Life Cycle Experiences with Micro-processor Based Relays and Roadmap to Sustainability

Vahid Madani - Pacific Gas & Electric Co.
Yujie Yin – Quanta Technology
Yong Fu - Mississippi State University
Sudhakar Chidurala - American Electric Power
Xiangmin Gao - GE Grid Automation
Jonathan Sykes - Pacific Gas & Electric Co.

***Abstract*— Microprocessor based protective relays have been widely used to provide many benefits including system performance, monitoring, technology and compliance. Recently utilities have started to replace earlier generation of microprocessor-based protective devices with modern protection and control Intelligent Electronic Devices (IEDs). The upgrade is partially due to increased failure rates of the earlier generation of devices, as well as to benefit from the new functionalities including system integration, Synchrophasor applications, IEC61850 communication and cyber security. The process to upgrade numerical relays is quite different and is more complex than upgrading of traditional electromechanical or solid-state relays with a functionally equivalent device. In addition to the hardware replacement, functions related to cyber security, protection, automation and control, event recording and digital communications must be considered. The protection and control system practitioners need to manage the asset and set the strategies, with inputs from other stakeholders across lines of business as well as externally with manufacturers, regulators, consultants or even neighboring utilities because the selection and application criteria have expanded with the introduction of new features and functions.**

This paper discusses the existing asset management, performance, replacement, and technology considerations based on utility practices at the T&D level. Strategies and practical concerns including hardware and firmware compatibility, protection settings, or other features such as automation or other possible functions integrated and associated set point considerations, as well as commissioning and testing when upgrading or replacing a microprocessor device are described in detail. This paper will assist utility or industry electrical engineers that have an on-going relay upgrade project or are planning to upgrade their aging microprocessor relays in lessons learned from some major power companies in North America.

Key Words— Sustainability, Upgrade Strategy, Asset Management, Microprocessor Relays, IED, Protection and Control

ACRONYM LISTING:

Acronym	Definition
BES	Bulk Electric System
CIP	Critical Infrastructure Protection
CPU	Central Processing Unit
DER	Distributed Energy Resources
DFR	Digital Fault Recording
DNP	Distributed Network Protocol
DSP	Digital signal processing
EM	Electromechanical
GPS	Global Positioning System
HMI	Human Machine Interface
ICMP	Internet Control Message Protocol
IED	Intelligent Electronic Devices
IT	Information Technology and Related Network
LAN	Local Area Network
LCD	Liquid Crystal Display
MTBF	Mean Time between Failures
NERC	North American Electric Reliability Corporation
NTP	Network Time Protocol
PMU	Phasor Measurement Unit
PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol
RADIUS	Remote Authentication Dial-In User Service
ROCOF	Rate of Change of Frequency
RTDS	Real-time Digital Simulator
RTU	Remote Terminal Units
SAIFI	System Average Interruption Frequency Index
SAIDI	System Average Interruption Duration Index
SCADA	Supervisory Control and Data Acquisition
SCT	System Configuration Tools
SOE	Sequence of Events
TCP	Transmission Control Protocol
PP	Power Profile
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

I. INTRODUCTION

Microprocessor based relays, or in a boarder term, Intelligent Electronic Devices (IEDs), have evolved over time in hardware and firmware with new features, functions and increased capabilities. Today, IEDs are the preferred solution in green field or retrofit projects to replace the older electromechanical (EM) or solid-state relays in majority of applications. Over the years, the desire for improved efficiency and reliability has placed emphasis on service restoration and protecting the integrity of the power system in transmission and distribution. The modularization initiatives in some utilities [1] have further increased the use of microprocessor relays for protection and automation. Figure 1 shows the typical mix of protective relay technology from a sizeable North American utility. Earlier generations of microprocessor based relays have reached their life expectancy and shown increased failure rates or malfunctions. Figure 2 shows a typical installation base of one fleet of relays with different platforms and firmware versions from a large North American utility. It can be observed that a large span of IED hardware and firmware versions coexist in the power companies highlighting the added task of asset management including monitoring and tracking performance such as hardware and software failures and firmware compatibility issues, and making strategic plans to maintain the protection system compliant with local or national reliability standards.

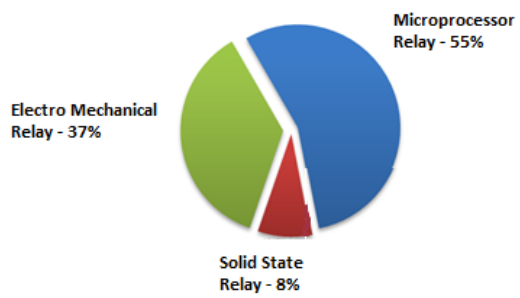

Fig. 1. Typical Protective Relay Inventory Today from a Large North American Power Company

Fig. 2. Platform and Firmware Installation Base from a Single Manufacturer

Meanwhile, electric utility engineers are facing the added challenges to integrate the new features offered by more advanced versions of the IEDs to leverage the added benefits, such as applications in smart grid protection and control, and compliance standards. Utilities are deploying newly launched protective relays with less than desired evaluation of performance, and lean on conformance processes where feasible. This paper makes an effort to discuss and aid engineers to prepare strategies and roadmaps when upgrading the relays as they learn from challenges facing some of the major utilities in North America. Practical and first-hand utility experience on microprocessor based relay upgrade is also presented.

This paper helps utilities better plan the IED life cycle management. A relay upgrade or retrofit project is more than the simple hardware replacement. New relay firmware and function compatibility, the migration of the existing protection and control logic and communication network requirements and device vulnerability to cyber security are some of the important aspects that need to be considered and well planned ahead of time. Furthermore, for a Utility that needs to upgrade thousands of relays, there must be a strategy on how to perform the upgrade systematically and efficiently.

II. DRIVERS FOR UPGRADING AN EARLIER IED RELAY

In this modern technology era, IEDs provide enhanced capabilities in protecting the increasingly complex power system. The business drivers to upgrade IEDs also include the adaptability and the flexibility required by the protection of modern power system. For example, new features from IEDs are required to support the protection and control of interconnected Distributed Energy Resources (DER), the implementation of "Smart Grids", Micro Grids, Nano Grids and energy storage systems.

Additional drivers to the upgrade of an IED are identified and discussed below.

A. Failure Rate

Failure rate (λ) is the frequency of the IED failures (No. of failures/year). The rate often varies over the life time of the relay. It follows the typical electronic devices – "bathtub" curve (Figure 3). The Infant Mortality failure rate is typically eliminated during the factory quality testing or utilities commissioning tests. During the in-service life of a device, a Utility will observe the normal life failure rate and part of the end of life wear-out failure rate. Some Reliability Compliance organizations require that utilities implement time-based or performance-based maintenance or both. The mean time between failures (MTBF), which is the inverse of the failure rate, is often adopted by utilities to measure the performance of an IED type.

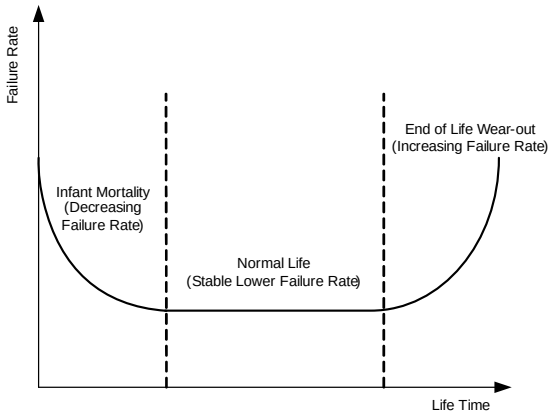

Fig. 3. Typical Electronic Device Failure Rate Curve

Most IEDs today have real-time self-diagnosis and alarming capabilities such as power supply failure, CPU failure, DSP failure, input/output module failure, communication failure, and security violation (e.g. unauthorized login attempt) alarms. This helps with enhanced and more accurate statistics on potential points of failure or areas of vulnerability of IEDs. The information collected from device self-diagnostics or access control measures can be used for the basis of a maintenance program by the user, as well from a manufacturing perspective, to know when parts or components used by a supplier maybe of substandard quality. Monitoring the relays real time also allows the owner to "catch" the failure as it happens. This, however, means that the owner must risk a failure that causes a trip or the failure can leave the owner and the grid in a compromised position. Age of protective relaying fleet and microprocessor failure rates by age of the device have been discussed in other literature [3].

Today, many utilities track the causes of customer outages, and it is important to know how equipment failure contributes to undesired or unplanned outages. The System Average Interruption Frequency Index (SAIFI) in Figure 4 is the average number of times that a customer experiences an outage during the year. This figure also shows how failure counts correlate to the SAIFI.

Fig. 4. Example of System Average Interruption Frequency Index and Equipment Failure Count

The failure mode of IEDs generally does not produce a trip. These relays generally take themselves out of service as they fail. However, this is not always the situation and some failures have caused trips. The utility would need to evaluate the risks of running the IED to failure or at least past its life time. The increased archiving capability of new IEDs gives us the detailed data for fault analysis and misoperation analysis such as caused by incorrect settings/logic design, relay failures and communication failures.

Another potential challenge may be the availability of redundant protection. In some situations, for example, the protection zone of coverage is changed to compensate, for the failed relay. In this situation, tripping for some faults will be time delayed or covered by the backup protection which may involve a greater portion of the grid. The risk of allowing device to operate beyond it useful life is to be evaluated to make sure when a failure of device occurs, reliability requirements are still met in addition to maintaining adequate protection for the intended equipment or system.

B. New Functional Requirements

The advancements in the communication and computing industry have helped with the development of latest protective relay technology. New features and communication protocols are being implemented into the IEDs to support the grid modernization initiatives and provide solutions for integration of new generation sources (wind, solar, energy storage, etc). Below are several key requirements that are driving the upgrade of aging IEDs.

- Time Synchronization

Some micro-processor based devices made in early 1990s have IRIG-B time synchronization, which was the prevalent and the only feasible technology to realize time synchronization at that time. IRIG-B used coaxial cables and can achieve 10 to 100 microsecond (0.1millisecond) accuracy, which is sufficient for tagging the sequence of events, fault records and oscillography. With the emergence of Ethernet in the substation and security concerns, network based time synchronization method is feasible. It improves monitoring, saves the installation and maintenance cost of the dedicated IRIG-B coax cable, and addresses some security concerns with wireless time synchronization from satellites. Network Time Protocol (NTP) was the first one to be adopted and when applied in electrical substations, the simplified version SNTP together with a GPS clock could achieve a typical time synchronization accuracy of 1 to 10 milliseconds. The NTP or SNTP time distribution is less accurate than the IRIG-B, but is still sufficient for many applications. However, with the introduction of synchrophasor technology, IEC61850 process bus, and some future applications of networked based protection such as differential protection, precise time synchronization is required to ensure the accurate time-aligned measurement. The implementation of Precision Time Protocol (PTP) according to IEEE 1588 allows multiple clocks in the

network to synchronize with one another with accuracy better than 1ns (1 nanosecond). The Power Profile (PP) is a PTP profile that suitable for use in power system protection, control and automation applications with a worst-case time error of less than 1us over a 16-hop network.

- IEC61850

The standard enables interoperability among relays from different vendors and interoperability among System Configuration Tools (SCT) from different suppliers. Interoperability in this case is the ability for relays to exchange information and commands on the same network or communication path, and for configuration tools to understand and configure each other's configuration files.

- Network Redundancy

Modern relays can support multiple Ethernet ports at 100Mbps and connect to multiple LANS with PRP or failover redundancy. One application would be LAN1 for relay configuration, maintenance and remote access. LAN2 and LAN3 for SCADA network, substation station bus, process bus, IEEE 1588 communication and can be set with redundancy. Figure 7 in section III. D shows an example of this network configuration. Unlike the failover redundancy, the support of Parallel Redundancy Protocol (PRP) in IEDs provides a high data availability in a substation automation network. In case of a network link failure in one network, connectivity is provided through another network without data interruption.

- Visibility and User Experience

Improvements on the Human Machine Interface (HMI) are another driving force for relay upgrade. Early IEDs were equipped with rather primitive front panel displays and key pads. Up/Down or Back/Forward arrow buttons were used to browse the content or selecting the inputs. The first generation relays had only seven-segment displays. Reading and entering settings from the front panel was a tedious task wrought with a chance for error. The computer software that communicates to the relays did not have a graphical interface, making it difficult to display voltage and current phasor diagrams or even quantities in relation to each other. Modern relays have dramatically improved user interfaces. The relays now not only have bigger LCD displays and graphical setting software, but also added features (e.g. touch screen) to make it more flexible and easier to browse the settings or test the protection functions. Many modern relays have user programmable pushbuttons, which can be utilized to replace the conventional panel mounted control switches and pushbuttons for general control purposes. Another notable progress is the logic status monitoring, where the relay internal logic variables are displayed graphically in real time together with the logic diagrams. This feature is a great tool for relay functional testing and troubleshooting.

These new features address the quality of the actions associated with the protective relays and increase the confidence level of the technician and engineer working with these devices. The new features reduce the chance for errors, increase the monitoring features and help the user with understanding the device.

- Multifunction and Complexity

Early micro-processor relays often only had the protection functions, due to the technology limitations of CPU performance or the amount of available RAM. As integration became more technologically feasible, additional functions or features have been introduced and coupled by increased network reliability, enhanced features for monitoring, automation and control (e.g; SCADA) have become feasible. With the added features, additional security concerns have also been introduced. Transmission line loadability requirement provides a good example of how the relay functions have evolved during the last few decades. Most early distance relays did not have a load encroachment function and to meet loadability requirements, additional devices were needed. In the last decade additional reliability standards such as the North American Standard, NERC PRC-023, have required relays to be tested for system loadability. Modern distance relays now have features to restrict the relay operation under load and allow the user to meet the standards without adding additional devices. Modern line protection relays also have advanced fault directionality as well as functionalities that comply with power system stability standards such as out of step detection, islanding, single-pole tripping and reclosing to name a few.

Manufacturers have been supporting the industry needs with developing features that provide smart grid functions, based on the information gathered by relays and smart sensors. Today, the hardware performance allows the integration of many features for both transmission and distribution applications. Some examples are:

a) Over Current relays that support arc-flash detection
b) Auto-recloser control relays that support line-monitoring sensor inputs
c) Transformer protection relays with transformer health monitoring sensors
d) Asset health diagnostics (i.e. breaker)
e) PMUs with ROCOF (Df/Dt)
f) Voltage Control
g) Islanding Detection
h) SSO (Sub-synchronous and Super-synchronous Oscillations), Power Swings, Traveling wave concept based distance to fault detection
i) Fault recording and analysis capabilities
j) New features with enhanced communications capabilities including
    - Multiple network ports
    - Cyber security

The single function relay to multi-function device concept offers the user the ability to adopt the desired functionalities based on the user business case and application requirements.

With increased functionality, modern IEDs can provide all the protection functions required for the equipment to be protected with only one single unit. As a matter of fact, the actual programming of an IED in most cases only uses a subset of the available functions. From redundancy and reliability considerations, utilities typically use two IEDs to protect the equipment. Unfortunately, with integrated features and device flexibility come the increased complexity for the number of settings in one single device and also the integration of responsibilities as to which lines of business need to provide the information for the respective device set points. Furthermore, the increased functionalities can inadvertently increase the complexity of firmware testing, relay set points and field commissioning testing, which can be intimidating even for the most talented protection engineers and testing technicians.

The skills sets of our work force must also be taken into consideration. The utility practitioner focus is changing and is not the same as it was in past. People that know the physics of how the electric grid functions may not be the same people that are programming these complicated relays and in some instances only a small fraction of the settings in new relays are associated with the physics. There will need to be close coordination between the team preparing the settings and the test team to help validate the safe operation of the grid, (also refer to section IV.B.).

C. Security and Compliance

Modern IEDs provide network capabilities that can be used for peer to peer information exchange or remote SCADA control and monitoring, EMS, Engineering, Operations and Maintenance. Therefore, security that includes controlling the physical access as well as protecting against malicious network related cyber-attacks and intrusion are critical. Security features in modern IEDs have been enhanced to comply with the latest North American Critical Infrastructure Protection (CIP) standards. The security measures typically include strong passwords, basic role-based password security within the device or server-based authentication, which a centralized RADIUS server is used to authentic the access rights to the IED. The increase of Ethernet based applications requires security measures to be implemented both in the IED application/device level and the higher network level. In some instances, a substation gateway may be used as a means of access control to the substation devices. Gateways and firewalls may have additional authentication features for access control. In many instances, the users have set-up a trial system to validate and perform comprehensive cyber security testing using comparable setup and applications as the field prior to performing the IED relay upgrade in a large scale roll out. The testing scope may include:

1) Port scan to make sure the IEDs do not have unnecessary ports open, see Table 1 as a typical test results.

Scan No.	Services	Port Numbers	Default Port Status	Configurable Port Numbers	Port Can Be Disabled
1	MODBUS/TCP	502	Enabled	Yes	Yes
2	HTTP/UDP	80	Enabled	Yes	No
3	IEC61850 (iso-tsap)/TCP	102	Disabled	Yes	Yes
4	PMU/TCP	4712	Enabled	Yes	Yes
5	PMU/UDP1	4713	Enabled	Yes	Yes
7	TFTP/UDP	69	Enabled	Yes	No
8	TFTP Data port/UDP (2)	0	Enabled	Yes	No
9	DNP/TCP	20000	Disabled	Yes	Yes
9	DNP/UDP	20000	Disabled	Yes	No
10	IEC104/TCP	2404	Disabled	Yes	Yes
11	SNTP/UDP	123	Disabled	Yes	No
12	EGD Data Port	18246	Disabled	No	No

Table 1: Port Scan Result using NMAP for an IED in the Testing Lab

Some of the more complex or rigorous technologies for automated open port detection, such as vulnerability scanning, are first experimented in lab environment. Further collaboration with protective relay manufacturers may be helpful before production level tests particularly when legacy products are also potentially exposed. Working with solution providers also helps with the beyond user functional tests of cyber solution and may lead to a new firmware or for example, blocking a port from the range of ports the scanner is set to test.

2) Denial of service testing that includes SYN flooding, ping of death, land attack, and UDP/TCP packet flooding tests,

3) Protocol mutation testing that conducts TCP/UDP/ICMP header tests, IEEE C37.118 command frame dumb fuzzing and smart fuzzing tests,

4) Device security feature testing that confirms password content, interactive session timeout, multiple failed password attempts, alarm contacts, security logs, setting file access, locking settings files and device firmware, traceability of setting file changes, security management system enabled by default and its access rights,

5) Network traffic disclosure testing utilizing both network traffic analysis and SSH man-in-the-middle password crack tools. Any vulnerability and incompliance with the security standard should be addressed by the relay

vendors or security measures taken in the network such as VLAN or firewall rules.

D.Maintenance Cost

Microprocessor and solid state devices in the electric grid have been in service for many decades and are aging to the point of necessary replacement. The variables involved in the decision to replace an asset are discussed in this paper. However, all assets cannot be replaced in a very short period of time. It takes a well-planned approach to develop a replacement strategy. This is no difference when considering microprocessor based relays. Everything has a finite life and predicting the life of a microprocessor based relay requires consideration of many variables. There are multiple ways to determine the impending failure of an IED. The traditional method is to perform periodic testing and/or maintenance on the relay. This requires technicians, asset planners, schedulers and possibly protection engineers to take part in the planning process to isolate a relay and perform the tests necessary to determine proper function of the relay. This costs the utility resources and significant budget.

IEEE has determined that the maintenance costs as an industry for protective relaying as a whole will double in the next 10 to 20 years. This is a complicated concept as many utilities are replacing EM relays with IEDs and as they are turning more and more of their fleet into IEDs, the early relays have reached their end of life. Figure 5 shows the expectation of maintenance cost verses the System Average Interruption Duration Index (SAIDI), which is used to calculate the total duration of an interruption for the average customer during a given period.

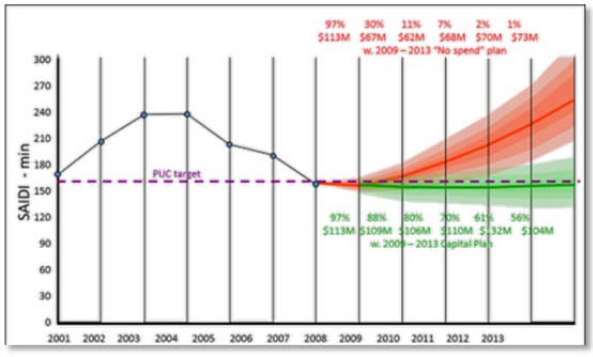

Fig. 5. System Average Interruption Duration Index (SAIDI) verses Maintenance Cost

III. CHALLENGES AND STRATEGIES

Challenges that utilities are facing when planning for upgrading an IED not only include the hardware but also the device firmware that has evolved over many years. The firmware that enables new features, bug fixes and algorithm changes, often requires more study, research and testing and may or may not be compatible with the existing application.

A. Technology Advancement on Hardware

New technology enables longer life cycles of hardware and self-monitoring capabilities (e.g. power supply board) and higher processing power of Central Processing Units (CPU), multiple independent Ethernet ports, the latest operating system for improved security and diagnostics, large storage capability with relatively small size and lower cost. The selection of relay hardware or platform should consider the support of aforesaid functionalities and features via firmware upgrade only.

B. Managing the New Features and the Complexity

IEDs have added vast arrays of new functions, increased flexibility and capabilities. Setting an IED will require engineers to have expertise not only in the traditional protection and control field but also on Ethernet and network protocols. Protection engineers may find it difficult to understand the inter-relationship between functions in order to produce the proper set points for the desired operation. For example, a setting in the circuit breaker function may affect the function of auto-reclosing or breaker failure. Some research from academia has been conducted to simplify the configuration of multi-function IEDs. For example, Dr. Meliopoules describes a setting-less relay approach based on the Dynamic State Estimation in [7]. Relay manufactures should study and shift the relay setting methodologies from traditional function based settings (inherited from the legacy electromechanical relays) to equipment based settings.

C. More Frequent Firmware Upgrade

There are many factors that contribute to a revision of a device firmware. With the addition of new functions, the IED firmware design, validation testing and programming are getting increasingly complicated. The opportunities for introducing firmware bugs are therefore also increasing. Utilities may find firmware updates or advisories happening more frequently than experienced with earlier relays.

In a comparison of features and functions between an earlier version and latest version of a line differential protection, the results show that in addition to supporting more protection functions, many of the new features are all related to the latest communication technology; such as IEC61850, synchrophasors (PMUs), cyber security and PRP redundancy.

It is not practical for utilities to upgrade all their devices to the latest firmware whenever it is available due to the frequency of the updates and the cost of updating relay firmware for in-service units. Unless there is a service advisory or a potential concern on the performance of the relay that might affect the performance of the device such as security or reliability, the IED will be kept in service until the end of its life or until some other change within the substation provides the opportunity to upgrade. Before accepting a new firmware, utilities typically do certification testing (sometimes even with RTDS). Most

utilities specify and standardize on an older pre-tested firmware version even when ordering new relays to save the cost of firmware validation and asset management. As a result, there are a considerable number of devices operating with very old firmware and on old hardware platforms. These will see increased failure rates and contribute to issues that affect the security, reliability and performance of the overall protection systems.

Due to the amount of IEDs in service (one utility has over 20,000 microprocessor based relays in service), making a decision and planning to upgrade the IEDs to the latest version is a large project and requires dedicated effort and resources. A business case should be designed to find a feasible solution. Utilities may need to consider the overall cost driven by the following considerations: hardware replacement, firmware validation testing, setting conversion/development, clearance schedules, site testing and database update, etc.

D. Impact on Substation Automation Architecture

IEDs have advanced communication capabilities and diagnostic functions compared to earlier generation relays and users leverage these enhanced communication capabilities to increase equipment and overall design reliability. The inherent internal monitoring of the latest generation of IEDs also facilitates easier root cause investigation of system performance. To take advantage of these capabilities might involve upgrading network switches, substation gateways and GPS clocks to mention a few items and it might also require reconfiguration of RTUs and retesting of SCADA systems etc. One example of this would be the DNP/Modbus communication with RTUs, where the earlier generation of relays would use serial communication (RS485 or RS232) with a low baud rate (see Figure 6) which may no longer satisfy the latest requirements of standards, the needs of the user or the needs of applications being implemented. Network (Ethernet) based high-speed communication could, on the other hand, provide real-time data with relatively lower cost and make the upgrade feasible by providing additional monitoring capabilities. Figure 6 shows the traditional serial communication with older generation relays.

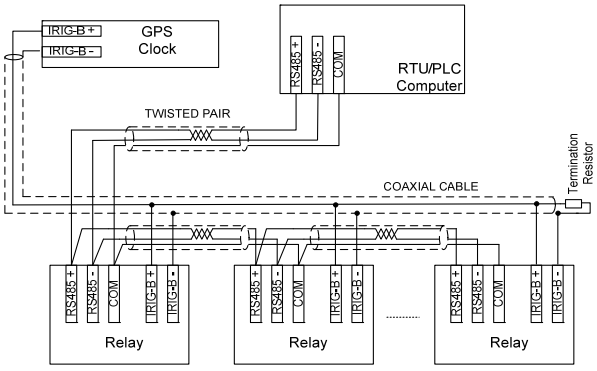

Fig. 6. Serial Communication and Time Synchronization with Older Generation Relays

Figure 7 shows a typical modern IEDs communication network using multiple Ethernet ports and LANs that support lots of available technology requirements and applications.

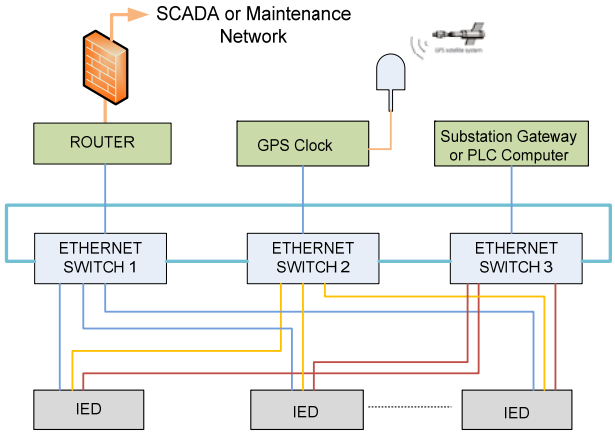

Fig. 7. IED Ethernet Communication and IEEE 1588 Time Synchronization

IV. Process to Upgrade an Aging Relay

Throughout this section, there are typical hardware and firmware upgrade discussions and implementation considerations influencing decision making strategies. In some instances, technology obsolescence may have led to an upgrade with a different physical size or orientation such that the replacement may not to be "one-to-one" compared with the legacy hardware. Device settings for protection, control or automation may not be compatible or may be from different manufactures or may not be available anymore. Careful consideration must be made for embedded algorithms and logic for in-kind upgrades, and testing of these features is also critical in the process chain described further in this section. Other contributing factors such as natural calamity or seismic events may require the power company to be prepared for such extreme contingencies, and the upgrade strategy and technology should be part of the decision making process.

A. Hardware Replacement

- Modular Devices and Protective Relays

Modular relays have the advantage of keeping the external wiring intact. The hardware upgrade can be done with simply replacing the individual modules. Some modules may be interdependent and have to be replaced when other modules are replaced. To simplify the upgrade process, some vendors provide upgrade guidelines and upgrade kits that include the required modules, new labels and software tools.

- Non-modular Devices

The labor cost associated with non-modular relay upgrades are generally higher than that of the modular relay since the relay wiring has to be removed and rewired in the upgrade process and there is typically some panel

work involved. In addition to the cost of wiring changes, there are also costs for documenting the changes on drawings and testing of the changed wiring connections. For non-modular relays, it should first be investigated that if it is feasible to replace the electronic circuit boards without changing the relay case. The use of "connectorized" terminal blocks where the entire terminal block with wiring attached can be removed from the relay in question should also be considered.

To bring the cost down, wiring changes should be minimized as much as possible. If the relay is upgraded to the same make and model with the exact physical size, electrical connection and the terminal numbering as those of the old model, then the re-wiring will be a straightforward one to one change. However, relay models that are 10 to 15 years old may now be obsolete and have been replaced with models that do not resemble the earlier version either in size or terminal connections. One solution in this scenario can be a pre-built vendor relay package to bridge the differences between the old and new terminals.

With this solution, the field relay wiring changes are greatly reduced. In other instances, spare prefabricated panels are made available, for a complete change out, where a prewired relay panel designed for protection and control of a single element (e.g; line or transformer) or multiple bus bays can be upgraded. These stand-alone prefabricated panels are kept in stock, and are transported and installed in place of a failed relay panel, or in place of a flooded control building to allow quicker restoration under emergency conditions. Likewise, prefabricated protection, control, and automation panels can be deployed for protecting mobile transformers as well as to aid the construction or to assist in transformer failure replacement. Modular protection, automation, and control building concepts, where relay panels are pre-wired, loaded with settings, functionally tested and are ready to deploy to minimize the field time and clearances [1].

B. Firmware Backward Compatibility

For an IED that is from the same vendor and series, the upgrade processes are much simpler than replacing with a relay from different manufacturer. When upgrading an IED of the same type, firmware backward compatibility is one of the big concerns and requires the engineers to explore the release notes history and user instruction manuals of both the earlier version and the current version. From the experience of a few utility IED upgrade projects, it was seen that the IED backward compatibility issues are common. These generally fall into the following two categories:

- Modbus and DNP Communication

Some of the Modbus addresses have been changed over the development of the IEDs. Therefore, Modbus address mapping needs to be carefully reviewed to make sure the actual items keep the same addresses, communication channel and point mappings might be impacted as well since the standard has been changed to support new features such as DNP over Network. The SCADA/RTU data point mapping will need to be updated to communicate to the new IEDs.

- Protection and Control Functions

Some protection or control functions may be working well in the earlier version. With the same settings, the same function might not work as expected unless some other settings are configured or setting values changed.

It is difficult to predict all the backward compatibility issues before the project starts, as it needs careful research on the difference of the relays not only functionally but also the underlying implementation. A typical approach to this is to test the relays in parallel, function by function and verify the test results are improved or as expected. If the reason for upgrading an IED is malfunctions due to firmware deficit or advisory list, verify the issues exist in the earlier version and do not happen in the upgrade candidate version.

C. Setting Conversion

Conversion of old relay settings to the upgraded IED can be classified into three categories.

- Same Vendor and Model

The new IEDs have added features and functions which require new configuration or setting files. The most straightforward method is to use the vendor software setting conversion function to convert the setting file from an older version. It should be noted that there are some limitations with this method. First, there can be hundreds of added settings due to the function and feature additions and improvements. Usually the default value that is assigned by the vendor software is accepted, but this should not always be taken for granted. Moreover, there can be tricky cases where some settings definition changed while the setting name remains the same. For example, a zero-sequence current setting in the older relay version may mean I0 while it was changed to represent 3I0 in the new version but with the same setting name. So protection engineers still need to evaluate if the default values or the converted values are appropriate to use. Furthermore, utilities often upgrade the templates of the relay logic to fix deficiencies or improve security. The old relay setting file may be based on an older logic template and the conversion method cannot carry forward the old logic into the new setting file. Manual logic modifications will be needed if a new logic template is required. Finally, one area that is often overlooked in the planning stage, but that can cause additional challenges is if the communication platform, profile, or parameters have changed from the original implemented architecture. For example, if the original implementation was Modbus and a life cycle upgrade is needed to conform to a new standard using DNP 3.0 or IEC61850, or even if the original Modbus

protocol is used and over time the Modbus addressing may have changed within the Utility. Should the process for upgrade go beyond the intended original plans to address broader issues for a large scale relay upgrade project where hundreds of setting files need upgrade? The planning of the project should evaluate options for overall project efficiency.

- Same Vendor, Different Models

Some vendors offer a setting conversion tool across different models. Caution should be used for the same issues that were discussed in the previous section in using the conversion tool. Also, if the theory of the protection function differs significantly from the previous device protecting the same equipment, then the interface with new settings also requires protection engineering review as describe in the next section.

- Different Vendors

This is the most challenging scenario for setting conversions. Even though the underlying protection theory does not differ much, relay vendors apply it with different algorithms, thus the settings and their definition will not look the same for different vendors. Sometimes the protection function and the setting name seem to be the same between different relay models, but there exist subtle differences which prevent a direct setting value conversion. A good example is the application of transformer percentage restraint differential protection. Each relay of this kind will have restraint differential characteristic settings, such as minimal pickup, slopes and break points. It is important, however, to understand the differences in the meaning of the settings, which are based on the relay's definition of differential and restraint current. Though the differential current definition is almost universal, the restraint current is often defined in various ways. Some relay vendors define it as the sum of the winding current; some define it as the maximum winding current; others define it as the "average" winding current, which is the sum of the winding current divided by the number of windings. Thus the actual restraint slope characteristics will be different though the relay setting values are the same. A direct setting value transfer across different models without considering the underlying setting definitions will result in mistakes in the conversion and possible relay misoperations [2].

Figure 8 shows a process of automatically converting the settings values and logic into new relay setting files using the setting conversion tool. The setting conversion tool plays a vital role in the IED upgrade process. The setting conversion tool should satisfy the basic function requirements:

a) Convert protection functions based on user specified function mapping table.
b) The converted protection settings shall have equivalent characteristics as the original relay.
c) Comparison of existing setting and converted settings.
d) List of settings that are removed or cannot be converted.
e) List of new settings added.

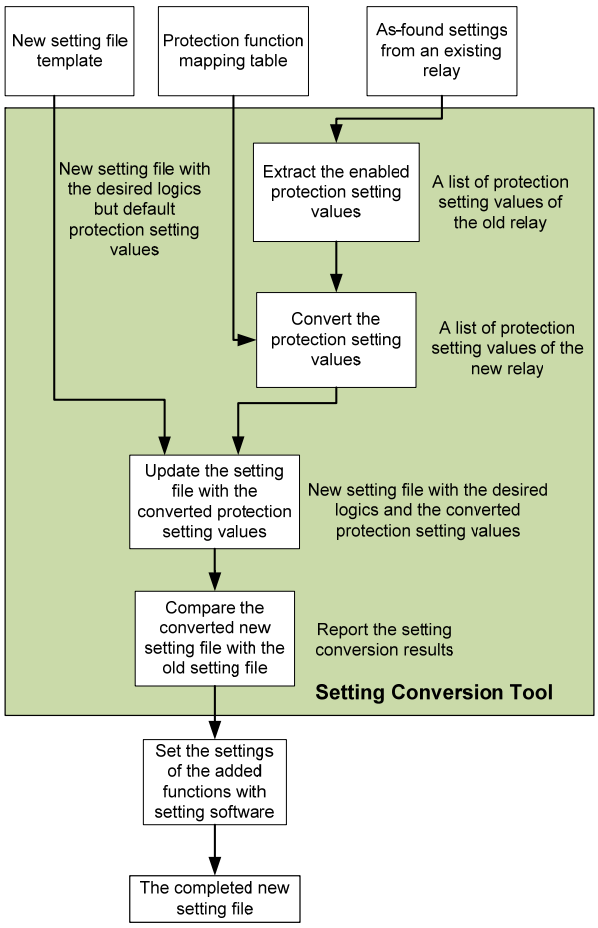

Fig. 8. Setting Conversion Tool Functional Diagram

Despite the difficulties in the settings conversion, it is still an easier way than performing new setting calculations. Manually converting the settings for many relays are inefficient, as discussed previously. The development of a setting conversion tool may also need to access the vendor specific setting files. So the developers have to know vendor relay setting file format or database structure, and vendor support may be needed to achieve the best outcome in automating conversion of settings as an initial stage by the protection engineer and before validation of set points.

Experienced engineers are needed for complex setting conversion to ensure the new setting values will have the exact or equivalent performance compared with the old setting values. Though most protection values can be converted satisfactorily, engineering review is still needed for complex applications, such as conversion between protection functions based on completely different algorithms, single pole tripping, or auto-reclose settings. Setting reviews should focus on three steps.

a) Settings removed (not existing in new setting file)
b) New Settings (Section D)
c) Algorithm differences

D.Review of New Setting

After the conversion of existing settings, some settings that only exist in the upgraded setting file have to be reviewed. Those new settings could be classified into two categories.

- New settings for an existing function

Some setting points may be added to a newer version IED for various reasons (increased flexibility, revised logic or improved functionalities). Typically, leaving them to default values will keep the same functionality as the older version for compatibility. It is recommended, however, to review those settings in detail.

- New settings for a new function

These settings are added due to the new features or functionalities. Utility protection engineers or IT should decide the set points and provide setting guidelines to setup the new features.

E. Site Commissioning, Isolation and Testing

Site commissioning is the next step in the upgrade process. Before the actual commissioning activities, the clearance schedule should be applied and approved. Proper isolation should be followed before removing the old hardware, installing the new hardware, cabling and testing.

Even though microprocessor base relays have evolved over many years with new features and enhanced functionalities, modern IEDs are still the digital replication of the early EM relays at the functional level. Therefore many features of the IEDs can be tested the same way as EM relays. IEDs can provide real-time testing interface and trouble-shooting tools via real-time analogue, digital and logic status, SOE and Oscillography. The testing of individual functions may seem to be easier than EM relays. The overall functional testing of IED, however, becomes more complicated and challenging due to their multi-functionalities and new technologies. A testing procedure that covers all used functions and features should be provided to testing technicians. This is especially true if an individual timer or phase or ground function is being tested because the IED will operate as a system and it will be responding to functions that have an interrelationship between all timers and all phases including the ground. It may be necessary to have particular functions of the IED tested under separate configurations with a rigorous tracking method to insure the IED is placed back into full operational configuration before being placed in service.

V. Asset and Record Management

There are many elements to the asset management strategy, including: 1) Enumeration of the Asset, 2) A robust Maintenance program, 3) Asset Performance monitoring, and 4) A Prioritization model

Enumeration of the asset requires the owner to gather and track the various characteristics of an asset such as age, installation date, location, model and firmware. It is also important for the owner to understand the performance of the asset including failure rates, manufacture (MF) recalls and alerts, vendor support, maintenance requirements and costs, resource skills, computer software and operating system compatibility. It is beneficial for the users to have a maintenance program that creates a history of the costs involved with maintaining the IED but also helps track any problems associated with the maintenance activity or the device itself.

The strategy for large scale upgrade often requires a prioritization model to support overall efficiency and effectiveness of the solution. The prioritization model should include Engineering and Record management, whether for example the device style is upgraded and bill of material needs to be updated, or if any of the baseline configurations have been updated to the extent. Likewise, the objectives and goals such as Safety, Environmental Benefit, Reliability and Affordability (Figure 9, 10, 11) should be captured as part of the prioritization process.

Impact Level (I)	Safety
Catastrophic (7)	Fatalities: Many fatalities and life threatening injuries to the public or employees
Severe (6)	Fatalities: Few fatalities and life threatening injuries to the public or
Extensive (5)	Permanent/Serious Injuries or Illnesses: Many serious injuries or illnesses to the public or employees.
Major (4)	Permanent/Serious Injuries or Illnesses: Few serious injuries or illnesses to the public or employees.
Moderate (3)	Minor Injuries or illnesses: Minor injuries or illnesses to many public members
Minor (2)	Minor Injuries or illnesses: Minor injuries or illnesses to few public members or employees.
Negligible (1)	No injury or illness or up to an un-reported negligible injury.

Fig. 9: Typical Safety Factors and Priority Impact Levels

A well-planned prioritization model considers synergies with other replacement strategies such as breakers and transformers or major capacity upgrades when feasible or practical for overall efficiency including project management, engineering, automation, network and IT, and field support.

Impact Level (I)	Reliability
Catastrophic (7)	**Location:** Impacts an entire metropolitan area, including critical customers, or is system-wide; and **Duration:** Disruption of service of more than a year due to a permanent loss to a nuclear facility, hydro facility, critical gas or electric asset; or **Customer Impact:** Unplanned outage (net of replacement) impacts more than 1 million customers; or EO: 50 million total customer hours, or more than 1 million mwh total load
Severe (6)	**Location**: Impacts multiple critical locations and critical customers; or **Duration**: Substantial disruption of service greater than 100 days; or **Customer Impact**: Unplanned outage (net of replacement) impacts more than 100k customers; or EO: 5 million total customer hours, or more than 100k mwh total load;
Extensive (5)	**Location:** Impacts multiple critical locations or customers; or **Duration:** Disruption of service greater than 10 days; or **Customer Impact:** Unplanned outage (net of replacement) impacts more than 10k customers; or EO: 500k total customer hours, or more than 10k mwh total load;
Major (4)	**Location:** Impacts a single critical location; or **Duration:** Disruption of service greater than 1 day; or **Customer Impact:** Unplanned outage (net of replacement) impacts more than 1k customers; or EO: 50k total customer hours, or more than 1k mwh total load;
Moderate (3)	**Location:** Impacts a small area with no disruption of service to critical locations; or **Duration:** Disruption of service of up to 1 full day; or **Customer Impact:** Unplanned outage (net of replacement) impacts more than 100 customers; or EO: 5k total customer hours, or more than 100 mwh total load;
Minor (2)	**Location:** Impacts a small localized area with no disruption of service to critical locations; or **Duration:** Disruption of up to 3 hours; or **Customer Impact:** Unplanned outage (net of replacement) impacts less than 100 customers; or EO: Less than 5k total customer hours, or less than 100 mwh total load;
Negligible (1)	No reliability to negligible impacts.

Fig. 10: Typical Environmental Factors and Impact Levels

Most users today, have a database to manage assets related to protection, automation, and control devices. The database typically contains equipment location, original purchase order and associated manufacturer, in-service date, and many other fields to document the history of the IED and protection system including firmware version, protection, control and automation set points, etc. When needed, reports are generated for assessment and evaluating the key factors of the protection systems or to tackle an advisory letter from a manufacturing.

Impact Level (I)	Environmental
Catastrophic (7)	**Duration:** Permanent or long-term damage greater than 100 years; or **Hazard Level / Toxicity:** Release of toxic material with immediate, acute and irreversible impacts to surrounding environment; or **Location:** Event causes destruction of a place of international cultural significance; or **Size:** Event results in extinction of a species.
Severe (6)	**Duration:** Long-term damage between 11 years and 100 years; or **Hazard Level/Toxicity:** Release of toxic material with acute and long-term impacts to surrounding environment; or **Location:** Event causes destruction of a place of national cultural significance; or **Size:** Event results in elimination of a significant population of a protected species.
Extensive (5)	**Duration:** Medium-term damage between 2 and 10 years; or **Hazard Level/Toxicity:** Release of toxic material with a significant threat to the environment and/or release with medium-term reversible impact; or **Location:** Event causes destruction of a place of regional cultural significance; or **Size:** Event results in harm to multiple individuals of a protected species.
Major (4)	**Duration:** Short-term damage of up to 2 years; or **Hazard Level/Toxicity:** Release of material with a significant threat to the environment and/or release with short-term reversible impact; or **Location:** Event causes destruction of an individual cultural site; or **Size:** Event results in harm to a single individual of a protected species.
Moderate (3)	**Duration:** Short-term damage of a few months; or **Hazard Level/Toxicity:** Release of material with a moderate threat to the environment and/or release with short-term reversible impact; or **Location:** Event causes damage to an individual cultural site; or **Size:** Event results in damage to the known habitat of a protected species.
Minor (2)	**Duration:** Immediately correctable; or contained within a small area.
Negligible (1)	Negligible to no damage to the environment.

Fig.11: Typical Reliability Factors and Priority Impact Levels

Different users deploy different strategies to address device upgrades. Depending on the nature and purpose of the upgrade, different priority weight scales maybe assigned in order to manage the asset pool. Some of the decision trigger factors, when a user has a large pool of

devices in the same vintage and by one manufacturer, include:

- Factory advisory and nature of the component or module failure. In some instances, the advisory may be component fatigue due to life cycle degradation. For this scenario, the action from the failure is then examined. If a device failure results in undesired trips, the user may need to put a higher priority than when the device failure generates an alarm and takes itself out of service.
- Firmware upgrades usually involve device set point testing. The user first needs to determine the process for upgrade including training for field resources, extent of testing, the duration of a clearance and related scheduling

Priority measures may include business case decisions such as impact due to component failure, e.g. bus differential operation, or breaker failure activation, or whether there is an alternate protection available. Other measures include reliability, impact to SAIDI, SAIFI, bulk electric system, etc. Some include operational decisions as part of the process. For example, they consider next level failure on the alternate system that is still active while the other protection level is taken out for replacement / upgrade. Also, the total number of devices that need to be addressed is a part of the prioritization review process.

Once the priority weight is determined, and depending on the size of the upgrade, a program with a detailed schedule for each line item is created and funding is secured. The program should include general guidelines for overall scope, protection and automation engineering documentation for upgrades (including device settings), clearance planning, procurement of parts or firmware, test procedures and the deployment schedule.

VI. Lessons Learned

The electric grid is now populated with some of the most advanced technologies and reliable operations of power systems are becoming more paramount from a life cycle support perspective. To meet the protection and control requirements in today's complex interconnected system, the IEDs offer many enhanced features in support of product and hardware standardization initiatives. At the same time, the concept of one size fits all requires alterations and custom fitting on the user side by disabling features not applicable to the particular project. Some of the life cycle upgrade decisions involve whether to upgrade with in-kind features, or expand the use as a result of technology. Whether an application needs the enhanced Cyber security features, or enhanced oscillography capture, or perhaps enhanced internal IED diagnostics for compliance purposes for example, may require some user interface decisions (settings). Of course part of the process will need to include which specialized group is responsible for providing the recommended set points.

Other more apparent business drivers cover the distribution landscape. The distribution system is getting more complex with deployment of distributed renewable energy resources, Smart Grid technologies, micro grids, nano grids and energy storage systems and the bi-directional power flow in the distribution systems are adding business drivers for making the life cycle upgrade more dynamic as opposed to the more traditional ways for asset management.

Another important lesson is product evaluation as new features or enhancements are embedded into the protective relays. Enhancements at times may inadvertently impact other components previously approved for use by a particular power company.

Our industry is experiencing change now more than any other time except in the beginning when Tesla, Insull, Edison and Westinghouse and others were setting the direction. It is important for the practitioners of our industry to always look to the future as far as possible to create sustainable applications and deploy products that can incorporate flexibility and allow change. The upgrade strategy should consider simplicity, reliability, sustainability and skill sets needed when applying microprocessor based equipment. A comprehensive strategy customized for each utility based on the concepts discussed in this paper will help the utility create sustainability for the microprocessor devices and affordability, reliability and safety for their customers.

References

[1] V. Madani, G. Duru, B. Tater, et. al; "A Paradigm Shift to Meet the Protection and Control Challenges of 21st Century", Georgia Tech Protective Relaying Conference; May 2007

[2] Y. Xue, Z. Campbell, S. Chidurala, et. al; "Mis-operation Cases on Transformer Differential Protection", Western P Western Protective Relay Conference, Washington State University, 2015

[3] J. Sykes, A. Feathers, E. Udren and B. Gwyn, "Creating a Sustainable Protective Relay Asset Strategy," in Western Protective Relay Conference, Washington State University, 2012.

[4] GE Digital Energy, "UR 3 Upgrade Guide", GET-8550.

[5] NERC, "Standard PRC-005-2 - Protection System Maintenance".

[6] GE Digital Energy, "Multilin DGPR Integrated Solution for Retrofit of the Multilin DGP Generator Protection Relay"

[7] A.P. Sakis Meliopoulos, George J., Zhenyu Tan and Sungyun Choi, "Setting-Less Protection: Feasibility Study", System Sciences (HICSS), 2013 46th Hawaii International Conference.

Biography:

Vahid Madani is a Principal Engineer scientist and technology leader for advanced power systems applications at Pacific Gas & Electric Co., headquartered in San Francisco, California, USA. His experience spans across System Planning, Operation, Protection and Control Engineering, Asset Strategy and Compliance. He is responsible for grid modernization, and deployment of emerging technology including Synchrophasor systems and geomagnetic disturbance resiliency.

Vahid has held many technical and leadership positions within the WECC Regional Reliability Council, the US DOE / North American Synchrophasor Initiative (NASPI), and the IEEE PES (Power and Energy Society).

Dr. Madani has many publications and has co-authored text books and reference handbooks. He is a Fellow of IEEE, an IEEE Distinguished Lecturer, Adjunct Faculty at Mississippi State University, and is a registered Electrical Engineer in California.

Yujie Yin is a Principle Advisor in Power System Protection and Control at Quanta Technology. Prior to joining Quanta Technology, Yujie was a Senior Application Engineer in GE Digital Energy's Technical Expertise team, where he has worked on many projects from North America utilities. He has over 20 years of electric utility experience from initial studies to detailed substation design, construction and commissioning. In the last five years, he was especially focused on multi-vendor IEC61850 system integration activities, Remedial Action Schemes (RAS) and Wide Area Measurement Protection and Control (WAMPC).

He is a senior member of IEEE, CIGRE B5 WG and a licensed Professional Engineer in the Province of Ontario and Alberta. He received his Bachelor of Computer Science and Master of Electrical Engineering from Western University, Canada. And also holds a Bachelor of Electrical Engineering degree from HFUT, China.

Yong Fu is an Associate Professor in the Department of Electrical and Computer Engineering at Mississippi State University (MSU). He received his B.S. and M.S. degrees in Electrical Engineering from Shanghai Jiao Tong University, China, in 1997 and 2002, respectively. In 2006, he received his Ph.D. degree in Electrical Engineering from Illinois Institute of Technology.

Yong has over 15 years of research experience in the area of power system operation, protection and control, and has published over 40 IEEE Transactions journal papers. He serves as a PI or co-PI on several projects including Smart Grid, Electric Ship Research, Micro-CHP, and Synchrophasor.

Professor Fu has been awarded the Tennessee Valley Authority (TVA) Endowed Professorship in Power Systems Engineering. He is a recipient of the NSF Faculty Early Career Development (CAREER) Award in 2012, and serves as an editor for the IEEE Transactions on Power Systems, the IEEE Power Engineering Letters, the IEEE Access, the Journal of Electric Power Components and Systems, and the CSEE Journal of Power and Energy Systems. He is an IEEE senior member and has served as Guest Editor of the IEEE Transactions on Smart Grid.

Sudhakar Chidurala: Received Bachelor's degree in Electrical Engineering from Osmania University, India in 1989 and Master of Technology degree in Electrical Engineering from Regional Engineering College Warangal affiliated to Kakatiya University (currently called National Institute of Technology) in 1999. He is working for AEP (American Electric Power) as Protection and Control Engineer, working on capital, rehab, and customer owned projects to design and provide relay settings for protection and control.

Prior to joining AEP, Sudhakar has worked in Protection and Control Engineering field operations group for (3) years with Hydro One Inc., ON, Canada and (13) years in AP Transmission Corporation, TS, India at various capacities in the field of Protection and Control Engineering. Sudhakar is an active Senior Member of IEEE, He is also a Member MIE (Member Institution of Engineers of India) and is a registered Professional Engineer (PE) in the State of Oklahoma, Texas and New York.

Xiangmin (Jonathan) Gao is a Senior Lead Project Engineer at GE Grid Automation. He is an IEEE member and a registered Professional Engineer in the Province of Ontario. His main interests are in power systems network protection, transient study and digital simulations. He received his B.Sc. degree from North China Institute of Electric Power (now NCEPU) in1993 and M.Sc. degree from Zhejiang University in 1996, both in Electrical Engineering.

Jonathan Sykes is the Senior Manager of System Protection at Pacific Gas and Electric Company (PG&E) in San Ramon, California. Jonathan graduated from the University of Arizona in 1982, is a Professionally Licensed Electrical Engineer (PE), and has more than 30 years of engineering experience in System Protection and working for electric industry. His career is rich with contributions to create sustainability within the industry and has evolved from applying new technologies to finding successes with ever increasing complex challenges of this changing industry. He is the driver to developing industry leading asset replacement strategies that is building awareness and providing the bridge to sustainability concerning microprocessor based devices.

Jonathan has authored and co-authored papers for conferences and publications and is an active senior member of IEEE and regularly contributes to the Power System Relay Committees and has been active in NERC and WECC standards interpretation and development of infrastructure related standards. He is past Chairman of the North American Electric Reliability Corporation (NERC) System Protection and Control Subcommittee (SPCS).