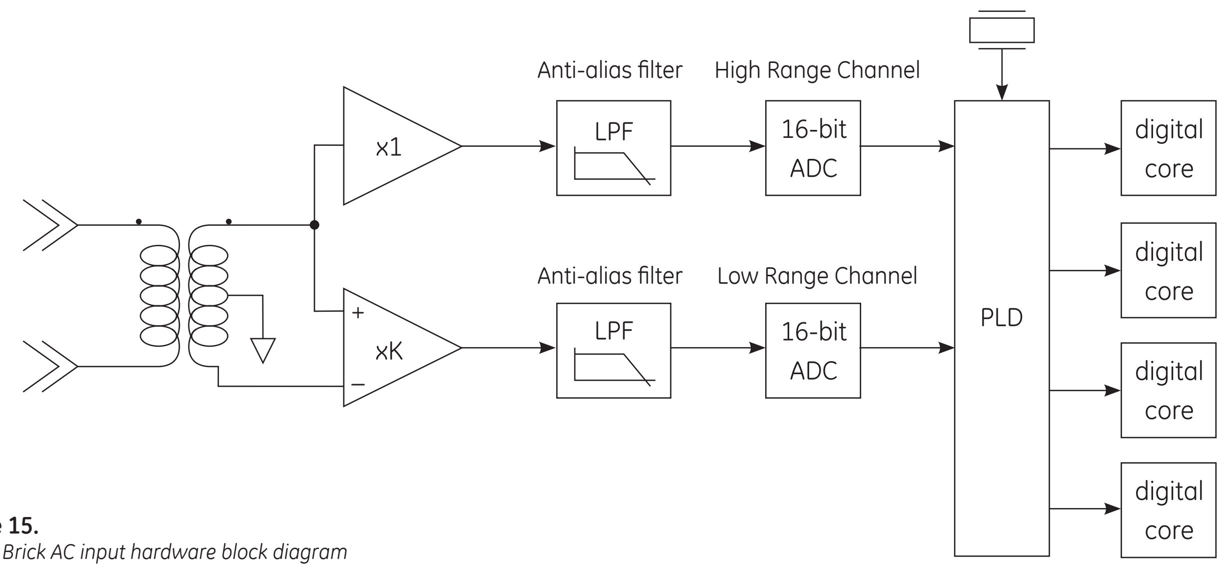


Figure 15.
Typical Brick AC input hardware block diagram

low range uses the entire secondary winding of the isolating transformer, while the high range uses only half of the secondary. Thus any trouble in the isolating transformer secondary will be detected as well. The comparison is made in the digital cores, providing detection of troubles getting the data through the PLD and into the microcontrollers. Thus the entire AC input hardware circuit is covered, with the exception of the isolating transformer primary, which for CT inputs consists simply of either one or five turns of heavy gauge wire.

Figure 16 illustrates the comparison process. The low (blue) and high (red) range scaled readings are shown in the top graph; the selected signal in the middle graph, and the error flag in the bottom graph, for the case of a 1.2 times nominal current experiencing a negative 20% error in the high range channel.

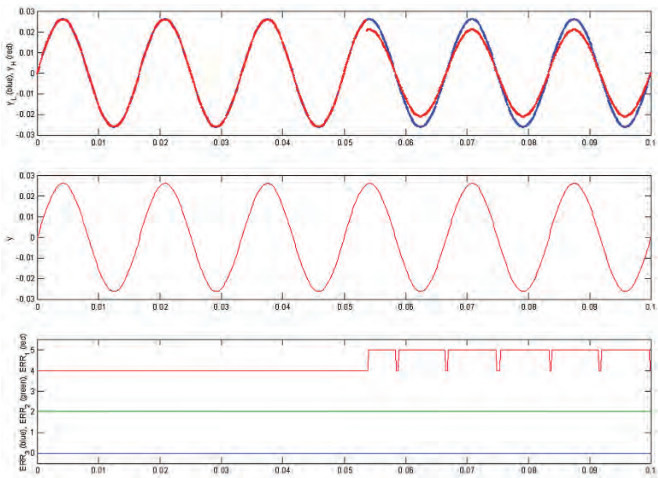


Figure 16.
Simulation of a high range gain error on a CT input

When the input signal is so high that the low range clips the peaks, as happens with normal values of VT inputs and on CT inputs during faults, the comparison can still be made in the vicinity of zero crossings. Figure 17 shows a case of a 70V voltage losing reference in the high range channel. The trouble is detected, but after a short delay of up to ½ cycle.

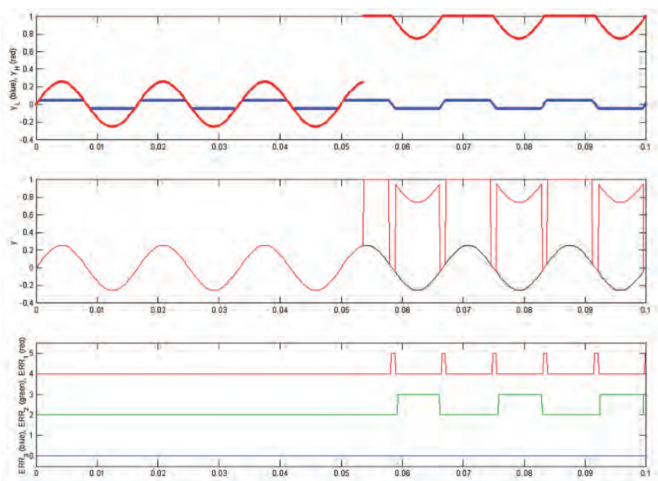


Figure 17.
Simulation of a loss of high range reference supply on a CT input

5.3 Relay

In the presented system, the relay (IED) portion transforms from a mixed analog and digital device to an almost exclusively digital device as all analog inputs and outputs are eliminated and replaced with digital communications. As a result, the relay portion of the system becomes much more reliable and intrinsically fail-safe. The reliability gain is achieved by reducing the individual part counts, and by using digital components that tend to be more reliable due to their highly integrated packaging and pre-determined failure mechanisms. The fail-safe improvement is caused by the nature of digital systems as explained in the previous section. The input and output signals are moved between different digital subsystems of the relay (receiving transceivers, communication processor, digital signal processors, main logic processor) as digital packages with embedded data integrity protection (CRC, check-sum). All digital components are properly engineered (monitored rails, watchdog, code integrity checks, etc.) yielding a very robust system.

Communication-based protection and control systems require more design attention in terms of dealing with permutations of various conditions related to distributed architectures, multiple devices and communication traffic and impairments. Development of distributed architectures is not a new enterprise - there is a great deal of experience accumulated from engineering internal architectures of modular relays and engineering and application of digital line current differential or distributed bus differential relays.

In the case of the particular design presented in this paper, the relays are built using an existing relay platform with a decade-long field record, the maturity of a large portion of hardware and firmware being carried over to the new system. This modular relay series uses just one new hardware module to interface with the remote I/O (Bricks) and keeps the existing power supply, CPU and teleprotection modules intact. Even the existing firmware is used – the I/O data are seamlessly integrated with the rest of the relay.

In this way some 80% of the relay hardware is not changed, and some 95% of the relay firmware is not changed. Moreover, the new relay is not a new model or variant of the existing relay, but an option on the existing platform. In this way even the impact of regression during development of the code has been drastically reduced as only a small amount of new code was added to the existing proven relay firmware.

In this way a significant portion of the field experience in terms of hundreds of thousands of unit years of run time, independent testing of hardware and algorithms, and exposure to actual system conditions can be instantly assigned to the relay and application portion of the new protection and control system.

5.4 Extensive self-testing

The described protection system implements extensive self-testing in order to reduce the repair response delay thus increasing availability and dependability, and to flag unreliable data so that it is not used to make operational decisions thus increasing protection system security. It is critical that internal self-monitoring within the system overlaps adequately to ensure complete end-to-end self-testing. The concept of overlapping test zones is shown in Figure 18.

It can be seen that there are a number of self-test zones within the system, each individual self-test zone overlaps with at least one other zone.

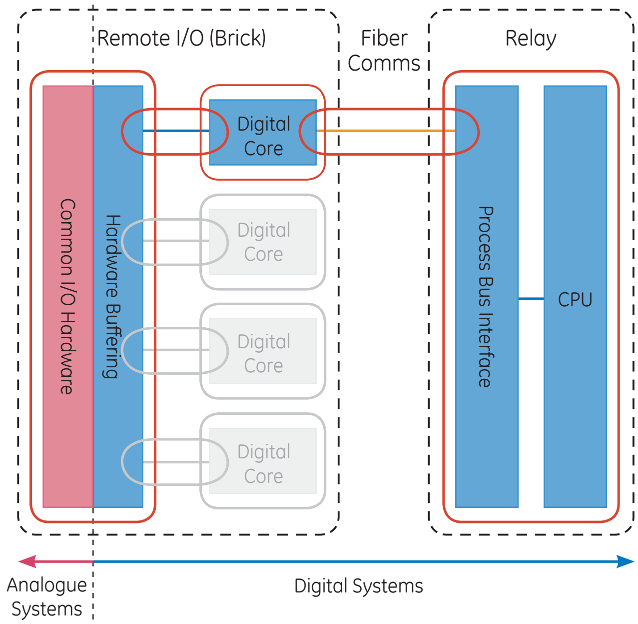


Figure 18.
Overlapping test zones within the system

The specific self-tests within the Brick include the following:

- On each AC and each transducer/RTD input, correspondence of the high range analog to digital converter output with that of the low range analog to digital converter.
- Proper sequencing of the analog to digital converters through monitoring of their Busy status output.
- Temperature of the analog to digital converter.
- Output levels of each of the internal power supplies.
- Watchdog timers, one external to each microcontroller, which together with firmware in the microcontroller verifies all tasks are running as designed.
- Microcontroller flash memory integrity through CRC-16 checking.
- Communications between the analog core and each digital core in each direction are uninterrupted and each frame's CRC-16 shows data is uncorrupted.
- Match in clock frequencies between the analog core clock and each digital core clock.
- Correspondence of each contact output driver to the received command for that contact.
- Correspondence of an auxiliary contact on the latching output relay to the latching output command.
- Monitoring of the voltage across and current through each SSR contact output, used by the relay to monitor the health of the external control circuit.

The tests of the fiber optic communications include:

- Signal quality of each of the optical fiber links, including the send and receive optical light levels at each end, transmitter bias current, and transceiver temperature.
- Integrity of each frame sent and received on the optical fiber links through CRC-32 checking, lost frames are detected with sequence numbers.

The relay itself also runs a complete set of internal self-tests as per established relay design philosophy, including processor watchdogs, program execution and internal data integrity checks.

Also, it is important to note the dividing line between analog and digital systems. The amount of the system that is based on analog circuitry is limited to the interface to the primary power system process. The rest of the system is entirely digital, allowing for this high degree of built-in error checking and diagnostics.

5.5 Continuous Monitoring

In order to ensure the security of protection, each Brick core continuously monitors its key internal subsystems including the common hardware (ADCs, output relay circuits) and the status of the core itself. Each core includes this diagnostic information with each set of samples transmitted to the connected relay. In the event of a failure of an internal diagnostic test, the connected relays are made aware instantly and can then ensure that the overall protection system will fail to a safe state.

Additionally, each core continuously monitors the optical transmit and receive power from the associated transceiver and sends this data to the connected relay. Each transceiver in the relay measures the same quantity and then calculates the respective power link budget for the connection. In this case, troubles related to the degradation of the optical communications path can be determined early and explicitly.

5.6 Duplicated I/O Hardware

The protection system presented in this paper provides the user with the ability to control the dependability and security of the system by supporting duplicate Bricks (the remote I/O modules), as illustrated in Figure 5. The primary sensors for signals critical to system reliability can also be duplicated, the signals transmitted thought independent Bricks and independent optical fibers to the relay, where a variety of options exists for reacting to loss of communications with the Bricks, Brick self-test error conditions, and inconsistency of the received values. The status inputs and control outputs may also be provisioned to provide a high degree of dependability or security.

Data Crosschecking

For instance, it is possible where CT reliability is of special concern, to use two independent CT cores per phase, one to the CT inputs of each of two duplicated Bricks. Alternatively, a single CT core can drive both Bricks. The elimination of long runs of CT wiring back to the control house results in virtually zero external burden on the CT, reducing voltage stress on the CT secondary, and thus increasing the already high CT reliability. This of course also decreases the CTs propensity to flux saturation. Each of the two Bricks independently samples its input CT signal, converts the samples to digital form, and sends the digital samples back to the relay over independent optical fibers.

VT inputs are handled in the same fashion, so the term AC input is used here to indicate either a CT or VT input.

At the relay, user settings control how the two streams of samples from the two AC inputs are combined into a virtual AC bank, which is used by the relay's internal functions operating on that CT/VT signal. Each AC bank has two settings that select the three-phase Brick AC inputs used for that bank. The Origin 1 setting selects the primary source for AC inputs that are to be used provided that the corresponding Brick is enabled, communications with the Brick are intact and correct, and the Brick reports no internal self-tests errors. The Origin 2 setting selects the AC inputs that are to be used when Origin 2 AC inputs are available and Origin 1 AC inputs are not available. If neither is available, the AC bank samples are forced to zero, as this corresponds to the normal failsafe state in traditional protection and control.

This simple auto-transfer scheme is illustrated in Figure 19, where the top group of traces are the samples from origin 1, the next group are from origin 2, and the bottom group are that of the AC bank. It is important to note that the AC bank is unaffected by all except the loss of both origins.

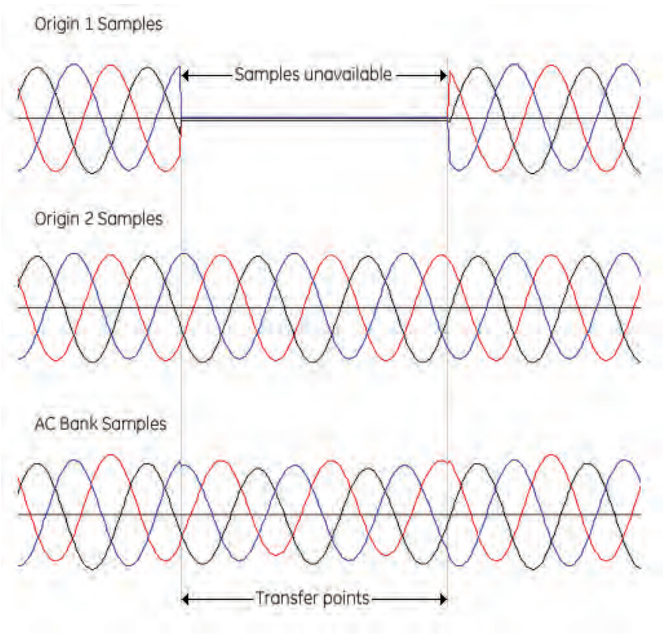


Figure 19.
Oscillography illustrating seamless auto-transfer on Brick trouble

To allow user control of the dependability/security trade-off when duplicated Bricks are provided, an AC bank crosschecking setting is available. This setting allows the user to enable comparison of the samples from the two origins, and to control the behavior of the protection elements in the event that the relay detects one of the two origins is unavailable.

When enabled, the discrepancy detection algorithm compares each sample from the two duplicated sets. If the two sets of samples are available, and are substantially different without clear declaration of a Brick self-test error, execution of the relay protection elements is suspended, as at least one set of samples is incorrect and the relay is unable to explicitly determine the valid source with which to continue operation. Note that due to the extensive self-checking, in virtually 100% of cases of HardFiber equipment failure, the relay is able to determine the invalid source, and thus can continue to operate using the other source. It is only when it is unable to determine this that operation need be suspended.

In applications where the duplicated CT inputs are from different CT cores, there is the possibility that under fault conditions the output of the two CT cores may differ to some degree due to manufacturing tolerances or unequal burdens. To prevent unwarranted discrepancy declarations, a restraint characteristic is applied under normal (i.e. load) conditions, and discrepancy checking is suspended when currents are much greater than the CT nominal rating. The discrepancy checking algorithm characteristic is illustrated in Figure 20. The feature of suspending discrepancy check is not applied for VT inputs, but for CT inputs only.

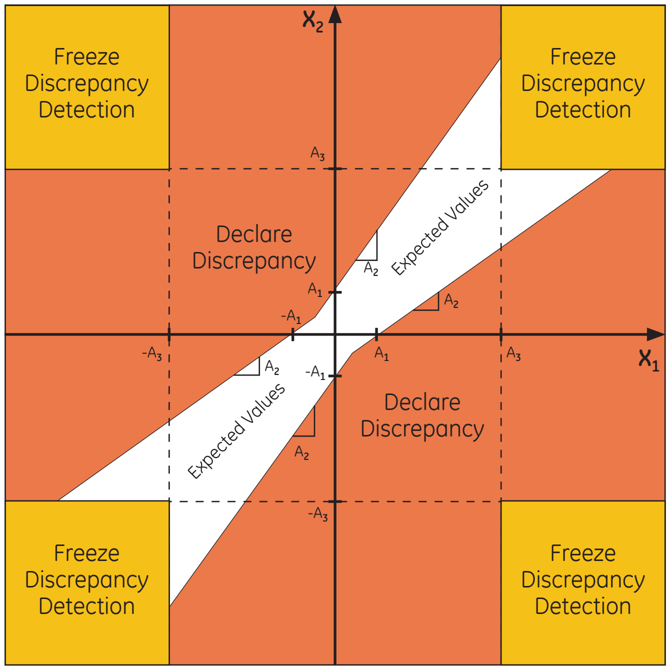


Figure 20.
X_1 and X_2 are the sample values from origin 1 and origin 2 respectively. A_1, A_2 and A_3 are parameters, values here exaggerated for clarity.

The discrepancy check algorithm can be enabled in one of two modes: Dependability Biased, or Security Biased. These differ in the reaction of the relay to the unavailability of just one of the duplicated Bricks.

In the Security Biased mode, protection will function only if both duplicate Bricks are available and both sets of samples are in agreement. The Security Biased mode is used in applications where the probability of a fault is relatively low and the system impact is very large, so it is important that protection not operate incorrectly due to AC measurement error – in other words it is justified to require two independent measurements be in agreement to operate.

In the Dependability Biased mode, discrepancy checking is only performed when sets of samples from both duplicate Bricks are available. The discrepancy check is therefore declared and protection blocked only if both Bricks are available and the sets of samples are substantially different. The clear unavailability of a single Brick (loss of communications, internal self-test failure) does not block protection. The Dependability Biased mode is used in applications where the probability of fault occurrence is higher and the system impact is lower, or in instances where a failure to trip may result in unacceptable damage to a major power system element like a generator. It is important therefore that protection is highly available – in other words it is more desirable to allow protection to continue to operate without two independent measurements.

It is also possible to use duplicated Bricks without running the discrepancy checking. By not choosing either the Dependability or Security Biased mode, the relay will use the samples from origin 1 exclusively. In the event that the origin 1 Brick becomes clearly unavailable, the relay will simply switch to using the origin 2 samples.

Origin 1 status	Origin 2 status	Discrepancy check	Crosschecking setting		
			Dependability biased	Security biased	None
Available	Available	OK	Protection available	Protection available	Protection available
Available	Available	Discrepant	Protection suspended	Protection suspended	Protection available
Unavailable	Available	Not relevant	Protection available	Protection suspended	Protection available
Available	Unavailable	Not relevant	Protection available	Protection suspended	Protection available
Unavailable	Unavailable	Not relevant	Protection suspended	Protection suspended	Protection suspended

Table 1.
Effect of dependability biased/security biased setting on duplicated Bricks

The effects of Dependability Biased verses Security Biased crosschecking modes are illustrated in Figure 21. In both graphs, the top two groups of traces are the samples from the two Bricks, the next group is the samples from the AC bank, and the bottom two traces are the pickup of an instantaneous and a timed overcurrent protection element respectively. In each graph, the origin 1 Brick samples become discrepant shortly after the start of a simulated fault.

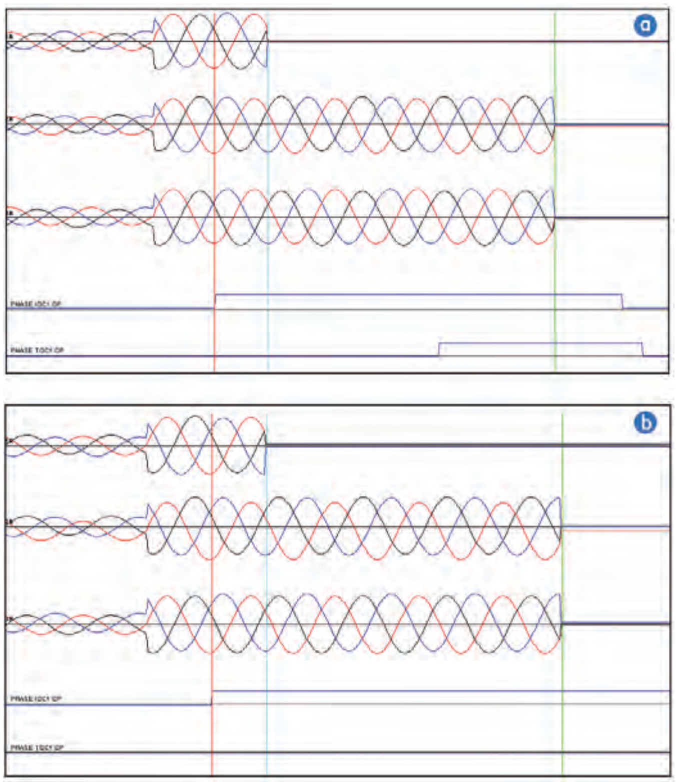


Figure 21.
Oscillography illustrating effect of (a) dependability biased vs. (b) security biased modes

The Dependability Biased mode is shown in the top graph (a), so the instantaneous protection and the timed protection picks up on the origin 1 samples, then timed protection times out on origin 2 samples; protection operation is dependable in spite of the Brick failure. The Security Biased mode was used for the bottom graph (b), so the instantaneous protection picks up as above, but then protection is suspended when the Brick fails, halting timeout of the timed protection, thus securing the protection.

Although in this particular case it is clear from the traces that the discrepancy was most likely in the origin 1 samples so the auto-transfer to origin 2 and subsequent tripping was the correct decision, in other cases the choice might not be so clear even to an experienced engineer looking at the post-mortem data, and especially difficult for a relay in a real-time operation.

Note that discrepancy checking is only done when both samples are received, and neither of the Bricks involved indicate any self-test error that calls into question the validity of its AC input data. The Brick self-tests are intended to detect internal Brick troubles that could corrupt AC input data, and so two available samples should only be found discrepant when the Bricks are otherwise functioning normally. Thus assuming failure independence, in the Dependability Biased mode, the unavailability of protection approaches the square of the unavailability of a single Brick. In the Security Biased mode, the availability of protection approaches the square of the availability of a single Brick.

Duplicate Input/Output Hardware

In addition to supporting duplication of AC inputs, the described system also supports duplicated contact inputs and outputs. As there are many different schemes to make use of duplicated contacts, user programmable logic is used.

Redundancy schemes for contact inputs include:

- OR the two contact inputs – dependable
- AND the two contact inputs – secure
- AND a form A contact input with the inverse of a form B contact input
- Main/backup contact inputs
- Instantaneous on both contact inputs closed, delayed on single contact input closed
- Last state where both contact inputs agreed
- Two of three, majority logic

Implementation logic for a main/backup scheme is shown in Figure 22. Here a main and a backup contact of a transformer gas relay are connected to main and backup Bricks. The protection (not shown) uses the main contact input provided it is available (Main Brick On), otherwise uses the backup contact. The scheme annunciates trouble should the main and backup states be available and discrepant. The alarm is delayed by 4.0ms to allow for unequal sensor contact operating times, yet still ensure alarming for discrepant operations.

Redundancy schemes for contact outputs include:

- Two output contacts in parallel - dependable
- Two output contacts in series - secure
- Four output contacts in “H” configuration – dependable and secure

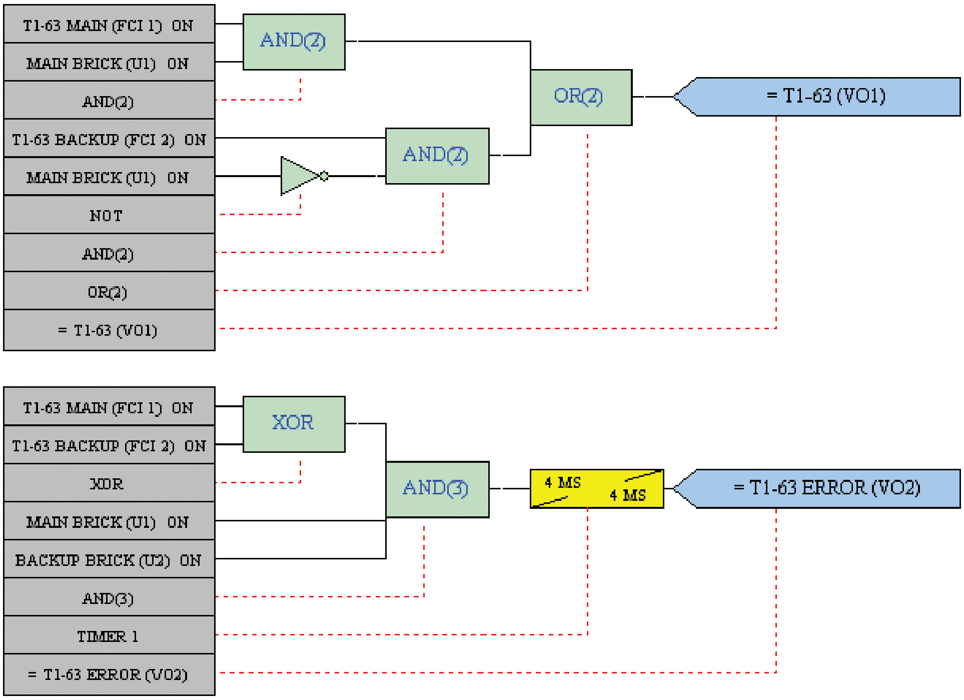


Figure 22.
Main/backup contact input redundancy scheme

One example of the H configuration is shown in Figure 23. This arrangement is dependable in that it will continue to operate should either Brick fail or any single contact output fail open. It is secure in that it will not operate should any single contact output fail short.

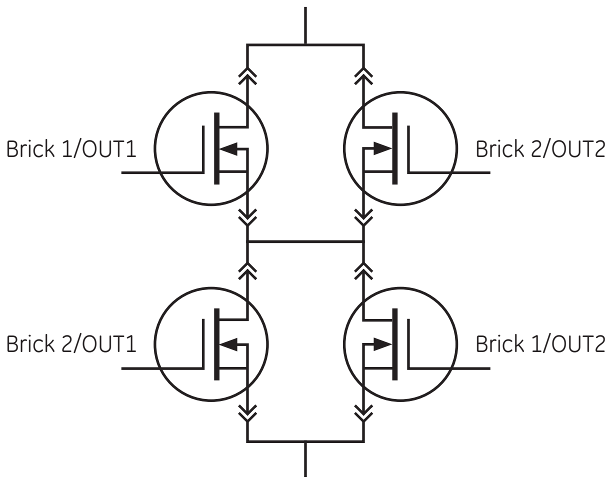


Figure 23.
Highly dependable and secure contact output scheme

6. Conclusion

This paper outlined the high-level design principles for protection and control systems. These principles are illustrated using a new practical solution for implementing ultra-critical protection and control IEC 61850 process bus applications. Several applications of these principles are explained. Moreover, the system allows eliminating significant amount of labour and therefore reduces costs and shortens the required deployment time.

A significant amount of detail is given regarding the design of this new solution as related to security and dependability. Special attention has been paid to the fail-safe aspect of the design. By relying more on digital interfaces and subsystems, the system is made more fail-safe: it either works or it stops functioning in a self-evident way, with a greatly reduced probability of a subsystem being in a faulted yet undetected state.

The system also supports the use of duplicated I/O devices for protection applications to achieve a high degree of reliability, and supports applications requirements for dependability or security improved over existing protection technology. The remote I/O devices are shared between multiple relays and therefore the solution is not cost-prohibitive compared to providing multiple independent remote I/O devices for each relay.

It can be demonstrated that the system is more reliable, dependable and secure when compared with existing solutions. The following key elements contribute to the enhancements.

- The total amount of hardware in the system is less compared with traditional solutions. This is due to the shared I/O devices. Systems with fewer components are generally more reliable.
- The I/O devices themselves incorporate a substantial amount of self-monitoring to detect internal problems.
- Duplicated I/O devices are used with constant crosschecking of input data, while supporting the use of inputs and outputs in redundant applications. The principle of duplication can be extended to instrument transformers providing for an extra layer of redundancy within each of the protection systems.
- Data is moved digitally secured with data integrity mechanisms. Digital systems are continuously monitored and will fail in predictable ways and self demonstrating ways compared with analog subsystems.

- The continuous internal self-testing, crosschecking and data integrity mechanisms will detect problems instantly allowing the field crews to rectify the problem quickly and precisely. This eliminates a considerable number of failures that may remain latent in traditional protection systems as well as failures that require a great deal of labour effort to diagnose and repair (for example DC battery grounds).

- The proposed system is easily testable and maintainable [12]. The physical provisioning of communication links using fiber patch cords provides a clear maintenance boundary that does not require relay maintenance personnel to deal with potentially lethal high-energy signals.

- The continuous monitoring of the digital communications links and the overall architecture greatly reduces the potential for human errors to result in undesired protection operations during testing and maintenance activities.

- The system is free from cyber-security concerns. The point-to-point, non-routable process bus network makes it inherently secure with no need for external monitoring mechanisms that would otherwise create extra cost and complexity and expose the system to external threats.

Also, the presented system is composed of only few highly connectorized standard devices in a modular, scalable architecture. This makes the solution very attractive from the point of view of initial installation as well as repair and/or reconstruction in the event of a catastrophic event such as a natural disaster.

The presented system allows protection relays to be made internally redundant and safe, making it very attractive in traditional as well as ultra-critical applications including nuclear power plants, and naval installations.

- 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 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.

7. 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 Process Bus System Reference Manual, GE Publication GEK-113500.

[3] Northeast Power Coordinating Council, "Bulk Power System Protection Criteria", Revised January 30, 2006

[4] FRCC System Disturbance and Underfrequency Load Shedding Event Report February 26th, 2008 at 1:09 pm Final Report Issued by: FRCC Event Analysis Team October 30, 2008 https://www.frcc.com/OC/Shared%20Documents/FEAT%20Report%20-%20Final.pdf

[5] B. Kasztenny, J. Whatley, E. A. Udren, J. Burger, D. Finney, M. Adamiak, "Unanswered Questions about IEC 61850: What needs to happen to realize the vision?" (Proceedings of the 32nd Annual Western Protective Relay Conference, Spokane, WA, October 25-27, 2005)

[6] 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).

[7] 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).

[8] Detail Specification MIL-DTL-38999L "Connectors, Electrical, Circular, Miniature, High Density, Quick Disconnect (Bayonet, Threaded, and Breech Coupling), Environment Resistant, Removable Crimp and Hermetic Solder Contacts, General Specification for", United States of America Department of Defense, 30 May 2008.

[9] "IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks—Specific requirements Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications" IEEE Std 802.3™-2005, clause "58. Physical Medium Dependent (PMD) sublayer and medium, type 100BASE-LX10 (Long Wavelength) and 100BASE-BX10 (BiDirectional Long Wavelength)"

[10] IEC International Standard "Environmental testing - Part 2: Tests. Guidance for solar radiation testing", (IEC Reference number IEC 60068-2-9:1975, IEC, Geneva, Switzerland).

[11] Test Method Standard MIL-STD-810F "Department of Defense Test Method Standard for Environmental Engineering Considerations and Laboratory Tests", United States of America Department of Defense, 1 January 2000.

[12] 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).

062609-v2

AEP Process Bus Replaces Copper

Innovations in stations translate to more savings in material, time and manpower

John F. Burger, Dale A. Krummen and Jack R. Abele
American Electric Power

A huge opportunity for material, time and manpower savings exists in the reduction or elimination of substation copper control cables. This has inspired American Electric Power's (Columbus, Ohio, U.S.) interest in the process bus technology.

AEP decided to evaluate a next-generation distributed protection and control system with all process interfaces located in the switchyard, thus taking control cabling, with its associated material and labor costs, out of the design and replacing it with fiber-optic communication.

1. At the Forefront

For decades, AEP has been at the forefront of power system protection and control technologies. In the 1970s, the utility participated in the introduction of digital relaying. In the 1980s, it took part in early research into optical instrument transformers. In the 1990s, it was an early participant of the Utility Communication Architecture (UCA) group, subsequently the UCA International Users Group, and the IEC61850 standard.

As the concept of a microprocessor-based relay matured and turned into practical products, AEP led the way with widespread adoption of the technology. Major improvements have been achieved in the areas of material cost savings, operational efficiency through remote access, control capabilities, multi-functionality, availability of data, simplification through integration of protection and control functions, and elimination of some auxiliary devices with associated panel wiring.

AEP envisions a possible future generation of protection and control systems with interface devices dispersed throughout the switchyard. The dispersed devices would provide the required input/output structure for the existing apparatus: a simple, robust standard communication architecture and interoperable intelligent electronic devices performing traditional functions, working exclusively with communication-based inputs and outputs.

AEP encouraged the vendor community to pursue this vision. In 2008, GE Digital Energy (Markham, Ontario, Canada) developed the HardFiber system, a complete and commercialized solution designed to eliminate copper control cables from the switchyard. In the second half of 2008, AEP completed the installation phase of an evaluation retrofit project with the HardFiber product.

Figure 1.
A demonstration installation at the AEP Corridor substation used the HardFiber process bus system, shown dispersed around the station, for communications interface.

2. Technology as a Brick

The HardFiber process bus system is a remote I/O architecture for protection, control, monitoring and metering that allows designing out copper wiring for protection and control signaling within substations, replacing it with standardized optical fiber-based communications. The system includes relays and fiber cross-connect panels, factory pre-terminated fiber cables and switchyard I/O interface devices known as bricks.

The bricks implement the distributed concept of an IEC61850 merging unit, expanded to optically connect relays with all types of I/O signals in the switchyard, not just instrument transformers. The bricks are interconnected to the relays in a simple point-to-point arrangement that does not involve other active components such as Ethernet switches.

Figure 2.
HardFiber protection panel with three relays and two patch panels (top and bottom). All I/O signals interfaced via fiber optic communications.

The relays are GE Universal Relay series devices. The relay's current transformer/voltage transformer and contact I/O plug-in modules are replaced with an IEC61850 process card to allow optical rather than copper signal interface. The balance of the relay hardware, firmware, functionality, configuration software, documentation and user-setting templates are unchanged.

3. Evolution of the Digital Substation

Early on in this Digital Age, American Electric Power recognized the applicability of digital technology for the protection, control and monitoring of the power system. As early as 1971, AEP began taking steps to foster this technology by funding research into digital architectures and algorithms. AEP teamed with IBM to develop and install a prototype of the world's first communicating digital relay. The device sampled voltages and currents, performed basic protection functions and communicated the resulting data and events to a mainframe at AEP headquarters.

In those early days, AEP envisioned architectures where a single digital data source could be shared by multiple protection units. As technology improved, AEP continued to track and evaluate what was available. In the mid-1980s, AEP evaluated a Delle Alsthom digital current transformer, whereby measurements made in the head of the current transformer were digitized and transmitted to ground through fiber-optic cables. The digitization was attractive, but at the time, there were no digital devices that could accept such a data stream. In addition, the concept of having active electronics at line potential was thought to be too revolutionary. In the late 1980s, companies such as ABB, Square D and 3M developed optical voltage and current measurement devices. The measurement technology was desirable, but the lack of integrated and complete solutions impaired AEP's use of the technology.

In the mid-1990s, work began on the development of a standard low-energy analog interface between measurement sources and protection, control and metering devices. During this time, AEP installed and evaluated an ABB 345-kV optical current transformer for metering. In a subsequent demonstration in 2003, AEP installed a NxtPhase 345-kV combined optical current transformer/voltage transformer and successfully integrated conventional and low-energy analog-output signals into GE and Schweitzer Engineering Laboratories protective relays and a Power Measurement revenue meter. The data from this demonstration also was used in a research project of Power Systems Engineering Research Center to evaluate the performance of a digital protection system.

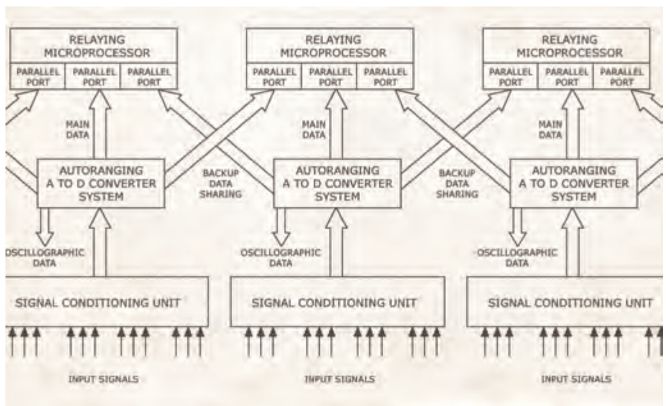


Figure 3.
AEP digital substation architecture concept, circa 1980.

Standardized communications were seen as the necessary link between the optical/electronic measurement devices and the end users of this data. AEP had played a lead role in the development of standard intelligent electronic device communications and interfaces — specifically with its support of the Utility Communications Architecture (UCA) protocol. The work with UCA provided relay-to-relay and relay-to-master communication, but did not address interfaces between measurement devices and relays.

Parallel to the development of UCA, IEC Technical Committee 57 began work on what has become known as a process bus and is now codified in the IEC61850-9-2 document. While some experimentation and implementation of process bus has taken place in conjunction with optical instrument transformers, it has not been widespread, mainly due to the lack of a consensus on the implementation approach and a solid fit-for-purpose architecture that would provide real-world benefits at low risk.

4. Demonstration Installation

The HardFiber demonstration installation is in AEP's Corridor Substation, a 345/138-kV transformer and switching station near Columbus that has been used for other new-technology trials. The HardFiber installation provides distance protection for the Conesville and Hyatt 345-kV line terminals and breaker-failure protection for breaker 302N, which connects these two lines in a breaker-and-a-half-like arrangement.

This portion of the station was considered typical and of sufficient size and diversity to demonstrate the HardFiber system technology. In addition, the lines already had existing Universal Relays installed. So the existence of these devices enabled event and oscillography records to be easily compared to those from the HardFiber system. The trip/close control outputs of the HardFiber system are not connected at this stage of the evaluation.

A site survey was conducted early in the project with the manufacturer. The survey confirmed the viability of the scope described previously, the quantity and location of the equipment, and the lengths of the required pre-terminated fiber optic cables.

Twelve bricks were necessary to provide fully redundant coverage: two bricks on each of the three circuit breakers, two on each of the two-line current-voltage transformers and two on the one free-standing current transformer in the zone. In each case, no space was found for mounting bricks inside the mechanism/marshalling boxes, so brick-mounting locations were selected either on the outside surface of the power equipment or on a supporting steel structure.

The fiber-cable routing for the 12 cables consists of a 200-ft (61-m) section in 6-inch (15-cm) duct, a section of up to 400 ft (122 m) in a pre-cast cable trench shared with conventional copper control cables, a direct-bury section of up to 150 ft (46 m) and an exposed section from grade to brick level. The factory-terminated cables required accurate cable-length measurements; a cable that was too short would have to be replaced and excess length would present slack management problems. Several length-measuring methods were tried, including use of site plans, timedomain reflectometry on existing spare conductors, a pulling tape with numbered foot markings and a measurement wheel. In the end, a surveyor's tape produced the best results. The cables were ordered with a 2% margin over the measured length.

Consistent with AEP's standard design practices, FT-style test switches were installed in the brick current-transformer circuits shared with in-service protection and the brick voltage-transformer circuits were fused.

5. On-Site Installation

Installation of the HardFiber equipment proceeded smoothly and did not reveal any obstacle to future deployments. Since the outdoor fiber cables were installed before the bricks were available, slack was left in the section between grade and the ultimate brick location. If sufficient slack was available, then a loop could be created in free space under the brick. This loop, not likely to be repeated in future installations, will increase the damage exposure in the evaluation installation, making the demonstration a more sensitive indicator of cable ruggedness. The bulk of the fiber cable slack was in the control house, where it was accommodated in an under-floor trench.

Figure 4.
HardFiber bricks installed on a bus support structure (left) and a breaker marshaling box (right).

A transcription error made in transferring the measured cable lengths to the ordering system resulted in several of the outdoor fiber being made shorter than intended, but they could still be used by relocating the relay panel within the control house. A manufacturer's engineer visited the site to correct a minor patch panel problem, but otherwise installation and commissioning was completed entirely by AEP field staff.

6. In-Service Experience

The HardFiber relays are connected to the Corridor Station local area network and thus to a station data-retrieval system, making the event records and oscillography of both the HardFiber and conventional relays available for remote access and analysis.

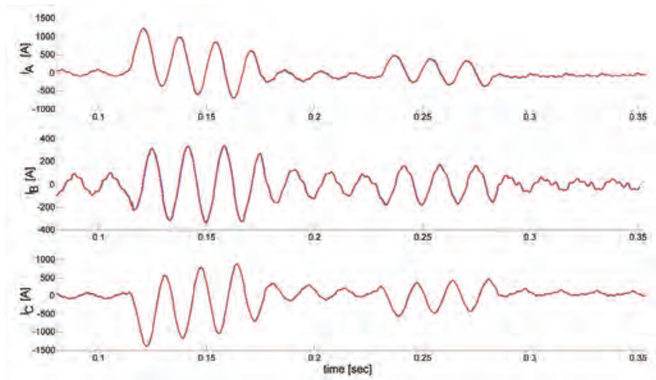


Figure 5.
On Sept. 30, 2008 event – Hyatt line currents: hardwired relay (blue) and measured by HardFiber bricks (red). The resulting pink color is due to exact overlay of traces.

The conventional and HardFiber relays are set up to cross-trigger oscillography through generic object-oriented substation event messaging over the local area network and force an oscillography record weekly in the absence of grid-generated events. Since the HardFiber systems for the Hyatt and Conesville lines were commissioned in June and December 2008, respectively, the corresponding records have been reviewed. Tens of external faults and switching events have been captured by both the traditional and HardFiber protection systems. All the records and responses of the relays are in full agreement.

The system operation meets expectations to date; not a single error or failure has been recorded. It is also worth noting that, through analysis of the HardFiber system oscillography files, a failed coupling capacitor voltage-transformer fuse was found.

7. Observations and Lessons Learned

Installation of AEP's first HardFiber system was successful and uneventful. The following factors contributed to this success:

- The HardFiber system is straightforward and practical. All obvious challenges are addressed "under the hood" and the user is not burdened with solving new problems. For example, once connected, the bricks and corresponding universal relays self-configure to establish communications.
- The system was engineered, installed and commissioned using AEP's existing workforce, procedures and tools.
- Early and continual involvement of the field personnel made the demonstration more efficient and successful.
- The manufacturer's initial site survey, field measurements and subsystem prefabrication shifted much responsibility for project success to the vendor.
- Reliance on a familiar product for the relay part of the HardFiber system made the integration easy.
- The plug-and-play nature of the system, with all components prefabricated, is an important component of next-generation protection systems.
- The factory-acceptance test, performed with the complete Corridor HardFiber system, reduced the time and effort to confidently commission the system on site.

The installation phase of the HardFiber system accomplished the early objectives of this demonstration. In particular, the system proved easy to engineer, install and commission, and is compatible with the existing workforce. Distributed I/O, process bus and replacing copper with fiber cables are seen as a stepwise evolution of traditional solutions.

Based on the evaluation project to date, the system seems to offer opportunities in shortening the construction times and labor required, standard designs for bricks, cables and panel building blocks, easier on-site integration of physical components and reduced complexity in the control building. A more formal comparison of performance and cost is planned in 2009.

The system still needs to prove, through wider field experience, the longevity of its outdoor components and overall performance. Given its simplicity and the rugged design of the bricks, it seems the required maturity is already there and any minor issues can be addressed. As a result, this fourth generation of digital protective relays, with input and output interfaces placed directly at the power apparatus, appears to provide a viable and practical option for utility engineers and designers.

Figure 6.
Before (left) and after (right) — the amount of cabling at relay panels is greatly reduced.

Continual development and commercialization of new technologies are required to address the problems of a shrinking workforce, rising costs, the volume of green field and retrofit projects, and the integration of new generation to the grid. If these technologies incorporate the latest standards, the utility industry can expect to build on the value of systems like HardFiber to arrive more quickly at functionally equivalent and interoperable multi-vendor solutions.

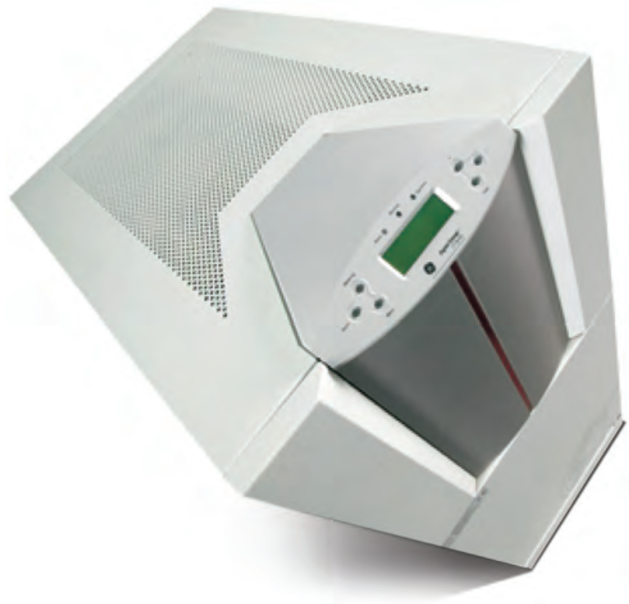
➲ *Originally published in Transmission & Distribution World Magazine, March 2009*

062909-v2

The Digital World and Electrical Power Supply
A Hypersensitive Imbalance

Raymond Kleger, BSc.
Editor of the Swiss periodical ˝Elektrotechnik˝

A complete failure of utility power is a normal occurrence. A company's power supply may be interrupted briefly or for longer periods of time because of lightning, building work, or network overloading. Electrical power supply companies (EPSCs) cannot guarantee an uninterrupted supply. Many power supply companies promise a reliability rate of 99.997%. This alone means interruptions amounting to 14 minutes a year! It is high time to think about how to survive the next power failure unharmed.



1. UPS systems yesterday and today

Faults in utility power supply cause half of all inexplicable computer problems, whether hardware damage, loss of data or complete system failure. A UPS unit eliminates the problem – but careful, they are not all of the same quality. It is only when the correct system is combined with other important measures that system administrators can keep cool in the face of lightning; self produced power spikes, long or short power failures and other electrical faults.

The nominal voltage of our utility power network is 400/230 V. Most equipment is designed to tolerate an under- or over-voltage of about 15%. Anything higher or lower than this may result in unforeseen malfunction. Light bulbs are an exception; their life span is reduced rapidly if operated with over-voltage. When operated with an under-voltage of 5% they produce only about half the amount of light. Statistics show that most power failures are shorter than 300 ms. Light bulbs flicker briefly but computer systems often suffer considerable damage because data can inexplicably be lost or changed. Such short power failures are especially detrimental to database systems.

Furthermore, it is important to know that the most frequent power problems are not long-lasting power failures but over- and under-voltage, frequency deviations, short sags, or extreme spikes. What many computer specialists don't realize is that these problems are often not caused by the EPSC that is delivering the energy but by other equipment or systems that adversely affect the power network. This paper will firstly explain the causes and effects of faults in the utility power and secondly the operation of Uninterruptible Power Supplies (UPS). The advantages and disadvantages of different UPS systems will be shown. An important topic will be that of redundant systems – because even UPS units can fail. Finally day and night maintenance needs to be looked at more carefully and here it is possible to use intelligently designed software that can monitor any UPS unit via the Internet.

Originally the use of UPS units was limited to the protection of larger computer network systems. In the last twenty years however the information technology world has undergone farreaching changes. The emergence and spread of the personal computer gave rise among critical users to a boom in the use of small single phase UPS units. During the last 20 years big computers have been replaced by efficient PC networks. At this point many UPS manufacturers became seriously concerned about the future of medium and large sized UPS units. However, this fear was unfounded. In no time it wasn't enough to have just one computer in the office. Each office worker in the firm would be equipped with a PC and almost every industrial process would be controlled by computer. Hardly any computers would be working independently as they would all be part of a network. It was quickly realized that it wasn't enough to have a UPS unit for each working station and the server. When PCs communicate over a network, files are open. If one computer has a crash the file which is open can be lost even if the power supply of the server is backed up by a UPS unit. It isn't enough to make sure that the server is provided with an uninterruptible power supply. For important work all the computers in the network must be backed up by UPS units. Of course with many PC systems a small UPS unit isn't enough. It also isn't sufficient to provide an uninterrupted power supply for each PC in the network. A computer network also comprises components such as routers and switches. These also need to be included in the UPS system because switches won't work without electricity. Incidentally, switches are also a problem because their network part only bridges minute disruptions in the utility power.

Today we can't imagine our world without computer technology. The sending of data over the internet is important everywhere where computers are being used. More and more firms do their business over the internet. E-Commerce is no longer only for the few big firms. Many smaller ones are also using this new platform, which provides the customer with extra conveniences such as downloading of information and leaflets. If a firm uses e-commerce, it mustn't upset any of its customers through computer crashes. A firm offering quick service in retail, consultation or problem solution can't afford loss of image through computer crashes.

1.1 Deregulation of the power market

It isn't long since many European countries completely deregulated their electrical power markets. The intention was to move from the cumbersome state run companies to free enterprise in the production and distribution of electrical energy. Since then, however, disillusionment has set in. These fundamental changes in the distribution of electrical energy have meant that the production of surplus energy has disappeared. There is also hardly any investment in the development of the utility power systems since that only generates cost – not profit. In spite of economic stagnation the amount of electricity used rises annually. Because of this it will be impossible to avoid bottlenecks in the coming years. Many countries have also decided to stop using nuclear energy. However, no one knows how this energy source will be replaced.

In the year 2003 New York experienced a total power failure lasting several hours. The cost of this blackout was estimated at over a billion dollars. The loss of perishable foods alone amounted to 250 million dollars. The blackout in Italy wasn't any less dramatic! How did it happen? On that unfortunate day Italy, the biggest importer of electricity in Europe, had to import 750 MW more electricity than it had foreseen. France was the supplier. The electricity was delivered through the Swiss mountains because there the resistance was lower. The high voltage transmission lines were so overloaded that the heat caused the cables to stretch. They sagged deeper and deeper until they discharged onto a tree thus causing the immediate automatic shutdown of the line. It wasn't possible to reconnect because the Italian power system was now in disarray (acute phase displacement). All the power was now automatically transferred to the remaining high voltage transmission line leading to Italy.

However here too due to the overheating there was a disruptive discharge on to a tree leading to the shutdown of that line. After the first breakdown the Italians should have immediately shut down all the pumps of their hydroelectric power stations. Because this didn't happen a chain reaction was unavoidable. The Italian power stations weren't able to meet the demand and so there was a complete breakdown in the power supply. A power system that has completely collapsed isn't so easy to resurrect and so it took many hours until the whole of Italy was again supplied with power.

Why this detailed account? When the deregulation of the electricity market began many years ago the EPSCs didn't really show any interest in redundancy, that is investment in extra capacities of production and infrastructure. However, power consumption has increased during the recent years of economic stagnation. Aside from this it takes years or even decades to obtain permission for new power stations and high-tension power lines. All these factors will lead to the quality of electrical energy supply deteriorating in the coming years. America has already sunk to the level of third world countries in terms of reliability of electrical supply. Experts had long been convinced of this and a study made by the government a short time ago confirmed this situation. In the coming years Europe will also inevitably have bottlenecks and hence more frequent electricity cuts.

The expectation of cheaper energy through deregulation was made attractive to voters and it was cheaper at first. Since then, however, the trend has clearly changed. The most striking example is Sweden where power prices have doubled. In Germany prices have risen by 9.6% per year following deregulation. New firms requiring a lot of power to operate are now unable to set up business in Amsterdam because the EPCS is unable to increase its supply of power. It's a crazy situation when the job opportunities that everyone is demanding are already out of the question because of the power situation. In recent years in China there has been amazing economic growth of almost 10%. There have been power bottlenecks in 24 of the 31 provinces. However China has the advantage of being able to build, at short notice, power stations using fossil fuel. If the demand for power in Europe continues to rise at the present rate over the next 15 years, power stations with a total capacity of nearly 300 GW will have to be built. That would mean building a hundred large nuclear power stations. We should also not forget that some old power stations will have to be closed down. In Germany and other European countries it is practically impossible to get permission even for hydroelectric power stations. Environmental and other organizations campaign against every possible development of the electrical industry.

Figure 1.
Lightning is a frequent cause of computer crashes.

1.2 Attacks from heaven

Lightning is a beautiful natural phenomenon– at least for those of us who aren't afraid of it (Figure 1). In a powerful storm, lightning strikes with half the speed of light and heats the air up to 20,000°C. This heat is four times greater than that on the surface of the sun. The frightening noise – the thunder– is caused by the explosive expansion of the air around the arc. Lightning is a major threat to much modern electrical equipment. Only private people, if they happen to be at home, can pull the plugs out at the first signs of the approaching storm and sit back to enjoy the spectacle. Employees at work should, with clear consciences, be able to work on during the storm. Quite apart from that why should an Italian businessman be affected by a storm in Germany when he is just in the middle of e-commerce business? Meteorologists count approximately 750,000 occurrences of lightning a year in Germany, most of which occur in the months of July and August. This sort of natural phenomenon causes enormous financial loss. UPS units may help to avoid damage generally but not that caused by lightning. For this, lightning and surge protection must be included in the electrical installation. This needs to be done for both the power supply of the UPS and any cables transmitting data to the outside world. Finally there must be good potential (voltage) equalisation in the building combined with an effective lightning trap around the building (Figure 2).

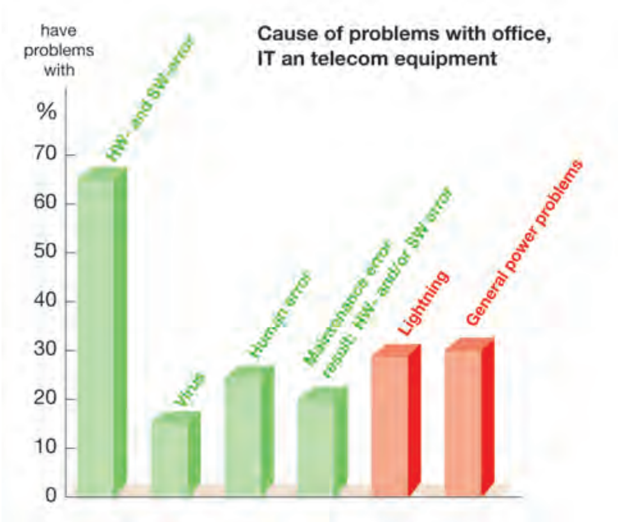


Figure 2.
Causes of problems with computers and other equipment in offices and industry.

1.3 Industry – without electricity nothing works

In order to remain competitive, firms in all western industrial countries must computerise their manufacturing processes. The level of automation has constantly increased and become more efficient. PLC and PC systems are increasingly the order of the day. Industry is of course dependant on a top quality power supply. Critical processes are therefore dependant on a UPS because even the shortest power cut can have fatal effects on the process. There will be rejects and the machine will possibly be damaged if half-finished products get stuck in it. The more sophisticated the automation the more the process depends on an uninterrupted supply of electricity. Complicated networks used to control lighting, blinds, air conditioning, and entry and security systems in buildings also all depend on a continuous supply of electricity. Here too centralised UPS systems which keep at least the essential processes going are increasingly being used.

1.4 The consequences of a computer crash

It is surprising to see how careless even large firms are in securing a reliable supply of utility power. They should know how much the success of a company is dependant upon it. A power failure of only some few minutes may have fatal consequences such as:

- Loss of image
- Loss of contracts
- Loss of a customer
- Breakdown of customer service
- Backlog in production
- Loss of operational data

Very important! No insurance covers loss of image or loss of contracts. Also don't forget the loss of working hours caused by a crash of the communication system. Companies asked indicated costs of 13000 € per hour in the case of system failures and the figure is even higher in the service sector. Many firms who have experienced a serious computer failure complained of months of increased economical difficulties.

1.5 To sum up

Before the deregulation of the electricity market, experts warned of difficult times ahead in terms of availability and quality of electrical energy. Their predictions have proved correct here in Europe more quickly than we would have liked. The requirements of the digital world have increased dramatically in the last two decades with regard to the availability and quality of electrical energy. There is a growing imbalance between the need for stable electrical energy and the situation as we have it on the energy market. A disquieting prospect – not for the manufacturers of UPS units though! They can reckon on a growing demand for their products.

2. UPS technology –separating the wheat from the chaff

There is a wide variety of UPS system architecture. There are simple systems which are capable of providing power until the computer network has been shut down. There are more costly systems which offer a complete galvanic separation from the utility power supply and guarantee that 'spikes' never get through to the computer network and its components. For installations where power interruptions even of milliseconds must never occur – even if the UPS unit breaks down – redundant systems are important. This chapter looks at UPS technology more closely.

2.1 Typical problems in the utility power network

Problems are not only caused by power failures. Short interruptions that do not even cause a light bulb to flicker can have treacherous consequences for different sorts of equipment. In computers, network components and telecommunication systems, overvoltage can cause the electronics to become defective. Hidden effects are the most treacherous. In such cases a sensitive electronic device still functions but its power consumption rises, leading to overheating of the element and finally to failure. Figure 3 shows the typical problems in utility power.

Low voltage (brown out)

Approximately 60% of the disruptions. This is the most frequent problem and is usually caused by large consumers of electrical power, not by the user or the supplier.

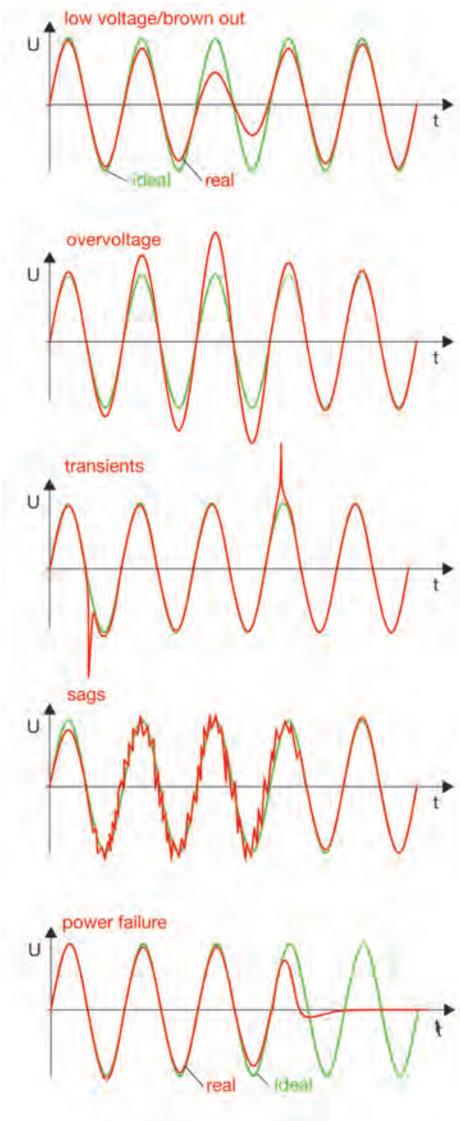


Figure 3.
Frequent faults in the utility power.

Over-voltage

Approximately 20% of the disruptions. It stems from switching operations performed by large consumers and can lead to hardware failure.

Transients

Approximately 8% of the disruptions. Transients (spikes) are extremely short occurrences of over-voltage. They can be several times higher than the rated voltage and get through the power supply units to the equipment, causing faulty transmission of data or leading to hardware failure.

Sags

These considerably distort the ideal sine waves of the utility power. The consequences can be 'inexplicable' system failures or faulty transmission of data. These problems are caused by pieces of equipment that do not draw a cleanly sinusoidal current (light controllers with phase shifting control or utility power command guiding systems).

Power failure

It is common to distinguish between those failures lasting milliseconds and those lasting minutes or hours. The latter are much less frequent in Northern Europe than the former. Every UPS system must be able to cope with both types of power failure.

2.2 What types of UPS are there and how do they function?

What does a user expect of a UPS? It must:

- Bridge power failures for minutes and even hours.
- Protect from over- and under-voltage.
- Keep transients in the utility power from reaching the load.
- Provide failure-free and stable voltage for any kind of load.
- Provide careful recharging of batteries and protection from low discharge.

An important characteristic of a UPS is the signal form it produces. The power plant delivers a pure sine voltage with an effective mean value of 220–230 V and 50 Hz in Europe. America and other countries have 110–120 V and 60 Hz. The operation of simple loads, for example a light bulb, depends only on the mean value and the resulting power. But modern switching power supplies for computers are more demanding and require a much closer approximation to a pure sine voltage. Simple inverters deliver a square wave voltage with peak and mean values that are identical. This can cause a power supply unit to malfunction. An acceptable approximation is a trapezium where the peak and mean values correspond approximately to a sinusoid. The ideal is of course that a real sinusoidal voltage is generated, which is what high quality UPS do.

2.3 Off-line mode

This is also called standby mode (Figure 4). This is the simplest type of UPS. It has two paths for the current. The concept of off-line technology is that when the UPS has utility power, the load is directly supplied with utility power voltage. The inverter remains in standby mode stepping into operation only when there is a power failure.

During normal operation (utility power voltage present) this type of equipment does not provide voltage regulation. The consequence of this is that in the case of fluctuation, the UPS must switch into battery operation in order to compensate for the fluctuation. This simple type of UPS is useful for single workplaces especially in private usage, but it should not be used to supply telecommunication equipment, network components or even server systems. The autonomy time ranges from 3 to 10 minutes, and the power range goes up to approximately 3 kVA.

Advantages:

- Reasonable in price.
- High degree of efficiency.

Disadvantages:

- No suppression of non-sinusoidal injection back into the utility power.

- Short voltage fluctuations have no problem getting through to the load.
- Switching to inverter mode takes several milliseconds.
- Low-cost equipment does not provide sine form voltage when in inverter mode.

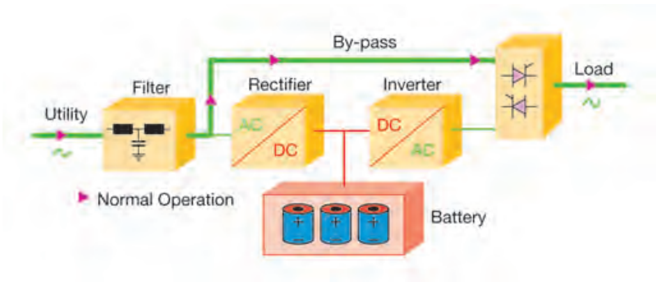


Figure 4.
UPS with off-line or standby mode.

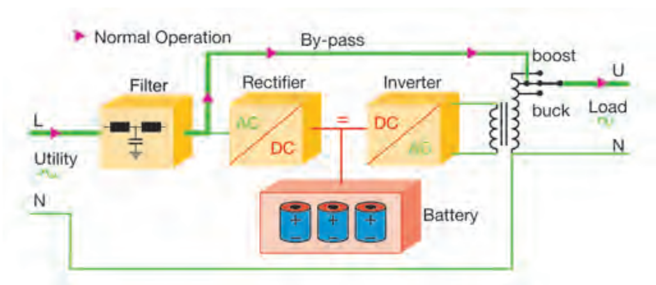


Figure 5.
UPS with active-standby or line interactive mode.

2.4 Active standby mode

Also called line-interactive (Figure 5). This is a refinement and improvement of the off-line mode (see above). During normal operation, the load is supplied directly with utility power voltage from an auto transformer at the output of the UPS. In many countries, the utility power fluctuates considerably depending on the load. The power supply units of computers and also other power supply equipment cannot take a fluctuation of more than±15%. Active standby technology functions in such a way that a switching device at the level of the auto transformer can make the voltage increase or decrease depending on what is needed. If the supply voltage is too low, the switch turns into 'boost' mode, if the voltage is too high, it switches to 'buck' mode. This correction of the utility power voltage is not very finely tuned and thus – as will easily be understood – not particularly effective. But it has the advantage that the inverter does not need to step into UPS mode with every slight fluctuation of the utility power voltage, thus conserving the batteries.

In the case of a power failure, the switch changes the UPS to inverter mode operation. Then the load is completely supplied by the battery. This technology is often used for small networks and equipment that is not too sensitive. Certain loads, however, do not tolerate the switching time (reaction time) of this type of UPS unit. The autonomy time lies between 6 and 10 minutes, the power range reaches up to 3 kVA.

Advantages:

- The batteries are spared because the UPS does not switch into battery mode until the voltage goes beyond over- or under-voltage.

Disadvantages:

- Switching into inverter mode operation takes several milliseconds.
- Faulty frequencies can only be eliminated in battery mode.
- Low-cost equipment does not provide sinusoidal voltage in inverter mode operation.

2.5 Double conversion technology

This type of UPS has two elements (Figure 6). On the input side, the alternating current is rectified to direct current, which in turn charges the battery. An inverter which is on the output side of the UPS uses this direct current to produce an alternating current with the frequency of 50 or 60 Hz (depending on the user's network). The inverter permanently produces the alternating current. Filters at both input and output end successfully eliminate practically all faults coming from the utility power. Single phase equipment is available up to 10 kVA, three phase equipment up to 1000 kVA. Higher power can be achieved by connecting several UPS units in parallel.

Advantages:

- Steady sinusoidal voltage and frequency at the output.
- A secure protection from over-voltage because of the continuous conversion.
- No substantial switching delay in the case of a power failure. This is very important if sensitive equipment is being used in the area of network and telecommunication technology.
- Well defined and constant conditions throughout the network.

Disadvantages:

- The degree of efficiency of the whole system is low.
- The technology is more complex and therefore more expensive.

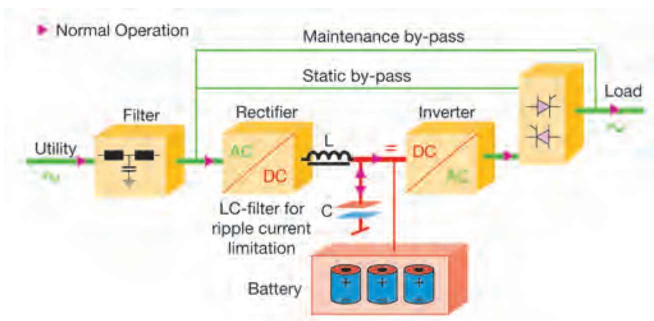


Figure 6.
UPS with VFI or double conversion technology.

2.6 Is a complete galvanic separation necessary?

Online and double-conversion technology can be divided up in another way, namely into UPS units with or without galvanic separation. Many users repeatedly ask themselves which technology is the best for their application. Figure 6 shows double conversion technology. The inverter is available with or without galvanic separation. Both types have their advantages and disadvantages.

2.7 With galvanic separation

IGBT (Insulated-Gate Bipolar Transistor) transistors generate direct current impulses from the battery voltage (Figure 7). One complete sine wave (one full period) is comprised of about 500 individual direct current impulses. Assuming that the output frequency is 50 Hz (duration of one period = 20 ms), it follows that the inverter frequency is 25 kHz.

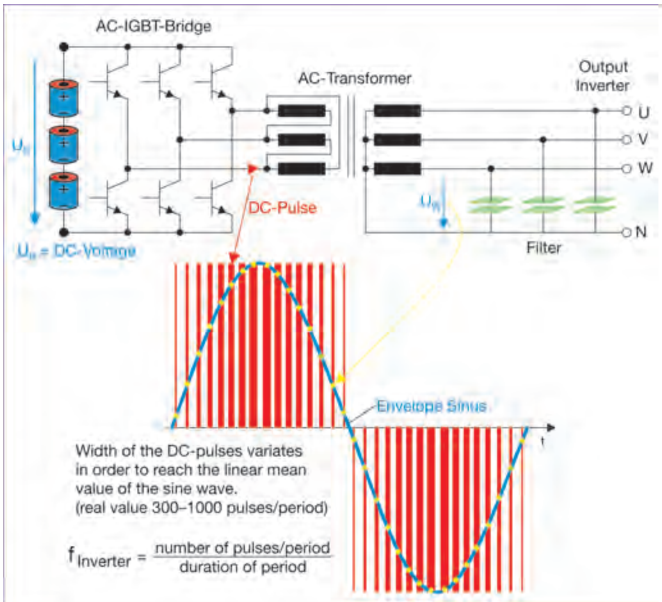


Figure 7.
UPS with double conversion and transformer in the inverter.

The width of the direct current impulses varies in such a way that the linear mean value of the envelope corresponds to a sinusoid. This sinusoidal envelope comes from the filtering in the secondary winding in the transformer in combination with the capacitor at the UPS output.

The higher the inverter frequency, the smaller is the physical size of the transformer. If the power stays the same, the size of the transformer diminishes almost in proportion to the frequency. The difficulty consists in finding materials for the core of the transformer which operate with minimal loss due to magnetic hysteresis and eddy currents. Laminated iron cores are problematic above 5 kHz. Ferrite cores are much better but also much more expensive.

Furthermore the capacity of the filtering capacitors at the output end of the UPS drops with higher frequencies. But a high frequency of operation results in better dynamic characteristics of the inverter. The narrower the direct current impulses, the quicker the reaction of the inverter to load jumps. Power supply units of computers, networks, telecommunication equipment and other electronic equipment draw a non-sinusoidal current. In simple inverters the consequence of this is that the curve deteriorates to a trapezoid.

IGBT transistors have the disadvantage of considerable energy loss when operated at high inverter frequencies. In recent years, the frequency has been increased due to the higher quality of IGBT transistors. Power-MOSFET transistors are used for small power applications. The UPS manufacturer optimises the inverter according to technology and cost. In the area of high power applications it is possible to work with frequencies around 12 kHz nowadays, and in systems up to 1 kVA with up to 30 kHz. The critical aspect of this optimization is that the IGBT transistors must be operated in such a way that they reach a high degree of efficiency on the one hand and maintain a sinusoidal output (despite the non-linear load) on the other. A special quality characteristic of an inverter is its capacity to react to load jumps quickly. Another advantage of high inverter frequency is the fact that frequencies over 15 kHz are practically inaudible for the human ear.

Advantages of the transformer technology:

- The load is isolated from the utility power.
- No direct current in the load.
- Good dynamic characteristics even when non-linear load is connected.
- Good short circuit performance.
- Only one battery voltage needed, the level of which can vary greatly.
- Power capacity up to 1 MVA possible.
- The static bypass can be directly mounted thanks to galvanic separation.
- Fewer components needed.

Disadvantages:

- The transformer is fairly large and heavy.
- Expensive in comparison to a design without a transformer.
- Especially in the low power range the energy loss is high when compared to a design without transformer.
- The realization of Power Factor Correction (PFC, the current which the rectifier draws at the input is sinusoidal) in the rectifier is more difficult than with the solution without the transformer.

2.8 Without galvanic separation

This approach requires the use of two sets of batteries because a double supply of direct current is needed (Figure 8). Single phase technology used this approach in the early nineties. The positive half-sine wave at the output is produced by the upper three transistors for all three phases. This is achieved in the same way as in a design with a transformer. The half-sine wave is comprised of direct current impulses of variable width.

It is clear that there is no galvanic separation between input and output. The negative side to this is that the output can be ‘contaminated’ with a direct current component. This component is caused by the fact that the linear mean value of the positive halfsine wave is different to that of the negative half-sine wave. It is very difficult to rectify this problem and consequently there is always a possibility of a direct current component at the output. This will not harm switched power supply units of computers, networks or telecommunication equipment, but it will harm supply units of toroidal transformers and AC motors. In this design the inverter frequency is higher than in the one with a transformer, lying between 15 and 30 kHz, because it only requires filter chokes.

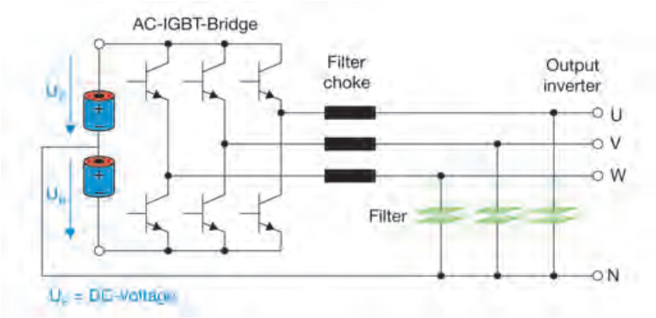


Figure 8.
UPS with double conversion and without transformer in the inverter.

Advantages of the technology without a transformer:

- Smaller in size
- Less expensive
- Higher degree of efficiency
- Less noisy

Disadvantages:

- No separation of the load from the power supply.
- Direct current component at output.
- If badly regulated, the neutral output line can carry a high current.
- Twice the number of boosters and batteries are needed.
- Limited to units up to 120 kVA.

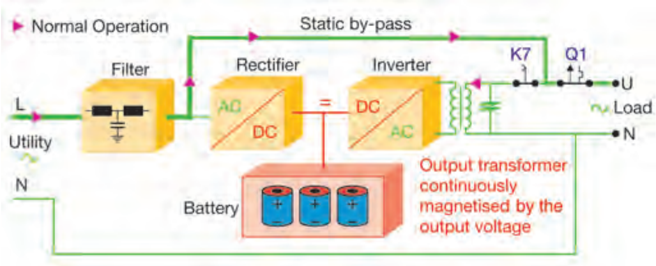


Figure 9.
Output transformer magnetised by the output voltage, efficiency of 98%, switchover time only 2 ms patented by GE (Super Eco Mode).

2.9 Which technology is better?

It is pointless to ask this question because both technologies have their advantages and disadvantages. One or the other solution is more appropriate depending on the requirements. This is why leading UPS manufacturers build units with or without galvanic separation in order to meet the varying requirements of customers. However, the customer should make sure he knows which design is being offered to him.

When to use the transformer technology?

- When the load has to be separated from the utility power supply and the battery.
- When the load is sensitive to direct current.
- When the dynamic characteristics of the UPS have to be very good (also in case of high load jumps and short-circuit behavior).
- When the application does not allow high currents on the neutral output line.

When to use a unit without a transformer?

- When the efficiency of the unit is important.
- When the price plays an important role.
- When the level of noise needs to be as low as possible (inverter frequency inaudible to the human ear).
- When galvanic separation is not mandatory.
- When the load is not sensitive to direct current.

2.10 Super Eco Mode

As mentioned previously, UPS units operating according to the off-line system are the most efficient because the utility power is normally led directly to the output via a static by-pass. The U I current on the silicon-controlled rectifier and the energy needed to sustain the charge of the battery are the only losses. The disadvantages of this system were given previously.

UPS units with transformers are naturally less efficient. The transformer alone absorbs approximately 3% of the power at full load and 1% at zero load. For safety reasons, however, UPS with transformers continue to be in use. The pros and cons are provided above.

In many countries in Northern Europe the tension and frequency of the utility power is remarkably stable. Hence it is obvious that the off-line system is the ideal UPS from various points of view. Unfortunately, however, this system does not satisfy the highest requirements regarding safety and stability. For very sensitive loads which do not tolerate direct current at all, users may have to resort to UPS with an output transformer. But such a unit cannot switch instantly from the 'dormant' mode of operation to the active one. The problem is the transformer, not the inverter. Even if the inverter can supply the output transformer instantly with the required tension, the load will not receive it instantly. The transformer has inductivity and this delays instant transmission. The delay mounts quickly to 20ms and in addition to that surges of tension are to be expected.

GE's research division has provided a solution with the Super ECO mode (patent pending). In this system the load current flows in the ECO mode via a bypass as with the off-line system (Figure 9), but of course only as long as the tension and frequency of the utility power lie within specified limits. The innovation is that the output transformer of the UPS is being 'kept primed' all the time by the load, i.e. kept magnetized. The benefits are as follows:

- If there is a power failure there is merely a drop in tension at the output, lasting less than 2 ms. There is no complete loss of tension.

- The output transformer and the filtering capacitors of the UPS act in the ECO mode as passive filters and thus improve the load parameters with regard to the utility.
- The inverter is turned off and the rectifier turned on occasionally in order to charge the battery.
- The user is sure that even with the worst case scenario of the UPS there will never be any direct current on the output side, since the unit has an output transformer.
- The efficiency of the unit is around 98% (the additional loss of 1% in comparison with the simple off-line system stems from the energy used for the permanent magnetization of the transformer)

2.11 DSP technology

Analogue technology is nowadays used by well-known UPS manufacturers for the generation of the signal. The processing of the signal, as well as the controlling of the transistors of the rectifier and the inverter, is achieved through a DSP (Digital Signal Processor). DSP technology drastically reduces the number of parts needed since it measures the tension of the three phases as well as the current directly and calculates the width of the impulses of the direct current by way of a complex algorithm transmitted to the IGTB transistors. In this way the reliability of the electronic system is improved, i.e. the MTBF (Mean Time Between Failure). DSP is nowadays so efficient that at GE, for example, the total control of a UPS system is reduced to one single print-out and this print can be used for systems from 10 to 500 kVA. DSP also makes the application of a new technology for UPS possible, the so-called Space Vector Modulation (SVM). This technology makes it possible for only minute drops or rises in tension to occur when the load changes. DSP generates three sinusoid tensions as well as the modulated impulses for the three phases, taking into account the current required by the load in order to control the IGBT transistors. DSP and SVM greatly improve the performance of the UPS, also in the most demanding case of redundant and parallel circuiting of several installations.

2.12 The myth of a high degree of power efficiency

A high degree of power efficiency is often used as a sales argument. A UPS in off-line mode, operating normally and directing the current from the utility power supply directly to the 'protected' load, obviously has the best power efficiency of approximately 98%. For line-interactive units the figure is 97%. For UPS in online mode the efficiency is 89–96% depending on the size of the unit, this being the real online-degree of efficiency. In systems with transformers the efficiency can reach a maximum of 95%, in those without 96%. The brochures of UPS manufacturers always indicate the highest degree of efficiency. However, the efficiency is dependent on the utilisation of the unit, the power factor of the load, and the input voltage. For example, a UPS unit using the so-called Delta Technology (not explained in this article) has a definitely lower efficiency with non-linear loads, i.e. in the case of poor power factors.

The decision to purchase a certain model must be well thought out because the protection of the equipment connected to the UPS must be given highest priority. The question therefore is: is it worth taking a higher risk in order to save expenditure on energy? The money saved by buying a cheaper unit and saving energy never justifies the risk of damaging, for example, a sensitive server system. Just one single unnecessary shutdown per year (together with the resulting costs) exceeds any saving in energy costs.

To illustrate this, take the example of a large network with approximately 200 computers, including the monitors, printers and other network components, all of which are dependant on a UPS for their energy supply. Let's assume that the network is used for 12 hours per day. For this network a UPS supplying 100 kVA is necessary. At full utilisation and assuming 3% less degree in efficiency there is an additional loss of power of 3 kW. Assuming further that these 3 kW are lost for 12 hours during 365 days per year – which is unrealistically high – the additional cost of energy amounts to 1000 €, if one kWh costs 0.10 €. This then would be the amount saved by choosing a system with a lower level of protection. It would never cover the cost of rebooting a network of 200 computers after a crash. One aren't think of the cost of the time needed to reboot it.

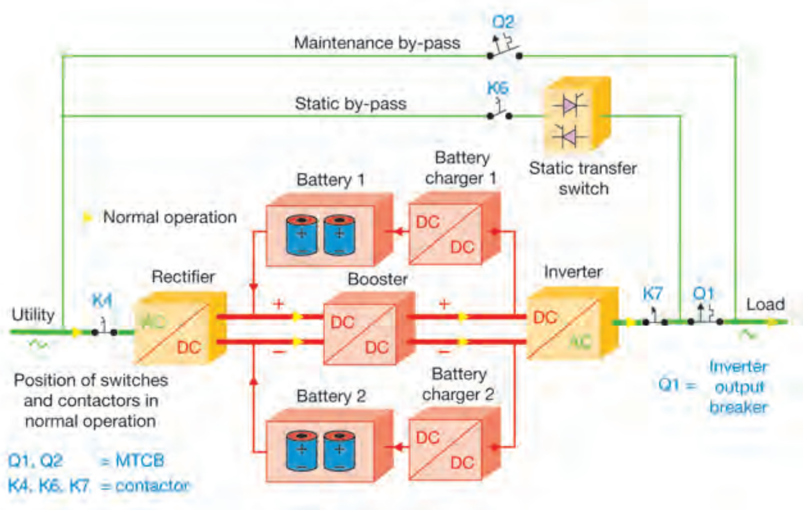


Figure 10.
Schematic diagram of LP 33 Series, trimmed for high degree of protection and highest degree of effectiveness.

2.13 GE's LP and SG Series units – examples of the most up-to-date technology

Taking the example of these ultramodern units, both designed for a power range of 80–100 kVA, let us examine the differences in the realm of technology. The following data is given for a 120 kVA system. Figure 10 shows the schematic diagram of the LP Series Model which incorporates the feature of galvanic separation. Both models satisfy the highest level of UPS standards. They are VFI units, i.e. units operating in online mode. Both can be switched to redundant parallel function by means of RPA (see below) and both are equipped with the Super ECO mode. The LP Series model, however, is a unit without transformer. The SG Series model has a transformer.

The first difference is a purely external one: the LP Series requires 0.52 m2 ground surface, the SG Series almost double – 0.96 m2 – which still makes it one of the most compact units on the market. The difference in size is somewhat balanced out when we take into account the number of batteries needed. The LP Series needs forty 12 Volt units, the SG Series needs only thirty.

The values of the output tension are almost identical. Both units overcome a load jump of 100% with less than 2% fluctuation of the tension. Both have a total harmonic distortion of less than 3% with 100% non-linear load. There is a small difference in the efficiency of the units: the LP Series reaches 93% in VFI mode and 99% in ECO mode, the SG Series unit reaches 92–98%. This small difference is the price paid for galvanic separation.

At a first glance the two models are similar, both fulfilling the standard range of expectations (Figure 11). Why then does GE offer two models? Just as big car producers offer different ranges of power and comfort, GE has produced two models for the important power range up to 120 kVA. One can view the LP Series model as the open sports car, and the SG Series as the luxury four-door four wheel drive. With the LP Series unit you can add up to four elements in parallel redundant setting – with the SG Series (thanks to SVM) you can add up to eight. Furthermore the SG Series is equipped with a whole range of additional conveniences and safety devices, e.g. redundancy ventilator, optimized soft start, greater capacity of the batteries and a convenient control panel.

Figure 11.
LP Series on the right – an ultra-modern UPS without transformer, SG Series on the left – units with transformers using very little floor space, 120 kVA each.

3. Assess your partner firm – avoid being left in the lurch

The need for upgradable UPS systems with highest fail-safe record has increased enormously. Computing centres of internet providers, banks, telecommunication companies and all those using large computer networks demand a high degree of availability. Many customers are now less cost conscious when it comes to power supplies. Yet some firms still entrust their complex server systems to a low-cost UPS. Upgradeability, that is the possibility of adding power and autonomous time, is more and more in demand. On the UPS market GE offers a unique failure-tolerance of N+1 redundancy.

3.1 What is a redundant system?

Important business activities and hightech control systems require an uninterrupted power supply. The installation of a UPS unit makes this possible. Such a unit is made up of electronic components, batteries and mechanical parts, all of which can break down. Hence it is clear that you cannot depend on a single UPS unit only when supplying computing centres or other important systems with electrical power.

A redundant system can cope with the failure of one of its parts without normal operation being impeded. An example will help to explain this. An aeroplane used for the transport of passengers has at least two engines. If one of the two fails to operate, the aeroplane must nevertheless be able to fly on to the next airport and land there. In an N+x redundancy, the N stands for the number of units operating in parallel. X stands for the number of units that can fail to operate without affecting the operability of the entire system. In our example we have an N+ 1 redundancy. In the case of a plane that has three engines it can lose two and still continue its flight; here we would talk about an N+2 redundancy.

However, this does not mean that the aeroplane with three engines necessarily has an N+2 redundancy. If there is one element in the plane upon which all three engines depend then this plane does not have redundancy at all! Here is the problem with most of the global UPS manufacturers. Individual UPS units in parallel may provide redundancy – or may not, depending on whether there is an additional component in the system upon which all the UPS depend. There must not be the possibility of a single point of failure in the system. Because of the importance of this point, several concepts of parallel architecture will be presented, highlighting their advantages and disadvantages.

3.2 Hot-standby systems

Here, as figure 12 shows, two UPS units are connected in series. In normal operation, unit 2 takes over the supply of the critical load. If unit 2 fails to operate, it switches to bypass mode and after 2–8 ms unit 1 automatically takes over the supply of the load.

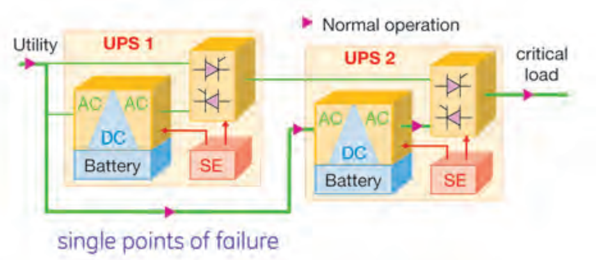


Figure 12.
Cascaded UPS system.

Advantages:

- Reasonable in price since no additional components are necessary.

Disadvantages:

- There are many single points of failure.

- There is no distribution of the load. If one UPS fails then the other one has to take on the whole load. This means that it must be able to cope with an increase of power supply from 0–100% within approximately 8 ms.
- Overload is limited to the capacity of one single unit.
- The MTBF of the whole system is lower than the MTBF of a single unit.
- The loss of energy is relatively high because one unit is only 'idling along'.

3.3 Parallel system with automatic switching mechanism

This architecture operates with two or more UPS units as well as an automatic transfer switch (STS static transfer switch). The sensor in the STS monitors the output voltage of each unit and immediately switches to a different UPS (or several) as soon as a failure is registered. Figure 13 shows that the system is not redundant because of the STS. If this component fails then the UPS are of no use.

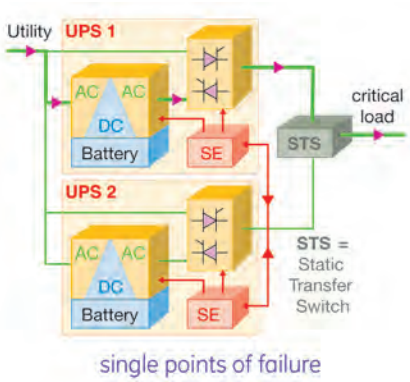


Figure 13.
Parallel system with automatic switch (STS).

Advantages:

- When one UPS fails to operate, a different one can take on the load.

Disadvantages:

- There is no distribution of the load.
- Additional expenses: an STS costs roughly what a UPS unit without batteries costs.
- Additional loss of 1% of the energy.
- If the STS fails then the whole system collapses (a single point of failure). The UPS units which actually still work are of no use.

3.4 Parallel system with external switching mechanism

UPS normally have an internal switch to change from inverter mode to bypass mode. Some manufacturers situate this switch externally for manual operation in order to facilitate the use 11 of several UPS units in parallel (Figure 14). The advantage of this configuration is that there is a distribution of the load and losses are minimal due to the fact that the load current does not run through two switches. Yet it is also clear that the external switch is the critical element in this configuration. If it fails, there is no redundancy. This configuration is comparable to a jet plane with a central hydraulic system. With regard to the UPS units that are aligned in parallel, the system is redundant, but not with regard to the central external switch.

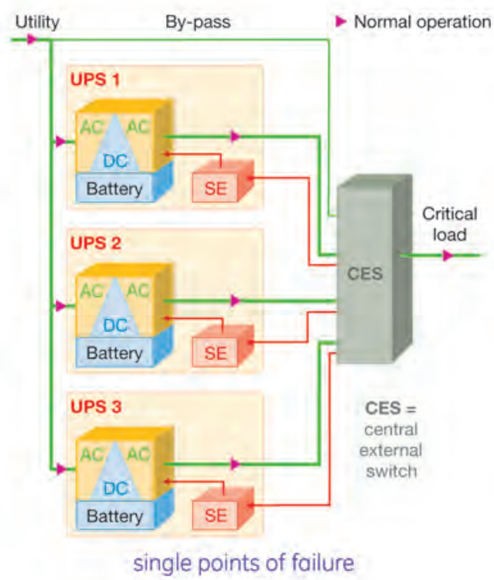


Figure 14.
Parallel system with with external switch.

Advantages:

- When one UPS unit fails to operate, a different one takes on its load.
- There is a distribution of the load.

Disadvantages:

- If the external switch (ES) fails (a single point of failure) then the whole system fails. The UPS units which actually still work are of no use.

3.5 Parallel architecture with master and slave

In this configuration, one UPS (or special circuitry) takes on the role of the Master and the other units take on the role of Slaves. The Master is responsible for the load to be evenly distributed among the UPS which are aligned in parallel. If one of the UPS units fails to operate the Master automatically redistributes the load to the other Slave UPS. It is clear from figure 15 that this configuration also has its weak points. If the Master UPS fails to operate, then it switches into bypass mode, but if the circuitry that controls the Master unit fails, then the whole set-up is without a Master and therefore no longer controlled. This configuration has at least two single points of failure.

Advantages:

- No casing with an external switch necessary.

Disadvantages:

- If the circuitry that controls the Master UPS fails, the whole configuration is out of control.
- The data bus is not redundant. If it fails, the whole system collapses.

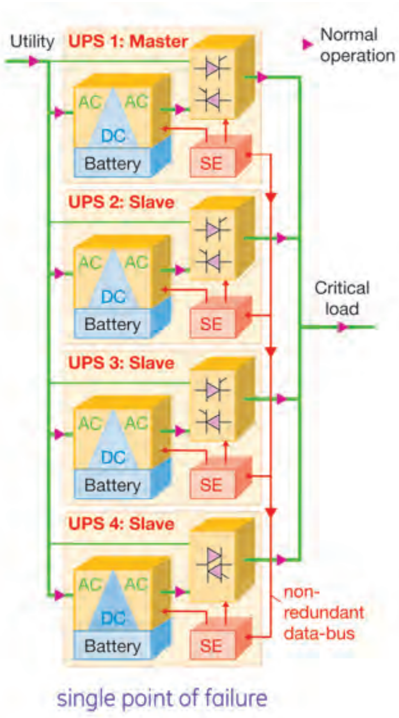


Figure 15.
Parallel system without external controls or switch, but with at least two single points of failure.

3.6 Real redundancy parallel architecture without a single point of failure

GE is one of few manufacturers on the market producing UPS units with real redundancy. The system is called Redundant Parallel Architecture (RPA). In it there is no need for external electronics or switches to control the UPS in parallel arrangement (Figure 16). With RPA, using so-called Active-Active-Technology, one of the UPS in the system temporarily takes on the role of the Master and the others follow, as in a democracy in which one person takes on the role of leadership. However, all UPS have access to all control parameters. The system is equipped with a redundant bus (featured twice) which ensures constant distribution of the load. If one UPS unit fails to operate, the load is automatically redistributed among the other units. If the Master UPS fails to operate, then a different UPS automatically takes on the role of the Master. If necessary, any of the UPS in this democracy can take on the role of leadership.

If there is a need for more protected power, it is possible to simply add further UPS in parallel to the existing ones. Furthermore, a UPS can easily be switched off or another one switched on. And here is the unique feature of GE's RPA: your critical load is always protected. As soon as a UPS is switched off, its load is taken over by the other units without the load even 'noticing' a change of voltage. The addition of a UPS unit is a more complex operation. The new unit must first be synchronised with the load voltage, and then the Master UPS must take care of the integration into the whole system requiring a new distribution of the load. In the designs offered by other manufacturers, a change in load distribution necessitates a change into bypass mode. This means that the critical load is connected to the utility power without protection in case of power failure.

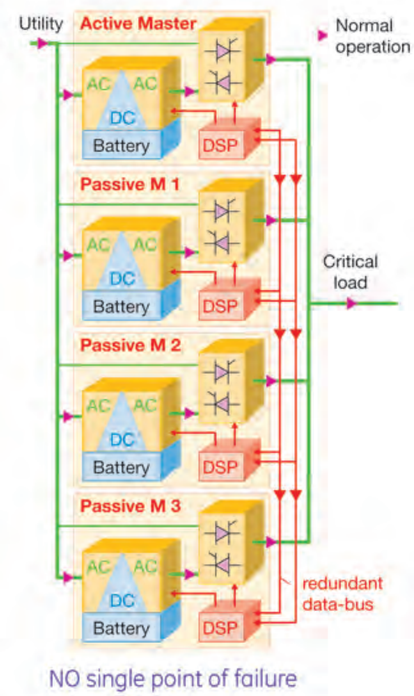


Figure 16.
GE real, redundant parallel system, without a single point of failure.

The critical point of this GE technology is the exact synchronisation of all the UPS that are aligned in parallel. The reference value is the load voltage, and depending on the load, individual UPS will need to provide more or less current. The supply of the necessary load current is the control-condition reference value. The distribution of the load with RPA technology is so precise that all the UPS in the system provide substantially the same current (it varies by only a few amperes). Finally, the excellent dynamic behavior of this architecture needs to be mentioned. It guarantees a negligible fluctuation of voltage even in the case of a sudden, big load jump e.g. a short circuit.

3.7 The cost advantage of a completely modular system

The need for upgradable UPS systems with highest fail-safe operation has increased dramatically. Few companies operate without having their own server, quite apart from all the internet service providers, banks, telecom companies etc. All of these need UPS systems. They are ready to invest capital in order to obtain a maximum of operability. Important criteria in the choice of a system are the questions of the expansion of the system later and the length of time that the UPS system can provide power during a power failure. It makes little sense to install an over-specified UPS system just because there might be a need for more power in the future. An over-specified UPS system produces unwanted heat and costs more.

For the above reasons the upgradeability and failure-tolerating N+1 redundancy is important for sensitive loads. The modular approach also makes for cheaper production and running costs.

There are different versions of the modular system on the market such as strict separation of the UPS into individual casings or into drawers in a main casing. Both versions have their advantages and disadvantages, which are not discussed in this brochure. The customer has to make sure that he is given the pertinent information.

3.8 UPS – only a part of a safe power supply

In a high-standard set-up the UPS with its set of batteries represents only part of the whole. The quality and correct installation of other parts such as the connection to the mains, the connections to the output, the type of fuses used and the selectivity of the different circuits all play a vital role.

The above points highlight the fact that the UPS is by no means the only element in getting a secure supply of electricity to your critical load. The experience of recent years has shown that integrated solutions are called for. Market research shows that manufacturers of UPS should offer integrated systems in the future. In other words, offering a high quality UPS is no longer sufficient. An overall solution is what is called for. This solution comprises all the parts between the connection to the utility network and the load.

3.9 The future: advantages through integrated solutions

If a UPS manufacturer offers an approved overall concept, a whole range of problems is eliminated. Here is an illustration: if you ask an architect to build your house you will get a house that is unique. If you chose your house from the catalogue you'll get something which is well-planned but off the shelf. In this house everything should work. Teething troubles, which one would have to expect in the case of a 'prototype house', should be eliminated. It may be that for your own special house you'll put up with 'teething troubles'. With regard to a secure power supply it is completely different. Here it does not make sense to develop the whole system from scratch again for each new application. For an every-day application this is less important. The parts simply have to be wired up correctly according to an existing diagram. It is rather like putting railway carriages in the right order on the rails. For a complex application, as required in the office or telecommunication sector, the design of an individual power supply system would be a demanding and time consuming job for a highly qualified 'architect'. To go for an individual special solution obviously does not make sense in this case. Here one must go for the proven solution off the shelf – one comprised of tested elements which can be put together in different ways.

Such a system should not only include switch cabinets with excess tension protection, power switches, automatic fuses, input and output connectors, distributors, the obvious UPS unit with its set of batteries, but also a comprehensive control and service programme. Ideally a comfortable design programme greatly simplifies the work of the system designer. The advantages are striking:

- Achieving greater reliability of the whole system.
- Saving through the use of standard modular elements.
- Testing of the entire system beforehand made possible.
- Shortening of the installation time.
- Dealing with only one partner.
- Permanent monitoring, making visual checks unnecessary.
- Discovering potential problems in advance.

3.10 Critical loads that overtax an ordinary UPS system

There are extraordinary demands on UPS systems in the area of telecommunication, medicine and also industry. Particularly critical are loads that must under all circumstances be supplied with electricity. Here a redundant system is imperative. But there are also other kinds of critical loads, namely those that draw power in an extremely pulsating manner (Figure 17). Medical scanners, computer tomography and x-ray machines fall into this category along with certain machines in industry. These consume large amounts of electricity for short periods of time. On the right in the picture the effect on the utility power can be seen clearly i.e. sags and peaks of tension. These adversely affect the operation of the instruments. It need hardly be said that a power failure in a hospital is extremely critical if some diagnostic process or op- Near-by grid distortion Dynamic current absorption Medical Scanner Figure 17 Pulsating power consumption of a medical appliance. 13 eration is in progress. Which patient would be pleased about a power failure while he is being examined or while the computer is evaluating his data?

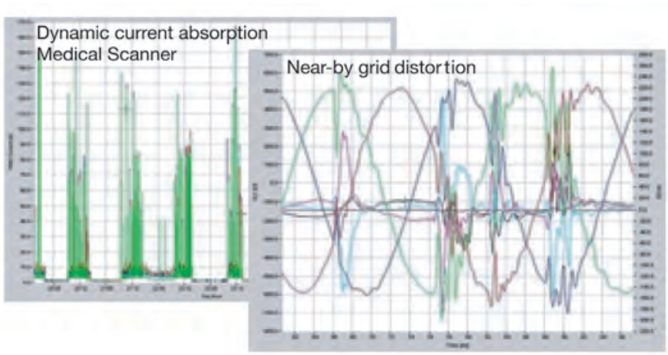


Figure 17.
Pulsating power consumption of a medical appliance.

What is the problem in this case? Ordinary UPS systems have great difficulty in supplying loads that use electrical power in a fluctuating manner. Here are the resulting problems: the tension drops sharply and this in turn causes the instrument to work improperly. The simple sort of UPS system may not even be able to supply a current that is higher than the nominal one, not even for a short time. What can the customer do? He could opt for a (highly) over-rated UPS so that it will be able to cope with the fluctuations. However, the problem is not yet solved. For a short interval of time his unit is likely to deliver undertension, because it cannot cope with the dynamics of fluctuation. When a load is switched on, i.e. starts operating, the initial current causes the tension of the UPS to drop, the switching off of the load causes the opposite, i.e. a rise in tension. The other loads connected to the UPS may suffer harm. The European standard EN 50091 for UPS defines variation in tension in terms of dynamic changes of the load. The UPS units of manufacturers which guarantee this standard are, however, far from being able to supply critical medical machines adequately. Class 1 standard allows a drop of tension of 30% during 6 ms while the load rises from 0 to 100%. The same is true for a drop of the load: the tension may rise up to

30% during 6 ms. 30% fluctuation in tension during 6 ms is a lot for average electronic equipment. GE systems offer ten times better values. With a change of load of 100% the tension fluctuates a mere 3%. It is to be noted that greater changes of the load occur with certain medical instruments. It is worth the purchaser's while to make a very careful comparison. A cost comparison alone with a standard unit (which would have to be an over-rated one) simply isn't sufficient. In the medical sector the difference in price is a relatively insignificant one when a high quality UPS is being purchased – it amounts to 3–30%.

How does GE achieve these superior values (compared to EN 50091)? GE achieves them through the use of an inverter with highly dynamic characteristics in combination with special output wiring. In particular through the following three features:

- The output transformer has zigzag windings, thus distributing a change of load on one phase to two phases of the output inverter. For very critical loads an output transformer is usually installed in the UPS unit for safety reasons so that even in the worst case no direct current gets through to the load.
- The output tension as well as the output current are monitored directly and are evaluated with regard to the tendency to change (i.e. in a differentiating manner).
- The highly dynamic SVM technology (Space-Vector-Modulation) is used for the control of the inverter. Most equipment on the market still uses PWM technology (Pulse Width Modulation).

These three measures allow the unit to discern changes of the load ahead of time, and react through the inverter within microseconds. The three features together with elaborate DSP technology (DSP=Digital Signal Processor) have resulted in GE producing a UPS unit with 10 times better dynamic values than those of the European specification for Class One UPS.

4. Intelligent software makes the difference

Worldwide there are hundreds of UPS manufacturers, but most offer only a very limited range of units. If you start looking for manufacturers who produce units for a few hundred watts up to the megawatt range, the number shrinks to a mere dozen. And if you start looking for companies that offer efficient monitoring and maintenance software, the figure drops to a mere handful of names.

Installing a UPS correctly is one thing. Shutting down all the computers in case of a power failure is another – especially if no one is around. Programmes that are running have to be stopped, open files have to be shut down, and unsupervised systems have to be shut down in a controlled way. When the utility power is on again, the UPS software takes care of rebooting the system again. This is the straightforward task of the so-called shutdown programmes which most UPS manufacturers offer free of charge. The operation becomes more difficult where a complex IT-system with different operating systems and hardware from different suppliers is in use (Multi-Platform and Multi-Vendor). The most difficult case is a decentralised system that has to be monitored by remote control.

4.1 Functionality of the UPS software

This is best explained by giving an example. Figure 18 shows in a simplified way the computer/UPS system together with the server and various customers online. By means of SNMP the UPS units are integrated into the IT-network (Simple Network Management Protocol, a worldwide standard language for the communication between components of IT networks). The UPS jumps into action as soon as the utility power fails.

Taking the example of the GE software 'Suite' the comprehensive functionality is easily understood. The software packet consists of two parts, which can be used individually or together.

JUMP (Java Universal Management Platform) affords high flexibility and wide ranging independence from the differences of the IT operating systems. JUMP jumps into action when the UPS are integrated into the IT network and when an orderly shut-down of the whole system has to be carried out, e.g. open communication links having to be closed.

IRIS (Internet Remote Information System) makes, as the name says, remote monitoring of UPS possible. Wireless systems such as GPRS and UMTS are used to supplement the link through the internet. IRIS has its place when an independent structure for monitoring is needed and when people who are not part of the internal network have to be contacted, e.g. service technicians of the UPS manufacturer.

JUMP will call on the person responsible for the software, IRIS on the person responsible for the technical infrastructure. Both software users can adapt the programme and receive the information in their own language. The person responsible for the software will receive it by means of SNMP right into his network management system (NMS) – the person responsible for the technical side of the set-up will receive it in the form of Volt and kW information.

Figure 18.
Typical network configuration of UPS units and computers.

4.2 Big supermarket chains – maintenance of 1000 UPS

A chain of supermarkets may have 1250 shops and 160 restaurants. The entire supply of goods is computer controlled. In total this chain may have 6600 cash points and 2600 computers to support the cashiers in their task. In most of the markets no UPS are planned for the server, the network and the scanner cassettes. If a UPS does not work properly no one is likely to notice it. After all you cannot expect the personnel, in the rush of serving customers, to take notice of a warning signal coming from a UPS. In an individual branch of a supermarket chain it's highly unlikely that someone is responsible for the computers and the software. Therefore no-one will do anything about the problem with the UPS. UPS are there to bridge power failures and these don't happen according to plan – but a faulty UPS will in that situation not be of any use. This calls for a solution. If there is a fault in a UPS or if there is a utility power failure the service centre of the chain would like know what has happened and where (Figure 19). Then, when the case arises, the service centre will be able to act, i.e. send instructions to the particular branch. In this way the problem can be solved or the damage limited. Causes for faults in UPS can be high temperature or unauthorized connecting of new equipment. UPS units do require maintenance! The batteries at least have to be checked regularly. To do this for 1250 supermarkets is a major job, requiring personnel. Therefore GE has worked on a system to monitor the state of UPS by remote control thus reducing the number of breakdowns.

All the UPS are connected to the local area network (LAN) by means of a SNMP card. This card gives access to remote maintenance. The UPS reports any fault automatically. The report goes to the regional centre as well as the headquarters of the supermarket chain. In addition, the technical service centre of GE is notified. Depending on the kind of fault reported it will be decided whether a GE technician has to go to site or not. At the moment this particular market chain has 300 UPS of 600 VA–400 kVA in operation, all supplied by GE. In addition to this it has 500 UPS in operation from various other suppliers, all of which will shortly be replaced. The new UPS are fitted with a device which calls the service technician of the market through a visual or audible signal.

Thanks to maintenance by remote control and a warning system at the main service centre it seldom happens that one of the UPS in a branch of this chain breaks down.

5. Other things that users of UPS systems need to know

How can I calculate the correct power requirement for a UPS system? How can the UPS be tested to see whether it actually works when there is a power failure? What maintenance work is required? And last but not least, what set-up suits the needs of my enterprise?

5.1 The right choice

Where you have one server with network stations (probably not backed-up by UPS) a unit providing a long autonomy time in the case of power failure doesn't make sense – continuing work is out of the question anyway. What is important is that the components of the network can terminate their application in a controlled fashion before the battery power is gone. Normally a server should be shut down within five minutes of a power failure.

In order to provide a fully automatic shutdown of the above system the right kind of UPS needs to be combined with the right sort of software. This software must be installed on the server and possibly on other computers in the data network. When the server is booted up after a power cut, the batteries are still not recharged. A second power failure could then lead to a tragic collapse of the system. A feature of sophisticated UPS systems therefore is that the load can only be turned on again after the batteries have been recharged.

In computer centres in hospitals, where shutting down the system is not an option, the UPS is mainly there to bridge the time between the beginning of a power failure and the emergency power generator (petrol or diesel) providing (synchronised) power. In this case a few minutes of autonomy time are sufficient, but it must be kept in mind that the back-up system has to provide several hundred kVA of power because the entire installation is running on the UPS.

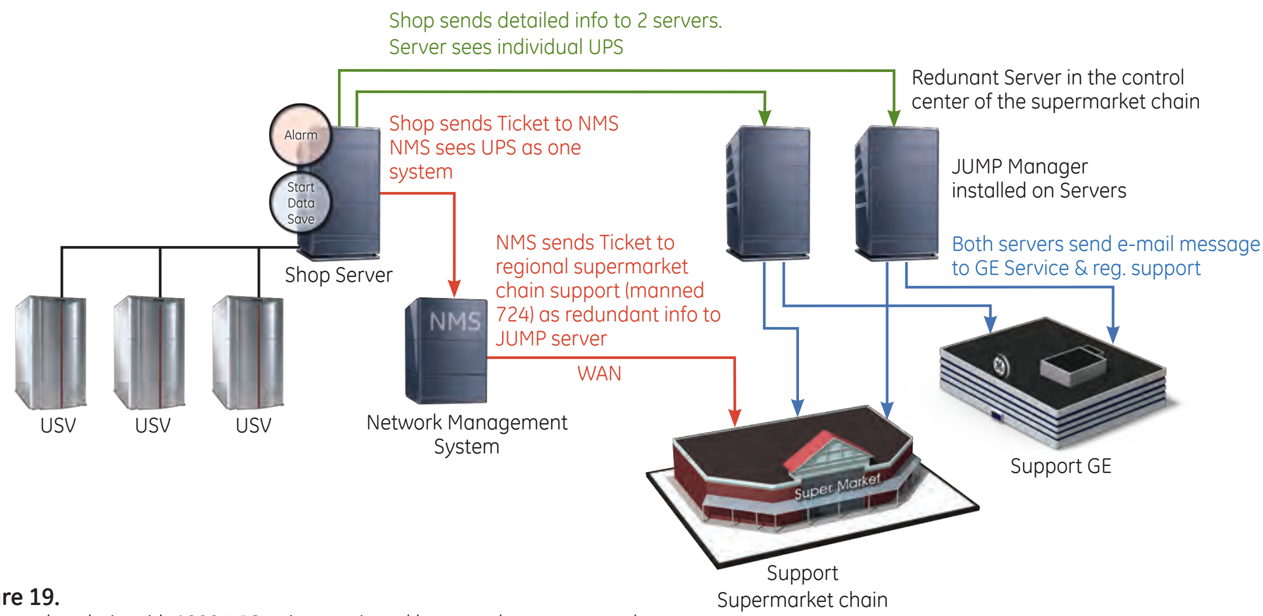


Figure 19.
Supermarket chain with 1000 UPS units, monitored by central remote control.

UPS are available from 300 VA rated power up to 500 kVA. In the case of more complex projects it is advisable to consult a UPS expert. As already stated, computer systems and industrial plants that require a high level of energy availability need a redundant UPS system. The electrical planning of such a project together with software that is needed on different computers requires considerable know how. In simple situations the customer can chose the UPS himself. In order to do that he first needs to calculate the power requirement.

5.2 What power does a UPS need?

1. The first step is to define all the different loads that will be connected to the UPS. It is important to remember that it is not enough to only connect the server. An operating system such as Windows NT requires that the computers in the network be shut down in a specific sequence if the rebooting after the power failure is not to last hours or even days. It is also clear that the monitors and external accessories such as hard drives, tape drives and active network components like switches or routers must be taken into account.

2. The next step is to determine whether any subsystems need special protection.

3. The complex power S* (VA value) of each piece of equipment is to be determined.

4. Is any system or network expansion foreseen in the not too distant future?

5. The UPS is to be rated according to the addition of all the VA values.

5.3 Is the UPS functioning correctly?

Modern UPS units are equipped with an automatic battery test that is performed once or twice a month, but the customer should perform his own test once a year in order to verify the capacity of the batteries. Customers of GE can leave this to GE specialists who do the test via the internet. A battery test monitors how the battery voltage behaves with time and load. If the voltage sinks too quickly, the batteries are defective. The time taken for the batteries to discharge must not be lower than the specified autonomy time. If this is the case, all the batteries must be replaced.

5.4 Is the UPS system adapted to the level of protection needed?

UPS systems must fulfil very different needs depending on the application. In practice different security levels are distinguished in UPS systems. For example there are computer users who simply want to protect their computer from crashing in the case of a power failure. Such users are at the lowest level of security. A highly complex computer network with a central server is at a high security level. This network must remain in operation 365 days a year and round the clock in spite of power failures, and any other problems.

Level of security	Type of UPS? Characteristics of the UPS?	Protection from what? Used for what?
1	**Off-line:** Dependent on utility power with regard to tension and frequency, switchover time 2–8 ms. Battery operation needed in case of under-voltage. Square, trapezium or sine wave voltage, shutdown and diagnosis software optional.	Protection from power failures, NO protection from over-voltage. Single work place.
2	**Active Standby or Line-Interactive:** Dependent on utility power with regard to frequency, over- and under-voltage is adjusted in steps using the auto-transformer. Switchover time 2–8 ms. Square, trapezium or sine wave voltage, shutdown and diagnosis software optional.	Protection from power failures, and from over-voltage. Single workplace and small multiple-workplace situations with network.
3	**Double conversion (VFI):** Double voltage conversion, load-stable sine voltage independent of utility power, quartz-controlled frequency, no switchover time, galvanic separation from utility power.	Protection from power failures and all faults in the utility power, such as over- and under-voltage, distorted frequency and spikes. Server and multiple workplace with network.
4	**Double conversion (VFI) with RPA:** Double voltage conversion, load-stable sinusoidal voltage independent of utility power, quartz-controlled frequency, no switchover time, galvanic separation from the utility power, parallel redundancy, upgradeable with regard to power and autonomy, system exchange without shutdown.	Protection as in 3 with additional system availability thanks to Redundant Parallel Architecture (RPA). Computing centres, internet providers, mainframes, demanding multiple workplace computer systems, very sensitive industrial applications.

5.5 Protection from lightning

A direct impact by lightning is very rare, but the spin-off effects of lightning are devastating none the less. Once lightning current has found its way into the building, the computer network is going to suffer major damage. However, as just mentioned, a direct lightning impact is very rare. Most cases of damage stem from indirect impact, i.e. when lightning strikes somewhere in the vicinity. These can be prevented, because an electrical installation or a computer system can be protected, even from a direct impact. But this is not possible simply by using a UPS. Over-voltage because of lightning (far or near) can reach the building via the utility power network, the telephone line or data-cables. In order to protect a building from this, several options are available: a good potential equalisation arrangement, Surge Protection Devices (SPD), and of course a good lightning trap.

5.6 And finally

Not all UPS are of the same kind and quality. Many users have had to learn this the hard way. In the case of complex systems in the computer sector and industry in general, basic electrical knowledge is no longer sufficient to chose a reliable – and at the same time adaptable – solution or even to evaluate it. Reliability, professionalism and performance of the manufacturer are at least as important as the technical specification of the system itself.

* Where the active power P is indicated, S is approximately 1,4 × P. The result is the approximate VA value. Or, where the voltage and current consumption is known, then S = U × I.

070209-v2

Industry Innovations

Featured Innovation

Intuitive and Intelligent Feeder Protection

Multilin 350 Feeder Protection Relay
GE Digital Energy – Multilin
www.GEMultilin.com/350

The Multilin 350 Feeder Protection System provides the utility power distribution & industrial industries with a technologically advanced, easy-to-use, and intuitive overcurrent (50/51) protection relay. The Multilin 350 performs primary circuit protection of medium voltage distribution feeders. The robust Multilin 350 streamlines user workflow processes and simplifies engineering tasks such as configuration, wiring, testing, commissioning, and maintenance via advanced communications and enhanced diagnostics. Mechanically designed for effortless draw-out, to eliminate re-wiring, the Multilin 350 enables fast installation, simplified retrofit and reduced lifecycle cost.

Measure Low Resistance from Anywhere

Heavy Duty Low Resistance Ohmmeter
Megger
www.megger.com

Equally at home in the laboratory, the workshop or in the field, on the bench or on the ground, Megger´s new heavy duty DLRO10HD low resistance ohmmeter combines rugged construction with accuracy and ease of use. It features an internal rechargeable battery and can also operate from a mains supply, even if the battery is completely flat. Like all models in the DLRO10 range, the DLRO10HD, when used with optional terminal insulating test leads, is rated CATIII, 300 V in line with IEC61010.

Uninterruptible Power & Energy Efficiency for Data Centers

750 kVA UPS System
GE Digital Energy
www.GEDigitalEnergy.com/pq

GE Digital Energy's 750kVA Uninterruptible Power Supply (UPS) has been ecomagination certified after completing GE's rigorous ecomagination certification Product Review (EPR) process. GE's 750kVA UPS system helps customers reduce their energy consumption and costs. At a typical 50 percent load, GE's 750kVA UPS system achieves efficiency of more than 94 percent, delivering uninterruptible power to the booming global data center industry at higher efficiency than competitors' systems.

Increase Safety with Arc Proofing Tape

Scotch® Fire-Retardant Electric Arc Proofing Tape 77 & 77W
3M
www.3M.com/electrical

Scotch® Fire-Retardant Electric Arc Proofing Tape 77 and 77W are designed to protect all types of electrical cables where exposed to potential failures of other energy cables. Its unique formulation expands in fire to form a thick char buildup. This insulating shield protects the cables and accessories from fault arc generated heat and flames.

Industry Innovations

Extend your Network's Reach

MultiLink MC-E Media Converters
GE Digital Energy - Multilin
www.GEMultilin.com

The MultiLink MC-E series of media converters uses the power of optical fiber to extend your Ethernet network to remote locations. Designed for harsh utility and industrial applications the MultiLink MC-E provides robust and reliable connectivity.

Tested. Proven. Trusted. Cable Bus

Cable Bus Systems
MP Husky
www.mphusky.com

MP Husky engineers and manufactures Cable Bus systems that utilize continuous runs of cable from termination to termination, eliminating the need for potentially faulty splices found in non-segregated phase bus duct systems. And since MP Husky Cable Bus utilizes highly reliable outdoor rated cables, moisture and weather do not damage the system. In fact, the system is designed to allow air, moisture and other elements to flow through the system, which eliminates the need for moisture canceling components such as filter breathers and heater strips. Optimal balance of the conductors within the system, achieved by MP Husky's exclusive Inductive Reactance Program, results in the most balanced load on each conductor which prevents overloading and overheating of the conductors. No splices, optimal ampere balance, air-cooled conductors, and fewer parts to fail equal a more reliable electrical feeder system.

Enabling AMI with Industrial WiMAX Communications

MDS Mercury™ 3650
GE Digital Energy – MDS
www.GEMDS.com/mercury

The MDS Mercury™ 3650 is a highly secure, industrial-grade WiMAX platform for creating wireless communications to support utility's Advanced Metering Infrastructures (AMI) that are designed to give electrical consumers the ability to monitor electrical usage and manage costs in near real-time. The WiMAX enabled MDS Mercury is also ideal for mission critical, industrial and public safety applications including SCADA, Distributed Automation devices, video, VoIP, mobile data, and Intranet applications. With up to 9 Mbps of aggregate Ethernet throughput (or 800 kbps for nomadic mobile deployments), and a choice of frequencies, MDS Mercury has the capacity and deployment flexibility to facilitate your immediate and long-term requirements.

Submersible Underground Connectors

MUCI Series
SICAME Australia
www.sicame.com.au

Designed for water-proof, underground connection of 2, 3 or 4 cables, the MUCI Series of Submersible Connectors provides reliable, secure connections. Suitable for copper or aluminum insulated cables, single or double insulated from 6 to 50 sq. mm. This solution is ideal for connecting cables in pillar boxes, buried connection pits and street light columns.

Universal tool for working with IEC 61850 IEDs

IEDScout
OMICRON electronics Corp. USA
www.omicronusa.com

IEDScout is a universal client to IEC 61850 servers (such as substation IEDs) and a publisher/subscriber for GOOSE messages. It provides numerous useful functions needed in the substation or the laboratory. As an IEC 61850 client it supports many functions, from generic reading/writing of data attributes to using the self description of the IED and producing SCL files from it. It detects GOOSE messages on the network and monitors them. The IEDScout also simulates GOOSE messages. With IEDScout, the protection engineer has new options to enhance the depth and quality of testing.

Compact, affordable Thermal Imaging

MikroSHOT
LumaSense
www.lumasenseinc.com

The MikroSHOT is the latest offering from LumaSense Technologies' Mikron Infrared thermal imaging product line. This fully radiometric thermal imager allows for affordable, pocket-sized portability with capabilities normally found in larger, more expensive thermal imagers. The MikroSHOT's Thermal-on-Visible mode allows radiometric temperature data to be displayed directly on the visible image. The MikroSHOT is lightweight (10.5 ounces) and uses off-the-shelf batteries (AC adapter included). Its 2.7-inch display and 160x120 pixel image resolution allow easy viewing of images. The MikroSHOT has a measuring range of minus 4 F to 662 F, operating temperature range of 5 F to 122 F, color alarm and autofocus at distances 1.4 yards to infinity. The SD card, USB and video output capability allow for convenient, quick analysis of the JPEG-format data on a laptop or other mobile device using common software. MikroSpec 4.0 software is included for image analysis and reporting.

Rugged Power Sensing for Utilities

ITI Outdoor MV Instrument Transformers
GE Digital Energy – ITI
www.GEDigitalEnergy.com/ITI

MV outdoor current & voltage transformers are now available at 60 Hz from 15-35kV. HCEP Epoxy and Automated Pressure Gelation are combined to produce the highest quality and reliability for outdoor applications. GE combines superior design and advanced testing with HCEP resin and APG process technology, to produce reliable Outdoor Medium Voltage Instrument Transformers that meet IEEE C57.13-1993 and CSA CAN3-C13 insulation level standards, and IEEE C12.11 dimension standards.

Expanded Design tools for Infrastructure Modeling

Autodesk 2010 line of 2-D & 3-D Design & Engineering Software
Autodesk
www.autodesk.com

Autodesk announces its new 2010 line of 2-D and 3-D design and engineering software. More than 50 new products offer new features and functionality, as well as improved tools for Digital Prototyping, Building Information Modeling (BMI), Infrastructure Modeling, sustainable design and analysis, which will help architects, engineers and designers meet increasing commercial and public sector demand for more energy-efficient buildings, products and infrastructure. The 2010 software for Infrastructure Modeling includes new features that enable suers to more easily aggregate multiple sources of data, improving the design of smart electric utility grids, making planning city projects easier, and enabling more efficient design and repair of highways.

Upcoming Events

DataCenterDynamics	Jul 17 – 18	San Francisco, California, United States

As a focal point for end-users, consultants and solution providers, the DatacenterDynamics Conference & Expo is the Bay Area's largest gathering of professionals involved in the design, build and operational management of 24/7 mission critical IT facilities. It is an unrivalled education & networking opportunity for the industry, where the regular audience is characterized by senior representatives of the of the financial, medical, media, service provider, outsourcing/managed services, and other Fortune 500 companies operating throughout the Bay Area, Silicon Valley and the Western US.

Hilton San Fransico
www.datacenterdynamics.com

Visit GE Digital Energy – Power Quality, in the Exhibition Area

ITE	Aug 9 – 12	San Antonio, Texas, United States

Join nearly 1,000 transportation professionals as they exchange ideas on transportation issues. Highlights include numerous technical sessions where you can share your perspective in the open dialogue between the audience and panelist(s) in the conversation circle sessions.

Attending this growing annual event will give you access to dynamic paper presentations, technical tours and professional development seminars. Stay abreast of the newest technologies and services at ITE's Transportation Products and Services Exhibit where displays from the public and private sectors.

Henry B. Gonzalez Convention Center
www.ite.org

Visit GE Digital Energy – MDS, in booth #121

IMSA	Aug 18 – 26	Orlando, Florida, United States

The 11th Annual IMSA Conference and 32nd Annual School is dedicated to providing quality certification programs for the safe installation, operation, and maintenance of public safety systems; delivering value for members by providing the latest information and education in the industry.

Omni Resort at Champions Gate
http://www.imsasafety.org/2009conf/2009conf.html

Visit GE Digital Energy – MDS, in booth #615

Upcoming Events

Protection & Automation	Sep 7 – 10	Moscow, Russia

The Actual Trends in Development of Power System Protection and Automation conference discusses the current state and prospects of architecture development, of design principles and operation algorithms of the relay protection and emergency control. Emphasis will be placed on main tools and techniques to promote efficiency and reliability of the relay protection, automation, and emergency control systems. The conference program will include a plenary session, paper sessions, poster session, round table and manufacturers' special presentations.

Hotel Borodino
http://www.relayprotect.ru/en/index.htm

GE Digital Energy – Multilin, Papers to be Presented:

- Problems and Solutions of Line Differential Application in Cable Transformer Protection
- New Approach in Functionality and Testing for HV Capacitor Bank Protection
- Evaluation of the Ground Operating Current in Industrial Systems with Network Distribution through MV Cables
- Reducing Conventional Copper Signaling in High Voltage Substations with IEC 61850 Process Bus System
- Improvements in Power System Integrity Protection Schemes

Visit GE Digital Energy – Multilin, in the exhibition area

UTC Canada	Sep 14 - 17	Halifax, Nova Scotia, Canada

UTC Canada is a trade association focused on addressing the critical telecommunications issues for utilities and energy companies in Canada and the providers of telecommunications infrastructure or information technology services. UTC Canada works to bridge the issues that impact both the parent utilities and their competitive telecom subsidiaries as an advocate for the telecom and IT interests of all Canadian electric, gas, and water utilities, and oil and gas pipelines.

Westin Nova Scotian
www.utccanada.org

Visit GE Digital Energy, MDS & Lentronics, in booth #200, 202

IEEE IAS PCIC	Sep 14 - 16	Anaheim, California, United States

The IEEE IAS PCIC is an international forum for the exchange of electrical applications and technology related to the petroleum and chemical industry. The annual 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.

Hilton Anaheim
www.ieee-pcic.org

GE Digital Energy – Multilin, Papers to be Presented

- Reducing Arc Flash Risk with the Application of Protective Relays
- Ground Fault Protection for MV Bus Connected Generators

Other GE Papers to be Presented:

- Arc Flash Mitigation by Fast Energy Capture
- Revisions to IEEE 1068: Standard for the Repair of AC Motors in the Process Industries
- A User's Guide for Factory Testing of Large Motors: What Should Your Witness Expect?
- Use of Thermal Network on Determining the Temperature Distribution Inside Electric Motors in Steady State and Dynamic Conditions
- Core Loss Testing: A Good Procedure Gone Astray?
- Predicting Let-Through Arc Flash Energy for Current Limited Circuit Breakers

Visit us in the GE Hospitality Suite – Hilton Anaheim

- Nightly from Sunday, September 13th through Tuesday, September 15th - Lainai Delux Suite

Upcoming Events

ASGMT | Sep 21 - 24 | Houston, Texas, United States

The American School of Gas Measurement Technology (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, leading industry manufacturers will exhibit the latest in products and services. This offers an exceptional opportunity to see the latest solutions available to the natural gas industry.

Marriott Houston Westchase
www.ASGMT.com

Visit GE Digital Energy – MDS, in booth #105

ISA Expo | Oct 6 - 8 | Houston, Texas, United States

ISA Expo is an exhibition for promoting Automation and Control technology. ISA is a leading, global, non-profit organization that is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems. Based on research, 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

Visit GE Digital Energy, in booth #1243

GCC Power 09 | Oct 19 - 21 | Riyadh, Kingdom of Saudi Arabia

The conference will offer delegates the opportunity to discuss the latest trends, challenges, developments and strategies to meet the region's rapidly expanding energy needs through a series of panel and technical sessions. Government decision-makers, leading regional and international power companies and respected industry advisors will attend to share past experiences, exchange ideas and get up to date on the latest scientific research. The conference will also provide delegates with a unique opportunity to enhance cooperation and collaboration throughout the region and will promote competitiveness and efficiency in the electricity industry.

Marriott Hotel
http://www.gcc-cigre-power.com/

GE Digital Energy – Multilin, Papers to be Presented:
- Reducing Conventional Copper Signaling in High Voltage Substations with IEC 61850 Process Bus System

Visit GE Digital Energy – Multilin, in the exhibition area

Upcoming Events

APAP 2009 & CIGRE B5	Oct 18 - 24	Jeju, Korea

The purpose of Advanced Power System Automation and Protection (APAP) 2009 is to invite the researchers, engineers, and experts in power system automation and protection filed, and to provide an opportunity to share their experiences and knowledge. APAP2009 is specially devoted to the advanced protection and automation technology in power systems, but not limited to. I believe that the conference will establish a clear goal and direction of the researches in this field and make a contribution to develop the protection and automation technology for next-generation power systems.

The mission of the Study Committee B5 is to facilitate and promote the progress of engineering and the international exchange of information and knowledge in the field of protection and automation. SC B5 annual meeting and colloquium 2009 in Jeju, Korea will provide a platform for the experts, scholars and engineers to exchange experience and share knowledge in three preferential subjects - Strategies for the Lifetime Maintenance of SAS Systems, Protection & Control of FACT devices and impact on Protection Systems and Wide Area Monitoring, Control & Protection Technologies.

Lotte Hotel Jeju
www.apap2009.org **www.cigreb5korea.org/english/portal.php**

GE Digital Energy – Multilin Papers to be Presented at APAP 2009:

- Design and Implementation of an Industrial Facility Islanding and Load Shed System
- Impact of Frequency Deviation on Protection Functions
- Designing Copper Wiring out of High Voltage Substations: A Practical Solution and Actual Installation

GE Digital Energy – Multilin Papers to be Presented at CIGRE B5 Annual Meeting:

- Improvements in Power System Integrity Protection Schemes
- Reducing the Costs of Periodic Maintenance of Secondary Systems in High Voltage Substations with the use of Process Bus
- The Impact of Digital Technology on the Maintenance of Substation Automation Systems
- Lifetime Management of Relay Settings

WPRC 2009	Oct 20 - 22	Spokane, Washington, United States

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

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

GE Digital Energy – Multilin Papers to be Presented:

- Reliability of Protection Systems: What are the Real Concerns
- Enhanced Algorithm for Motor Rotor Broken Bar Detection
- Designing Copper Control Wiring Out of High Voltage Substations: A Practical Solution and Actual Installation
- Fault Locator Based on Line Current Differential Relay Sychronized Measurements
- Fully Utilizing IED Capability to Reduce Wiring

Visit us in the GE Hospitality Suite – Red Lion Hotel at the Park – Room 5009/5010

- Nightly October 20th through 22nd – 6:00 pm to 10:00 pm

Upcoming Events

MIPSYCON	Nov 3-5	Minneapolis, 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.

Earle Brown Heritage Center
http://www.cce.umn.edu/conferences/mpsc/index.html

Visit GE Digital Energy – Multilin in our Hospitality Suite

EUTC 2009	Nov 3 – 6	Budapest, Hungary

Technology is rapidly changing the role of telecommunications in Europe's electric, gas and water utilities, energy companies, and other critical infrastructure companies. Many are using their vast experience in building and managing sophisticated telecommunications networks to enter Europe's new competitive telecoms markets. Many are also facing issues introducing new wireless communications systems and managing internal telecoms businesses in a shared services environment. To meet this need, the Utilities Telecommunications Council created a uniquely European program that builds on UTC's 60 years of experience, existing strengths and services. UTC's programs in Europe is led by Europeans, designed for Europeans, and is uniquely European in focus.

Corinthia Hotel Budapest
http://www.eutc2009.utc.org/content/eutc-2009

Visit GE Digital Energy – Multilin in the exhibition area

Digital Energy
Multilin

The right career is waiting for you

We protect and connect the world's critical equipment to ensure safe, reliable power

With operations in over 160 countries worldwide, GE employees have an unparalleled foundation on which to build their careers and abilities.

We are seeking innovative, self-motivated, imaginative and entrepreneurial candidates to join our fast-paced, technology-forward environment in:

- Protection Engineering
- Product & Program Management
- Hardware & Firmware Design
- System & Application Engineering
- Sales Application Engineering

To join our dynamic organization please forwards your resume to hr.pc@ge.com

Advanced Training

GE Multilin 2009/2010 Course Calendar

Comprehensive Training Solutions for
Protection, Control and Automation

SCHEDULED COURSES IN NORTH AMERICA

Courses for 2009/2010	Tuition*	CEU Credits	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN
Smart Grid: From Basics to Practical Applications (Rochester, NY)	$2,400	2.1			22-24									
Fundamentals of Modern Protective Relaying	$2,400	2.8	20-23		14-17		9-12		18-21			19-22		
Introduction to the IEC61850 Protocol	$2,400	2.1				5-7				17-19				
Distribution Protection Principles & Relaying	$1,800	2.1			9-11								17-19	
Motor Protection Principles & Relaying	$1,800	2.1	6-8			14-16	17-19	1-3		9-11				8-10
UR Platform	$1,800	2.1		17-19								12-14		21-23
UR Advanced Applications	$3,000	3.5				26-30							10-14	
Enervista Software Suite Integration	$600	0.7			18		13				18			
MM300 2 Days Hands-on	$1,200	1.4									16-17			15-16

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

*Tuition quoted in US dollars

SCHEDULED COURSES IN EUROPE

Courses for 2009/2010	Tuition*	CEU Credits	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN
UR Advanced Applications	$2,400	2.8			18-22			21-25		15-19			17-21	
UR Platform	$1,800	2.1			13-15			16-18		10-12			12-14	
Distribution Protection Principles & Relaying	$1,800	2.1	10-12				7-9				9-11			
Fundamentals of Modern Protective Relaying	$2,400	2.8				8-12								7-10
Motor Management Relays	$1,800	2.1	24-26				21-23				23-25			
F650 Platform	$1,800	2.1		20-22		23-25						19-21		21-23
Introduction to the IEC61850 Protocol	$1,800	2.1		23-24								22-23		

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** for the most up-to-date schedule.

Protection & Control Journal

Content Index

Articles

Advertiser Listings