RELIABILTY OF PROTECTION SYSTEMS

(WHAT ARE THE REAL CONCERNS)

Jonathan Sykes	Vahid Madani	John Burger	Mark Adamiak	William Premerlani
SRP	PG&E	AEP	GE Digital Energy	GE Global Research
Sr. Member, IEEE	Fellow, IEEE	Sr. Member, IEEE	Fellow, IEEE	

I. ABSTRACT

Protection Systems have a significant role in maintaining the stability and reliability of the electric power grid. Their optimal performance plays a vital role and becomes more critical when the power system is operating near its limits. Protection Systems are used to detect and isolate faults or to arrest adverse conditions that occur on the grid. Subsequently, misoperation of these systems must be kept to a minimum. This paper discusses protection applications and reliability considerations, and methods such as Synchrophasor monitoring of system conditions that can be incorporated into protection schemes to reduce problems stemming from a variety of hidden failure modes and increase the effectiveness and reliability of Protection Systems. The impact of Protection System failures on dependability and security is discussed. Failure modes initiated by Calculation of Settings and Modeling Errors, Firmware issues, and Hardware failures will be analyzed. The various components of the Protection System are described and plausible failures of these components are presented. The use of separate but equivalent (redundant) protection systems is presented to illustrate methods that could increase reliability of the protection systems. This includes a discussion concerning same or different manufacture of protective relays. The probabilities of these failure modes will be presented. The effect of the new NERC guidelines on protection system redundancy is evaluated.

II. INTRODUCTION

Recent newsworthy wide-area electrical disturbances have raised many questions about the causes and cures for such occurrences and have demonstrated the vulnerability of the interconnected power system. The increasing demand for energy has resulted in power grids approaching their limits, and at times blackouts have occurred in parts of a grid as the result of series of unanticipated events. Figure 1 shows the frequency of transmission outages based on data from NERC Disturbance Analysis Working Group (DAWG). The Figure shows approximately 24 outages per year in the United States with curtailments in the 100 to 1,000 MW range, about 5 outages in 1000 to 10000 MW range, and one outage every 4 years at 10,000+ MW, [1]. The large scale outages are not unique to one country or a specific region or part of the world [2], and could be triggered by mechanical failures in the power grid networks or by external forces such as natural calamities (earthquakes, hurricanes) and more recently the threat from human induced damages (e.g. cyber attacks).

“Relays can not start a disturbance” is a common phrase used during the post mortem event analysis. But this is not exactly telling the whole story. Electric Grids are designed and operated to withstand any single (and often double) contingency including a relay misoperation. However, there can be significant impact to the grids operation if a relay misoperation occurs during a contingency (i.e. a fault). In most widespread disturbances, there is usually a misoperation that aggravates the events.

In the last few years we have seen several events in North America, and abroad, that would have been contained if it were not for unanticipated and unexpected protection system performance. Often, the test of properly functioning relaying system is during contingencies or faults. Protection systems (protective relays and associated relay systems) are expected to perform correctly during a grid disturbance. This expectation places a priority in maintaining the highest degree of reliability in the protection systems.

Frequency of Transmission Outages

- **While large-scale outages of over 10,000 MW are relatively rare, there are many events with curtailments in the 100 MW to 10,000 MW range:**

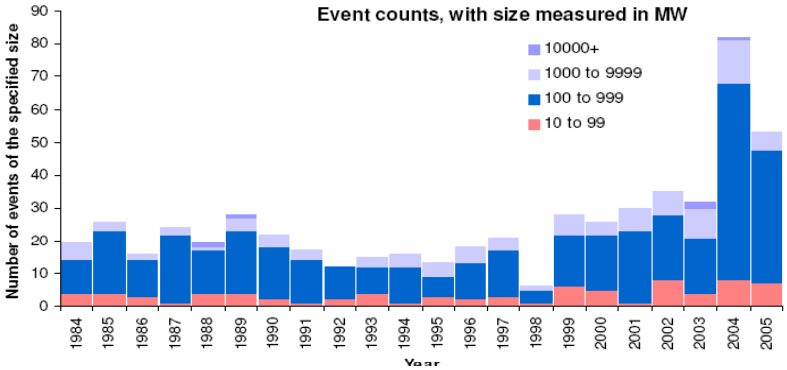


Figure 1 – Blackout Frequencies, 1984-2005, Source: Hines et. al [1]

Protection Systems can also misoperate in the absence of an electrical disturbance and this can impact the availability of facilities and the power company's ability to meet power delivery obligations. Contractual and regulatory requirements can be affected and additional operating solutions may be needed that could cost the owner revenue. Given the ever-increasing drive to maximize use of existing grid facilities, there is a need for an advance warning system that can distinguish the different power system phenomena as well as locate and forecast their movements. To achieve this goal, there is a progressively growing strategy for implementation of wide area monitoring schemes that can adjust and maximize the effectiveness of control and protection decisions.

III. OVERVIEW

The reliability of protection systems needs to consider all factors within the protective device manufacturing, overall system design, maintenance, and setting procedures. The failure to maintain integrity in any one of these areas can lead to a misoperation. The evolution of relays and relaying systems from completely electromechanical (EM) to microprocessor (MP) based relaying has introduced many new challenges for the relay manufactures and practitioners. Microprocessor based relays have extensive hardware and firmware and many more settings than electromechanical relays. The complexities associated with integrated multi-function devices impacts manufacturing and technology development as well as the end users. Even though a single microprocessor relay has many more components than a single electromechanical relay, a EM-based protection scheme will deploy 10 to 15 devices to perform the functions contained in a single MP relay. The failure of any one device can disable the protection system and cause a protection system misoperation. As a result, the overall availability of a microprocessor-based system is greater than a system of electromechanical relays. Given the large component count in microprocessor relays, there is a probability of failure that is a function of the part count. The well-noted benefit of the microprocessor relay is that it can monitor and detect many of these failure modes and issue an alarm. Manufactures provide sound designs with reliable components and place emphasis on internal monitoring of microprocessor health and availability but hidden failures do occur. The undetected failures have been termed "hidden failures" because the type, factory, and commissioning test procedures don't detect them. The reliability of Protection Systems as an aggregate must take into account all failure modes.

Since a single MP relay replaces many EM relays, the new relays may have hundreds of settings as an aggregate of all the devices the microprocessor relay replaces. For example, one relay may have:

- Traditional relay settings (such as impedance and overcurrent settings)
- Pilot communication settings (such and POTT scheme keying and receiving logic)
- Breaker fail and synchronizing settings
- Station LAN relay communications port settings
- Auxiliary tripping and closing functions
- SCADA and RTU interface settings, local alarming and control
- SIPS (System Integrity Protection Scheme) or Remedial Action Scheme (RAS) or Special Protection Systems (SPS) settings
- Remote maintenance port settings.

This integrated application requires a rigorous settings development, installation, and tracking process. The application of MP relays may need "proof of concept" development and type testing, transient simulation testing, commission and acceptance testing, and recording/auditing of the process to insure that incorrect settings do not get installed on relays.

Finally, regulatory compliance measures help asset owners in maintaining a high degree of reliability of protection systems. It is necessary for the utility industry to continue to participate in the regulatory process to provide guidance in the development of industry standards. Regulatory oversight of the Electric Power Industry is necessary to protect public safety and provide power quality, performance, and reliability. To provide consistency in the development of reliability recommendations across the North American continent, the North American Electric Reliability Corporation (NERC) was formed, dating back to after the 1965 blackout. NERC has been tasked with owning and updating standards after the 2003 Northeast blackout. The NERC System Protection and Control Subcommittee has produced a technical paper discussing Protection System Reliability [15], and has started the Standard Authorization Process (SAR) to develop a standard concerning Protection System Reliability in engineering and design. Each utility will need to review and evaluate how Protection System Reliability will impact their ability to meet all the pressures of operating the grid.

IV. PROTECTION SCHEME DESIGN AND IMPACT ON RELIABILITY AND SECURITY

The electric power system is designed to survive the loss of any one element and still function. Protection Systems also need to be engineered and applied to properly detect faults and distinguish abnormal or stressed conditions. Protective systems also need to withstand the loss or malfunction of components or devices and still provide adequate functionality to isolate faults and disturbances. When a fault occurs on the electric system, it is the function of the protection system to detect and provide isolation. It is can be disastrous to the electric system if the protection does not detect and initiate the isolation of the fault. Therefore, protection systems are deployed in such a way that there is a backup system available to isolate disturbances[1]. The rigor in design of these systems depends on performance requirements and the speed needed to isolate a given disturbance.

The overall protection philosophy does not mean that all local schemes need to be completely redundant. The rigor installed in protection schemes is directly associated with the performance required by planning studies. This might mean that remote backup of a local scheme is an acceptable solution to meet performance. The failure

[1] ***Protection System Names:*** *The names applied to the multiple protection systems include: Primary, Secondary, Alternate, Backup, Main 1/ Main 2, Local Backup, Remote Backup, System A and B, System 1 and 2. For the purpose of this paper, the application involves having multiple relay systems combined into an aggregate protection system that provides adequate operation during single component failure. Each of these systems meets the performance requirements, such as minimum clearing times. Backup relaying may provide adequate protection and usually may have less speed and / or less selectivity. This paper differentiates between duplicate and redundant systems as explained in later sections.*

modes of protection systems need to be compared to performance requirements and expectations. The reliability of the protection and control system is a balance between security and dependability. In general, high speed operation requires local schemes to have increased dependability.. The design of a protection scheme has significant effect on the overall performance during faults, disturbances, or other abnormal system conditions. Different protection solutions offer different advantages and disadvantages that need to be considered during the protection scheme design process. Therefore, the delicate balance of dependability and security is the key to a robust design.

Asset value and facility availability are other reasons the owners require protection systems to be very dependable. High voltage transformers for example, are expensive and have long lead times on delivery. Therefore, it is prudent practice to minimize exposure to fault conditions and not rely on delayed clearing for a primary protection system failure. In addition, long-term loss of this device could cause an extensive and expensive operating solution such as re-dispatch of additional generation and delaying of other scheduled outages. Both of these examples are reasons that owners would deploy multiple level protection systems to protect transformers with a high degree of dependability. Other facilities such as buses, large generators, DC valves, SVC, and series capacitors also have long lead-times and represent extensive capital investment - again identifying the need for a delicate balance between dependability and security.

The requirement for reliability is typically satisfied by increasing the number of protection devices, thus ensuring that even if there is a failure of one or more relays, the fault will still be detected and cleared. Using devices with different hardware and software designs as well as diversified operating principles further improves the reliability of the scheme, by reducing the probability for a common or hidden mode failure. In such applications, all devices operate in an OR logic scheme. However, keeping in mind that different protection functions might be susceptible to misoperation under certain abnormal conditions, if just one of the relays in the protection scheme operates, it will result in an undesired trip of a transmission line that may lead to further deterioration of the system stability. To improve the security of the protection scheme in an over-trip situation, some applications implement voting schemes. A typical arrangement is a 2-out-of-3 vote. In order for a trip output to occur, at least two of the three protection devices have to detect the fault. Such logic eliminates "undesired" output activation in the case of a single relay misoperation. However, one should keep in mind that in some cases when two of the relays operate, the operating time of the scheme would be determined by the slower relay. This has to be taken into consideration when selecting the individual relays to be used in order to avoid any potential stability problems due to delayed clearing of the fault. Such schemes should also address a "fail safe" mode of operation. Examples:

- When the two different systems (overall voting scheme) identify two different types of faults.
  - ❖ Correct fault identification (characteristics and location) impacts the overall scheme performance.
  - ❖ Automatic equipment restoration is affected by the identified fault type of the overall voting scheme. Multi-phase (vs. single phase) line faults may result in slower reclosing for momentary faults.
- When a portion of the voting scheme fails during a fault detection, or fault clearing, or when one level of protection is out of service for scheduled work.

V. PROTECTION RELIABILITY, HIDDEN FAILURES & UNINTENDED OPERATIONS DETECTION

A. Protection System Reliability -

There are two facets to Protection System reliability: dependability and security as defined by IEEE standard C37.100–1992 and are shown below (see figure 2):

- Dependability — "The facet of reliability that relates to the degree of certainty that a relay or relay system will operate correctly." For purposes of this paper, dependability is a measure of the degree of certainty that a protective system will operate correctly when required, and at the designed performance. Dependability is a concern when a fault occurs within the protected zone.
- Security — "That facet of reliability that relates to the degree of certainty that a relay or relay system will not operate incorrectly." For purposes of this paper, security is a measure of the degree of certainty that a

Protection System will not operate incorrectly. Security is a concern for external faults, normal (unfaulted) or stressed operating conditions.

The availability of protective relays for proper operation during any system conditions is one of the most important factors that can help reduce the risk of cascading disturbances following a fault or any other system event. 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 [3]. Detecting and compensating for hidden failures is a critical task that requires a good understanding of the principles of operation of the protective devices, their self-checking functions and their limitations [4].

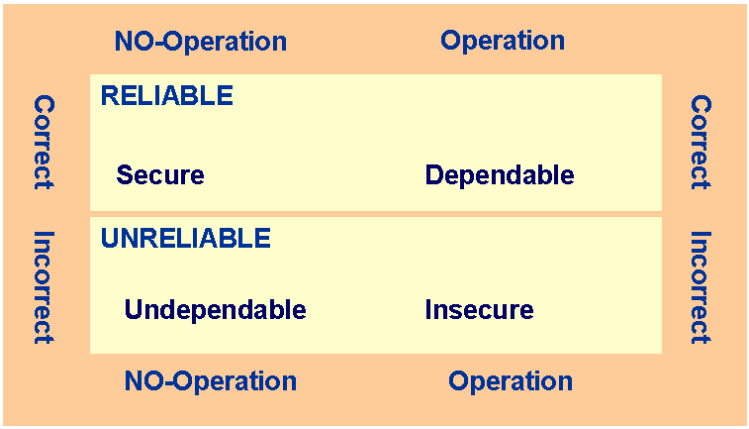


Figure 2 - Definition of Protection Reliability [3]

Application of new technologies (e.g. Synchronized Phasor Measurements) could help mitigate undesirable response of devices due to hidden failures in advance, by monitoring system changes affecting settings and thus provide early warnings. Figure 3 and 4 are simplified diagrams describing the application of PMUs in connection with balancing security / dependability. Under normal conditions, each level of protection operates independently, Figure 3. When the stressed system state (or the actual phasor quantities) corresponding to impending out-of-area trouble is communicated (through the phasor data concentrator) to the protective relays for a particular relay system or relay systems in a particular corridor, the protection for the respective piece of equipment (e.g. line protection) would change from an "OR" function to an "AND" (or voting) function. Note this concept requires sufficient levels of protection systems - each capable of accepting status information and designed to support voting conditions [16]. This application requires determination of triggering logic for the protection system. The triggering logic may be as simple as a line fault coupled with the probability of a hidden failure in the study area.

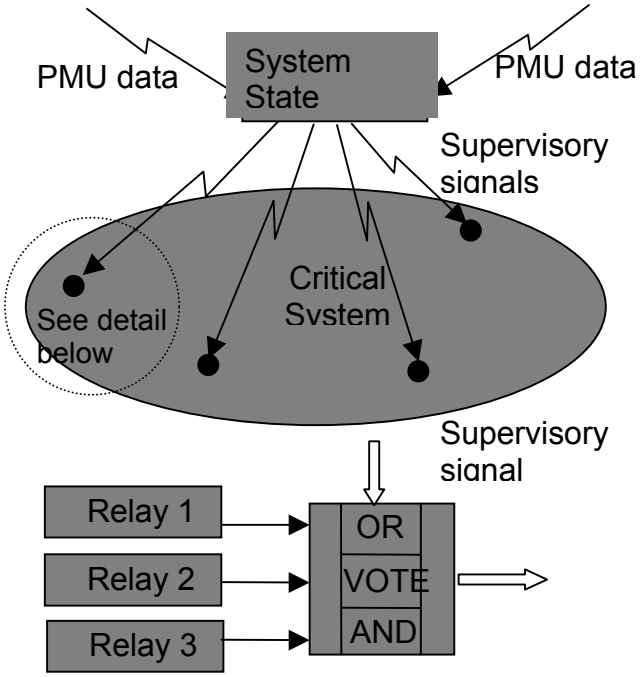


Figure 3 - Adjustment of Dependability-Security balance under stressed system conditions, [16]

Figure 4 reflects another application of PMUs to determine balance of security / reliability [17]. In this example, the relay settings are evaluated in connection with the PMU data (initially off line in the PDC). Alarms are generated, when the relay settings are identified to be out of tolerance or impedance characteristics are approaching load conditions, notifying system operators and protection engineering staff that relay settings need to be looked at and updated [17].

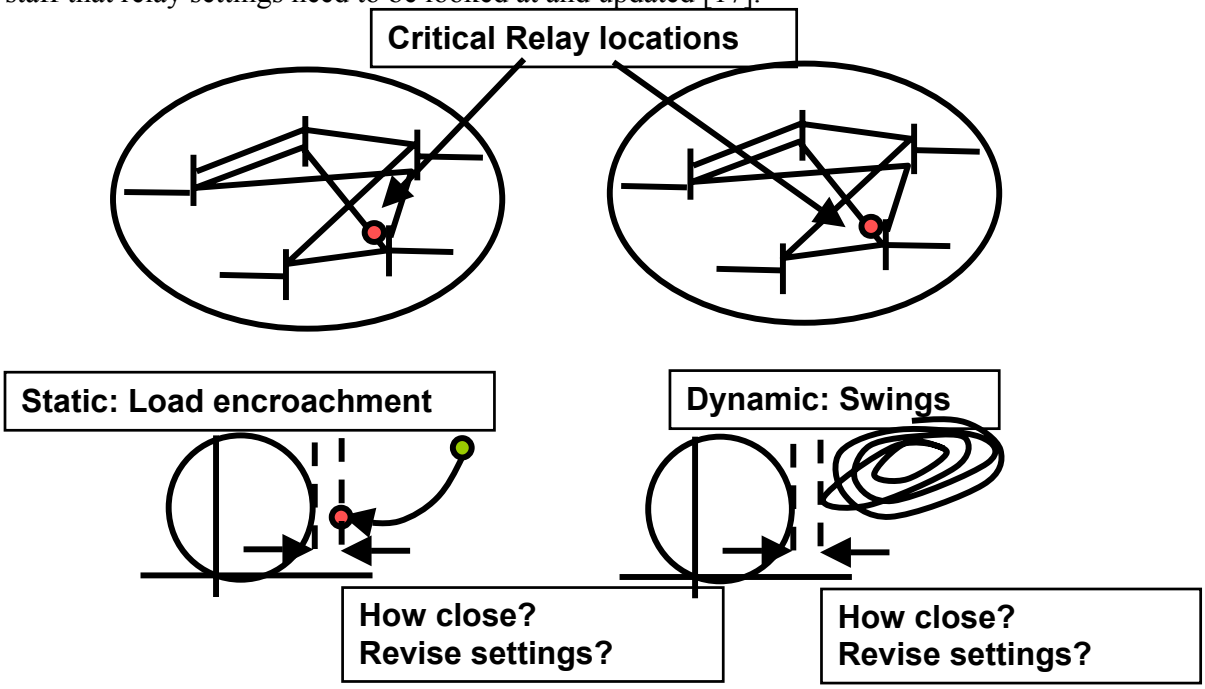


Figure 4 – Monitoring Vulnerability of Relay Settings Using Phasor Data

B. Hidden Failure Modeling and Analysis - Modeling techniques allow estimation of:

- Component in Failed Condition and Undetected (trip coils, stuck pole, etc.)
- Component Failure Due to Unexpected Operating Stress (Example: CT driven to saturation, induced voltage on pilot wire, etc.)
- Component Failure Due to Unexpected Transients

Protection Reliability Indices such as protection insecurity or dependability can also be assessed by detailed modeling of the protection and control system including the probabilistic analysis of hidden failures [10], [13].

C. Monitoring of 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.

A failure of a protective device to perform correctly may also result from incorrect settings. Setting errors may be caused by calculation error, incorrect instrument transformer parameters, inaccurate power system model, or when transferring settings to the protective relay. Verification of the models used in any analysis or coordination software thus becomes very important. Comparison of the fault records from protective relays with simulations of the fault in the analysis tool can be used to evaluate the accuracy of the model. Manual or automatic comparison of a setting file and the settings uploaded from the protection device can detect errors in the actual relay settings.

Relay misoperation may also be caused by failures in the analog (current and voltage) circuits of the protective device. Modern protective relays are typically equipped with voltage and current circuit supervision schemes and continuous monitoring of sources. The voltage transformer supervision (VTS) feature is used to detect failure of the ac voltage inputs to the relay, which may be caused by internal voltage transformer faults, overloading or faults on the interconnecting wiring to relays, or fuse failure.

Furthermore, augmented relay capability and complexity are important trends that need to be addressed. The complexity of implementation, maintenance, testing, and verification of applied relay settings has increased significantly in recent years due to:

- Multi-function devices
- A large number of options (e.g. multiple setting groups)
- Different approach by each vendor

D. Other Protection Related Contributing Factors:

When the electrical system is operated at or near its design limits, any deficiency in settings, testing, application may become a significant contributing factor to a large-scale cascading outage depending on the severity of the disturbance. Hence, the need for comprehensive protection and control studies and overall protective scheme testing is once again highlighted and the benefits of redundant protection systems become more apparent. Some examples of protection and control contributing factors:

- Use of protection set point criteria developed from a fault clearing prospective for generation or transmission equipment, without considerations for the power system operating near its limits
- Application of impedance based protective devices without the Out-of-Step recognition algorithm, where Zone 1 may operate.
- Generic breaker failure timer set points without performing system studies
- Generic switch-on-to-fault set points responding to voltage collapse
- Generic closing angle set points for restoration devices
- Use of type test results for instrument transformer as opposed to field testing

- Use of type test result from protective relay manufacturer as opposed to comprehensive system simulation testing
- Incorrectly routed telecommunication circuits. For instance, a microwave based protection system when a channel card at one of the repeating stations, is setup to loop back the signal to the transmitting station, demonstrating the importance of loop back monitoring and alarm systems either within the protective relay systems, such as current differential or phase comparison, or within the tele-protection portion of the communication path. Closed loop field tests using COMTRADE generated files would be the best method to detect this type of hidden failure on initial startup and the systematic scheduled tests.
- In-depth understanding of protective relay operating principals for the main and peripheral protection functions. For example, backup elements in a differential operating principal protective device.

Use of generic set points for auxiliary devices and timers have added value in terms of consistency within the terminals in a station or throughout the owner's system, uniformity in application, ease of record keeping, expediting fault analysis, as the investigation requires less consultation of records, etc. However, generic set points are not well suited when the system is operating close to its limits.

One other type of failure could be in the test methods used. For example, inadequate test procedures in testing auxiliary tripping devices have resulted in EHV line faults near large power plants not to clear in time resulting in a cascading wide area outage [12].

VI. PROTECTION AND CONTROL APPLICATIONS, TESTING, AND REDUNDANCY CONSIDERATIONS

From the reliability perspective, selection and application of protective relays goes hand-in-hand with testing. Initial tests may be product selection tests, followed by a series of application and performance tests, and later installation and commission testing. A variety of methods have been used for protective device performance testing from use of high-power model power system tests, to Transient Network Analyzers, to today's digital simulators. Open and closed looped testing for more complex applications of line protection is also prescribed by many practitioners. In the most critical applications, these devices may interact over an extended physical or geographic area and utilize extensive communications systems from multiple owners. IEEE has also published a Guide that provides a comprehensive approach and specific procedures for testing protective relaying systems that include multiple interacting relay components, auxiliary devices, and power apparatus [5]. The procedures in the IEEE Guide focus separately on design testing, commissioning testing, routine maintenance testing, and ongoing performance assessment with discussion of what each of these test categories aims to accomplish.

Another aspect of protection and control system reliability is the application of devices and the redundancy philosophy including the overall system design that may vary among power companies. To a certain extent, the protection and control application philosophy of a power company may be based on several factors unique to the environment of the system that has been designed. Factors such as the geographical diversities, transmission system design, feasibility of having diverse communication paths, experience of the individuals working on the system, etc. each influence the decision on the level of redundancy. Additional factors such as load growth and available natural resources to run major generation plants uniquely influence power system design. Finally, operation practices may influence schemes designed to protect the power system integrity. Hence, each system may be designed or operated differently yet still be expected to meet minimum reliability standards [6].

In general, most practitioners consider a redundant system one in which failure of a single element or component will not impact performance of the aggregate protective system. Redundancy in selection and application is a common approach. However, different views are exercised in the definition of redundancy and redundancy is not same as duplication. A redundant system uses diverse hardware platforms, diverse communication routes, diverse operating philosophies in measurements and detection, and independent DC sources. A duplicate system on the other hand has identical major non-diverse components. While a duplicate system may facilitate maintenance activities, it has distinct differences from a redundant protection system. A duplicate system has many components and operating principals of the original system, and therefore is likely to have same design, same scheme, and will probably have the similar protection set points as the first protective scheme making the engineering and design a non-diverse application and increasing the probability of common mode errors.

The application of different platforms of protective relays between primary and alternate protection schemes requires:

- In-depth understanding of the operating principals for each of the redundant technologies
- Different operating principals require different types of system studies, hence requiring more comprehensive coordination between settings of redundant systems
- More comprehensive review of overall system design and applications
- More systematic approach to the application of technology
- Balancing maintenance practices and overall asset strategy.
- Different methodologies for testing and overall performance evaluation

The complexities in the use of microprocessor protective devices coupled with advancements in acceptance and prototype testing, described earlier, have made the benefits of a "redundancy" philosophy less transparent to many power system professionals, and has generated a healthy debate over pros and cons over what "Redundancy" in application means to different individuals or systems. The protective relay manufacturer-provided "turn key" solutions also drive the type of "Redundancy" or "Duplication" applied when the customer specification is not specific enough to require true redundancy.

While there are numerous reasons one can list in terms of the benefits of a duplicate protection system vs. a complete redundant protection system (including different platforms) in protective device application, it can be numerically shown that with the existence of hidden failures, the application of protective devices from different manufacturers best support the conventional theory and definition of redundancy. This assumes that factors such as equipment maintenance frequency, manufacturing services and support, and environmental exposure are at comparable levels. When properly studied and applied, in almost all cases, a complete redundant protective system offers lifetime benefits over a duplicate protection and has the added advantages of technology and asset strategy beyond a duplicate system. Redundant systems also provide more interactive system design and provisions for more comprehensive system testing since the operating principals are completely independent. A duplicate system has the potential for performing poorly on both systems for example for an out-of-section fault. A true redundant system also offers the possibility of identifying or detecting faults that may go undetected (hidden failures) when using duplicate protective devices as alternate level protection.

Protection is often referred to as an insurance policy. Hardly any corporation would invest in duplicate insurance policies from the same company regardless of the comprehensive coverage level, types of services provided, or the reputation of the insurance company.

VII. Probability Model of Relay Redundancy Options

The previous sections have presented a qualitative overview of relay redundancy options. It is possible to provide a quantitative evaluation of relay redundancy options based on the probability of the

existence a "Hidden Failure" in a particular relay. This section looks at the effect of a Hidden Failure on both Dependability and Security.

Effect of Hidden Failures on Dependability
In a dependability view of operation, the concern is that a system does not operate for an in-zone fault. Given relays from two different manufacturers, R-M1 and R-M2, the probability of a hidden failure manifesting itself in each of these relays during a fault or a system disturbance is defined as:

- $P[R\text{-}M1_{HF}] = x$ – the probability that a hidden failure in a relay from manufacturer M1 will be uncovered by an event

- $P[R\text{-}M2_{HF}] = y$ - the probability that a hidden failure in a relay from manufacturer M2 will be uncovered by an event

Where "x" and "y" are some non-zero values – as evidenced frm analysis of major power system blackouts.

It can be argued that the probabilities of failure of relays from different manufacturers - due to hidden failures – are independent events. As such, the probability of both manufacturers' relays failing due to a hidden failure being exposed is:

> $P[SysFail\text{-}Dependability] = P[R\text{-}M1_{HF}] * P[R\text{-}M2_{HF}]$, *Hidden Failure probability of two devices from different manufacturers*

Whereas, if two relays from the same manufacturer, say M1, are used in a scheme, the probability of a hidden failure being exposed is not independent and the probability of a system failure is:

> $P[SysFail\text{-}Dependability] = P[R\text{-}M1_{HF}]$, *Hidden Failure probability of two devices from same manufacturer*

In all cases, even if the probability of a hidden failure from a given manufacturer is small, the probability of a common mode hidden failure in a single manufacturer's relay being exposed is always greater than common hidden failures existing and being exposed in two different manufacturer's relays.

Effect of Hidden Failures on Security
The security of a relay system is based on a relay not operating when it should not. In this case, a hidden failure would result in an over-trip of a relay system. In a conventional "OR" relay system, the probability of a hidden failure results in an undesired trip is:

$P[SysFail\text{-}Security] = P[R\text{-}M1_{HF}] + P[R\text{-}M2_{HF}]$ – that is, the probability of a system security failure is the sum of the probabilities of a hidden failure in each relay

As mentioned, earlier, the security of a protection system can be enhanced through the use of a 2 out of 3 voting scheme. In this model, the probability of an over-trip for independent devices is computed as:

$P[SysFail\text{-}Security] = P[R\text{-}M1_{HF}]*P[R\text{-}\mathbf{M2_{HF}}] + P[R\text{-}M1_{HF}]*P[R\text{-}M3_{HF}] + P[R\text{-}M2_{HF}]*P[R\text{-}M3_{HF}]$

With M1, M2, and M3 being independent devices then the probability of a system failure due to an over-trip is greatly reduced. Similarly, if any of the relays are not independent, there is a probability of common-mode failure mechanisms. As such, the probability of a false operation becomes the sum of the probabilities:

$P[SysFail\text{-}Security] = 3*P[R\text{-}M1_{HF}]$

Example Calculation the effect on a Hidden Failure on Dependability:

- Manufacturer #1 has a probability of a hidden failure of 0.1% (or .001)
- Manufacturer #2 has a probability of 1% (or .01)

The probability of a system failure due to hidden failures in both devices is:

$P[SysFail\text{-}Dependability] = .001 * .01 = .0001$

With both primary and alternate protection from the same manufacturer, the overall probability of a system failure due to a hidden failure is equal to the probability of a single device failing or .001 - which is 10 times greater than the probability of a system failure due to independent hidden failure events.

Addressing Hidden Failure Modes in Achieving System Reliability

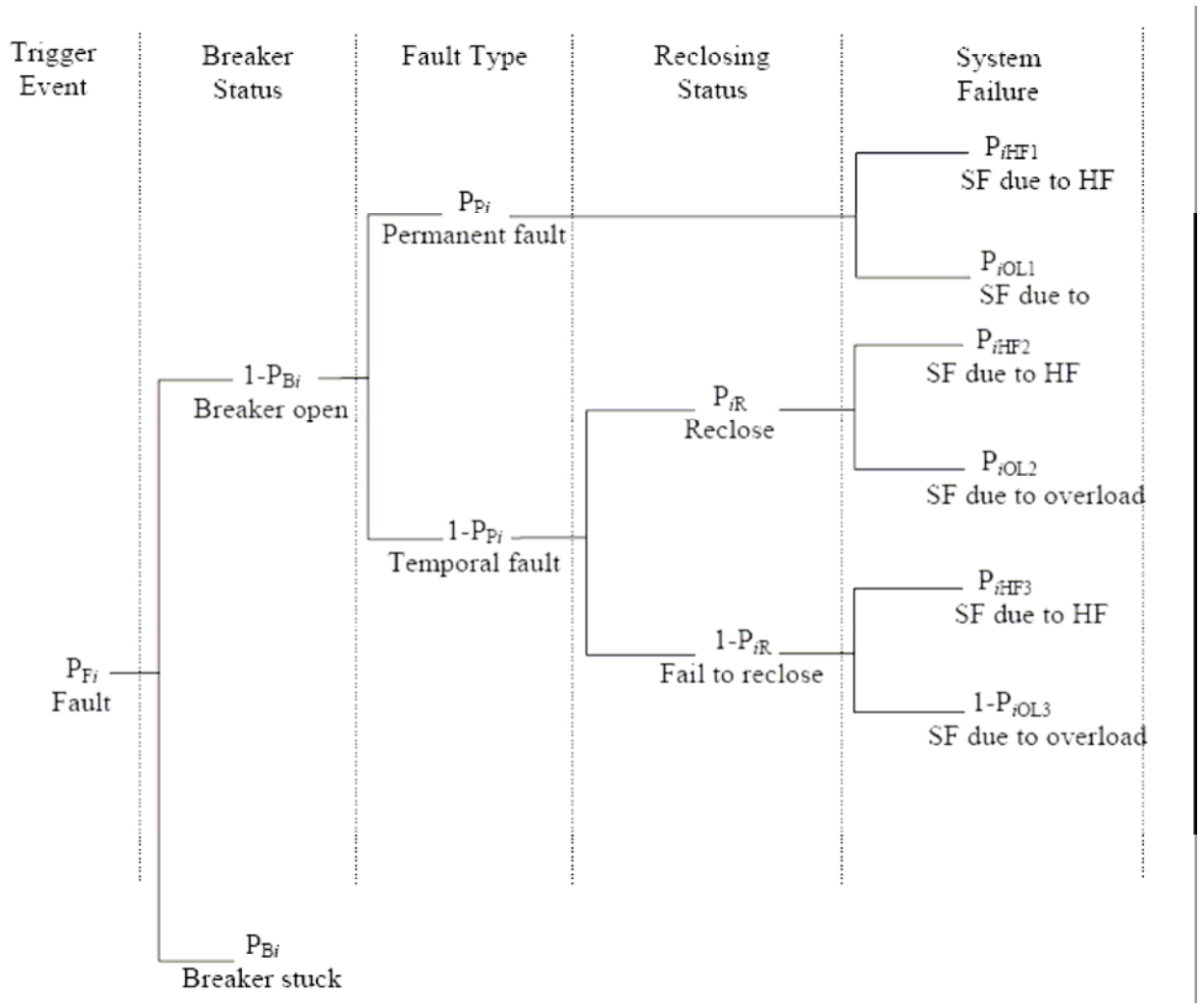
Reliability Cantered Maintenance (RCM) is not new, [7]. Airline Maintenance Steering Group (MSG) Logic, the predecessor to RCM, has existed since the early 1960s. Stanley Nowlan and Howard Heap of United Airlines introduced formal RCM to the commercial aviation industry in 1978. Airline reliability is primarily based on this work. The vision is as relevant today as it was when the first edition of Reliability Centered Maintenance was published in 1978.

Today, almost everyone in a manufacturing, power systems, or technological environment is familiar with the concept of RCM. However, the degree of familiarity or the level of RCM application varies with RCM based on the criticality of the system. For example, RCM application at a nuclear plant in comparison to the power grid type RCM. In their ultimate applications, the two should be the same. RCM is simple in concept but also sophisticatedly subtle in its application. The true reliability benefits of RCM become evident only with a thorough understanding of how to functionally analyze a system. Understanding hidden failure modes, understanding when a single-failure analysis is not acceptable, and understanding when run-to-failure (RTF) is acceptable, are the real cornerstones of RCM. Additionally, the subtle but important distinction between true redundancy and redundant components fulfilling a backup function is also a key to reliability success.

Prudent industry practices call for proper testing and verification of protective equipment performance over its life cycle. Most owners have established extensive maintenance programs for protection systems and follow these programs closely to maintain reliability. Microprocessor based and self-monitoring relaying systems provide the owner an opportunity to optimize and extend the maintenance cycles by using condition based maintenance programs.

As stated previously, local redundancy of protection systems may not be required if performance does not warrant it. This would mean that the backup or remote system provides the surrogate function of the redundant protection system. These backup systems would need to be maintained with the same rigor as the primary system.

Fault Tree Analysis (FTA) is another tool originally developed in early 1960's by Bell Labs for use in studying failure modes in the launch control system. The tool now finds wide use in numerous applications from accident investigation to design prototyping and is also finding use for protection and control related applications, [10,13]. A Probabilistic Event tree as identified in [13] for a Power System failure is shown in figure 3.



Mean Time to Failure

The mean time to failure (MTTF) of a device refers to the mean (average) time from when the device is first put into use until it fails for the first time in the case of a device that is not repairable. For a repairable device, the Mean Time Between Failure (MTBF) is an average time the device is operating. This quantity can be described as a period of time, a number of operations, or a distance driven. The MTBF and MTTF are expressed in units of time. The Mean Time To Repair (MTTR) of a device is the average time that the device is unavailable. It is the "down time" of the device while the device is being repaired.

The strict definition of the MTBF is the sum of the MTTF and the MTTR, however, for most power system components the MTTR is usually quite small compared with the MTTF and the assumption is

often made that the MTBF is the same as the MTTF.

The failure rate is the probability that a device will fail in a period of time Δt (from time "t" to time "t + Δt ") for instance, given that the device was functioning properly up to point "t". Often, the failure rate is dependant upon how long the device has been functioning – usually, it is not a constant at every point in time. The failure rate of a device is its "proneness" to failure after a given time has elapsed.

For the majority of power system components, the failure rate is best described by the "Bathtub" curve, as shown in Fig 3. When a device is first installed, there is a burn-in period with a high likelihood of failure (high failure rate), area I in Fig. 3. As the device is in service for some time, the failure rate levels off (area II), then becomes high again during the end of its useful life (area III). For simplicity, the failure rate is usually expressed as a constant and is equal to the total number of units that failed over the total in-service time of the units.

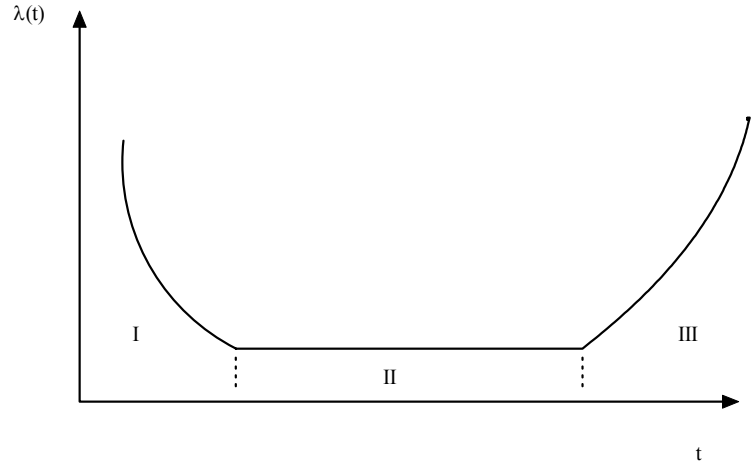


Fig. 4. Bathtub Curve - Showing Failure Rate

An important feature of the Fault Tree method is that it is capable of accounting for mixed reliability attributes (failure rates mixed with failure probabilities).

Relay reliability is often measured in terms of MTBF. Relay practitioners should work with their relay vendors to understand how each vendor computes this value. Additionally, the MTBF number must be augmented with an end-of-life evaluation because, independent of the failure rate in area 2 of the Bathtub curve, the utility owners need to have an understanding of when to expect the End of Life (area III) for a device.

Component Failure Rate Data

Several sources of data exist for obtaining failure rate data; unfortunately very little publicly available data exists for application in the field of protection and control. However, as noted above, some manufacturers can provide reliability figures for their devices.

One of the primary resources for failure rate data information is Military Handbook 217F, which has failure rate data for numerous components. It contains information on how to obtain reliability data by evaluating various equations [9]. For obvious reasons, failure analysis is a vital activity in military or aerospace endeavors. This is one method of obtaining failure rate information that can be used for discrete components and auxiliary relays.

There is some controversy about using the methodology given in MIL HDBK-217F as it gives very conservative results. On the one hand, it is convenient to use and freely available, on the other hand, it

may not be totally applicable to each device or it may not be derived in the best means suitable for the particular analysis at hand.

Failure rate data can be obtained via the following means:

1. Based on actual experience with the component
2. Based on actual experience with a component having a similar design
3. Life testing on the actual component
4. Life testing on a similar component
5. Field or test data from the component supplier
6. Specialized database
7. Standard handbook for reliability data (such as 217F)

Conclusion:

Along the path of reaching higher levels of reliability while maximizing the use of assets, many critical contributing components of power system operation need to be studied and prudent investments in technology for hardware and tools should be considered. In the case of the recent widespread blackouts, the design and operation of conventional protection and control schemes have been scrutinized. From this analysis there is clear evidence that conventional protection systems that operate solely through the local measurements are often unable to adjust control actions based on the condition of the power system.

This paper covers some of the key considerations in selection and application of protective relaying, explores dangers of hidden failure, and describes differences between duplicate and redundant protection systems. Protection Systems are an important and integral part of system reliability and asset owners should show good stewardship over the selection and application and overall asset strategy. Part of being a steward of the asset includes making sure the performance meets expectations. This practice includes monitoring and mitigating failures of the hardware and software and in work processes such as setting development and implementation. Protection Systems must be designed with the appropriate reliability to meet the performance requirements of the electric system but also the individual requirements of the asset owner. Following sound practices requires that asset owners monitor and observe regulatory guidelines and standards. The regulatory requirements offer overall reliability benefits and the impact of these regulatory compliances are of outmost importance to achieve common levels of reliability. In addition, owners will also have to recognize when to exceed these requirements and there are many reasons that will drive the decision. The settings and programming of the protection systems will need to have the proper rigor and oversight necessary to insure that errant settings are not introduced. Duplicate protection systems may require less overall Engineering, design, and training to set and maintain, however, a duplicate system may not provide the highest level of reliability. One of the biggest reliability concerns of our industry is the skill of the individual stewards of this business and a “relaxed skill set” does not necessarily translate to increased reliability for the future. As we build a bridge from the present to the future, owners will need to maintain the complete set of skills needed to understand all facets of implementation and application of protection systems. Finally, it will be necessary for owners to recognize that new techniques and equipment such as synchrophasors may require new applications, schemes, and training to meet the requirements of the future. Owners should be ready to deploy these devices and techniques as the opportunity appears.

References

1. Hines, Apt, Liao, Talukdar; The frequency of large blackouts in the United States electrical transmission system: an empirical study, Carnegie Mellon, 2006
2. V. Madani, D. Novosel, “Getting a Grip on the Grid”, IEEE Spectrum Magazine, December 2005.

3. V. Madani, D. Novosel, P. Zhang, S. Meliopoulos, R. King, "Vision in Protection and Control Area Meeting the Challenges of 21st Century" – IEEE PES Power System Conference and Exposition, October 2006
4. S.H. Horowitz and A.G. Phadke, "Boosting Immunity to Blackouts," Power and Energy Magazine, September/October 2003.
5. IEEE C 37.233 Guide for Power System Protection Testing, 2009
6. C. Henville, E. Struyk, "RAS and Stretched Power Systems", Western Protective Relay Conference, October 2006
7. N. Bloom, "Understanding Hidden Failures in RCM Analyses" Maintenance Technology Publication, January 2003
8. V. Madani, D. Novosel, A. Apostolov, S. Corsi, "Innovative Solutions for Preventing Wide Area Disturbance Propagation", International Institute for Research and Education in Power Systems (IREP) Symposium Proceedings, August 2004.
9. V. Madani, R. King, "Strategies to Meet Grid Challenges for Safety and Reliability", International Journal of Reliability and Security (IJRS) InderScience Publishing – Special Publication; Volume 2, Nos. 1/2, 2008
10. R. Beresh, J. Ciufo, G. Anders, "Basic Fault Tree Analysis for use in Protection Reliability", International Journal of Reliability and Security (IJRS) InderScience Publishing – Special Publication; Volume 2, Nos. 1/2, 2008
11. MIL-HDBK-338B, "Military Handbook - Electronic Reliability Design Handbook," 1 Oct, 1998 Available: http://www.weibull.com/knowledge/milhdbk.htm.
12. "Guide for the Application of Protective Relays Used for Abnormal Frequency Load Shedding and Restoration", Working Group C-9 IEEE PC37.117, System Protection Subcommittee, IEEE PES Power System Relaying Committee, May 2004.
13. Q. Qiu, Risk Assessment of Power System Catastrophic Failures and Hidden Failure Monitoring & Control System, PhD Dissertation; Virginia Tech University; December, 2003.
14. NERC website About NERC, Company Overview, History: http://www.nerc.com/
15. NERC website About NERC, Committees, System Protection and Control Subcommittee: http://www.nerc.com/docs/pc/spctf/Redundancy_Tech_Ref_1-14-09.pdf
16. J. Thorp, E. Bernabeu, Adaptive Security and Dependability with PMUs, proceedings of the Innovations in Protection & Control for Greater Reliability Infrastructure Development (i-PCGRID-2009), March 2009, San Francisco.
17. A. Phadke, Wide Area Measurements for Improved Protection of Power Systems, proceedings of the Innovations in Protection & Control for Greater Reliability Infrastructure Development (i-PCGRID-2009), March 2009, San Francisco.

Biography

Vahid Madani is the primary architect and developer of standards in protection and control integration applications and substation modernization at Pacific Gas and Electric Co. (PG&E). His responsibilities include:

- Protection and control standards development and equipment evaluation for PG&E
- Development and application of synchronized phasors for precision protection, integration of phasor data into RAS, wide-area monitoring and disturbance prevention
- Integration of protection and control, automation and applications of UCA and IEC-61850
- Situational Awareness, system visibility, and smart restoration techniques
- Technology and innovation Lab– exploring practical modernization while working with vendors and consultants
- System Integrity Protection (SIPS) and Remedial Action Schemes (RAS) - Currently implementing advanced applications in RAS and Disaster Recovery Systems.

Vahid is a Fellow of IEEE, is a Tau Beta Pi member, and a registered Electrical Engineer with more than 25 years of academic and utility experience and recipient of many honorary and distinguished citations, for his leadership, inventiveness and contributions to the power system industry and education. He has various technical, advisory, and leadership roles in North America and internationally, and has contributed to the development of many advanced applications (Theory & Implementation) in System Protection and intelligent restoration.

For a decade, He served as Chair of the WECC RAS Reliability Subcommittee and received the best Chair Person award for his leadership in the Remedial Action Reliability Subcommittee. He Chairs the Performance Standards Task Team within the North American Synchrophasor Initiative (NASPI), and has authored more than 60 publications in transactions and refereed international journals in system automation, protection & control applications, and practical wide-area monitoring systems with advance warning and fast restorations.

Jonathan Sykes is the Manager of System Protection at Pacific Gas and Electric Company in Oakland California. Jonathan graduated from the University of Arizona in 1982, is a Professionally Licensed Electrical Engineer, and has over 26 years of engineering experience in System Protection. He is active on several committees in the Western Electric Coordinating Council and is Vice Chairman of the North American Electric Reliability Corporation System Protection and Control Subcommittee. Jonathan has authored and co-authored papers for conferences and publications and is an active member of IEEE and regularly contributes to the Power System Relay Committees. Jonathan has been involved in EHV protection and control for over 10 years and established standards in EHV relaying and SPS/RAS design and implementation. Jon has been active in NERC and WECC standards interpretation and development and is a subject matter expert in the interpretation of various protection and critical infrastructure related standards.

Mark Adamiak is the Director of Advanced Technologies for GE Multilin and is responsible for identifying and developing new technology for GE's protection and control business. Mark received his Bachelor of Science and Master of Engineering degrees from Cornell University in Electrical Engineering and an MS-EE degree from the Polytechnic Institute of New York. Mark started his career with American Electric Power (AEP) in the System Protection and Control section where his assignments included R&D in Digital Protection and Control, relay and fault analysis, and system responsibility for Power Line Carrier and Fault Recorders. In 1990, Mark joined General Electric where his activities have ranged from advanced development, product planning, application engineering, and system integration. Mr. Adamiak has been involved in the development of both the UCA and IEC61850 communication protocols, the latter of which has been selected as a NIST Smart Grid protocol. Mark is a Fellow of the IEEE, a member of HKN, past Chairman of the IEEE Relay Communication Sub Committee, a member of the US team on IEC TC57 - Working Group 10 on Utility Communication, the US Regular Member for the CIGRE Protection & Control study committee, a registered Professional Engineer in the State of Ohio and a GE Edison award winner for 2008.

Dr. William Premerlani is a recent retiree from GE's Global Research Center in Schenectady, New York and a holder of over 20 patents. His research interests are in phasor measurement, advanced algorithms for diagnostics and protection, with applications to motor diagnostics and power system relaying. Other recent work have included object - oriented technology, with application to achieving interoperability among communicating intelligent devices in power systems. He is a co-author of the popular textbooks: "Object Oriented Modeling and Design" and "Object-Oriented Modeling and Design for Database Applications".

John F. Burger is a staff engineer and a supervisor of Protection and Control Asset Engineering at AEP. John has a BSEE and MSEE and is a Professional Engineer in Ohio and New Jersey. With over 35 years experience in station and line relay protection and control, he has worked at AEP, primarily in Protection & Control, for 29 years. John currently has responsibilities for developing protection, control and automation standards, application guides and supporting the relay setting project work. He is an IEEE Senior Member, past chairman of the PES Columbus Chapter, and currently serving as Board Chairman of the UCA International Users Group. As chairman of a PSRC Working Group on the application of IEC 61850/UCA2 he led the group in issuing an award winning report titled "Application Consideration of IEC 61850/UCA2 For Substation Ethernet Communication"