Abstract—Breakthroughs in power system protection and control technology support significant industry facelifts. Streamlined selection and application of products and systems have become possible and tools for design and implementation have become easier to work with. Nonetheless, the planning, engineering, procurement and implementation of protection, control, data management and automation at a major power utility is a complex endeavor, from both the technical and the business process perspectives. This paper will explore the experiences of a major power company in managing through a true paradigm shift, and further narrow the focus to the impact of these changes on substation networks, data management, technology risk management, and cyber security. The key elements of success include a clear vision, in-depth understanding of past practices, a detailed roadmap, support and encouragement from internal leadership, and partnership with key manufacturers willing to support the process with R&D investments that benefit not only the power utility but also the industry.

Index Terms—Automation, Communications Systems, Data Management, Data Security, NERC, Network Reliability, Protection, Protective Relaying, Power Industry, Substation.

I. INTRODUCTION – FROM SILOS TO INTEGRATION

Just a few years ago, protection and control engineering designs were based on medium range (5-10 year) choices for standards and vendor approvals. Protection Engineering delivered specific project-related designs and configurations. From there, Engineering would coordinate procurement and installation of projects, commission them with support from Construction, and hand them off to Maintenance and Operations. The Maintenance Division was then responsible for keeping the installed equipment operational.

Relay terminals for transmission substations would consist of a mixture of electromechanical relays, switches, some first-generation digital relays, and basic forms of access to configure relays and transfer data to an RTU and on to the EMS system, using some combination of polling via a permanent leased line and report by exception. Where there was a requirement for WAN-level data transmission, the Telecommunications team would arrange for channel bank or frame relay access as applicable. Departments were essentially “silod”. In this earlier period of design standards, logic was binary and supplied by multiple hard-wired status and relay position inputs, and in many cases direct operator control. Similar to its predecessors, the electromechanical and the solid state technologies, the selection and application of first generation microprocessor technology was specific to a site and to local operational and engineering requirements.

As the ‘90s progressed, the Information Age expanded its reach into industrial applications including the Power System industry. First-generation digital relays became second-generation digital devices, no longer putting out small strings of serial data; but instead, crisscrossing the wires with parallel data streams conveying 3D color graphic Comtrade files in excess of a megabit. Engineers began discussing phasers and synchro phasers and constraints on bandwidth! The medium was no longer RS-232 but copper or fiber 100 Megabit Ethernet.

PG&E decided to create a new paradigm that encompassed design criteria, standards, procurement methods, and expectations for stakeholders such as Operations, Planning, Engineering, Maintenance, and Asset Management, as well as requirements from other divisions such as Information Technology. Even prior to 9/11, pressures were driving these changes. There was a conjunction of: upcoming retirement for high numbers of skilled technicians, operators and supervisors; better automation technology; deregulation; and technology advances that seemed to change again even as the engineer was just finished evaluating the last set of changes. PG&E’s challenge was to make a paradigm shift, get buy in throughout the organization, and do it in a way that would incorporate technology migration into the very standards and designs.

II. THE PROCESS

A. Background

From about 1999 to 2002, a Program Manager, and principal technical team members held a series of meetings designed to qualify suppliers, inform stakeholders, train field technical staff, and familiarize engineers with new products [1]. Starting with the concept of a modular protection and control “drop in” prefabricated building (a concept that had been done as an experimental project at one location at PG&E in the late ‘90s), new standards were developed focusing on modularized protection, control and automation while
eliminating nearly all electromechanical relays, auxiliary relays, and switches in the relay terminals. Field hard-wired input and output, and thus labor, were reduced. Additionally, new devices appeared — earlier dial-in port switches were supplemented with serial servers that would move data onto Ethernet protocols and media. Ethernet switches were needed to facilitate communication and status information of both the Ethernet capable devices and the actual data network. WAN access devices appeared as part of the relay terminal/control building, and functions such as routing and firewalls were discussed. For the first time, Ethernet communications and the idea of an intelligent substation network were a part of the design standard.

The Modular Protection and Control (MPAC) program and process took time and a deep commitment from management and staff, and from key vendor management and technical personnel, as well as a willingness to move ahead with significant change by the stakeholders who would “live with” the new concept and systems, Figure 1. The intent of the program was to address aging infrastructure and take advantage of offerings of the new technology, in addition to other previously mentioned drivers. PG&E initially set a target of reducing costs by 20%; with an ultimate goal of 30%. The new design included a prefabricated building and key vendor support with modularized design and implementation that would provide significant savings via a standardized process which included Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT), selected as main suppliers for protective relays after careful evaluations with the idea to expand once the process was further refined. All participants agreed to build on each other’s knowledge and committed to helping one another in the development of features as needed and options such as specific firmware versions, preconfiguration of general parameters, custom labels for panel interfaces, or development of wiring or cabling diagrams as applicable. Within the concept development process, tasks were treated as projects with timelines, budgets and deliverables. Partnering strategies, evaluation of vendor’s responsiveness, and evaluation report cards were included as part of the process.

The report cards include overall quality in engineering, procurement, design, construction, FAT, and building delivery to project site, and are reviewed twice annually between key project sponsors and management. They have proven to be an invaluable part of the process.

![Figure 2. Simplified Task Selection Diagram](image)

**B. Task Selection**

As part of the task selection step, the development of engineering and protection and control standards was a key factor in making the MPAC program successful. Partnering with product vendors and building manufacturers was identified as a requirement. In addition, the need for vendor selection criteria, as well as the areas of responsibilities between the power company and individual manufacturers, had to be defined, Figure 2. Two vendors were initially
the respective building manufacturing site shortly after wiring verifications were completed to assist in the in-depth logic and FAT process. The process also supported having start-up engineering team members to provide training to the internal PG&E resources as well as when other building manufacturers would be added.

As of the fall of 2007, the utility has installed 15 transmission buildings with 14 operational, and a goal of 200 buildings by 2014.

D. Impact on Data Management

From an operational data management perspective, the architecture of MPAC was a significant step forward. In the mid 1990s, a typical substation would have hard-wired contact status feeding into an RTU, and some first-generation digital relays, which could be accessed via a port switch and modem. Data rates of 1200 or 2400 Baud were typical. The RTU was the gateway for data going to the EMS system. There was no substation “network” per se. Different manufacturers had different interface tools and protocols, so communication to devices required specific knowledge and software. For maintenance and asset management, little data was available.

The required functions identified were WAN connectivity and Routing, along with Ethernet and serial connectivity. The data clients included the EMS system, protection engineers, maintenance and operations and in some cases third parties like the California Independent System Operator (ISO).

By the late 1990’s, major suppliers were pushing for direct Ethernet connectivity to IEDs and ideas were circulating about a common “language” to allow interoperability among IEDs in a substation, or among substations. In the western part of North America for example, the Remedial Action Schemes (RAS) required coordination of information and action over large geographies and across state boundaries. Soon, the ISO and RTO organizations (driven by FERC requirements that have been, in part, a response to some widespread blackouts) were asking for access to real-time data, via a separate RTU device from yet another manufacturer.

As the industry was moving toward a global standard for IED interoperability, the use of Ethernet networks had become much more attractive, with the benefits of speed, bandwidth and routing capabilities, along with the transparency to protocols including, DNP, Modbus and most recently the IEC 61850 standard. Now, in addition to immediate productivity improvements, the power company and the industry can take advantage of an architecture that will be extensible for compatibility with new requirements and the capabilities developed to support them.

E. MPAC Data Management and Network Architecture

The new MPAC standard bridged the gap between first and second generation IEDs. Serial multiplexers (or serial servers) coexisted with managed Ethernet switches, a substation computer, a router and WAN connectivity, Figure 4. This powerful data management structure has the ability to use Virtual LANs (VLANs) to manage operational versus non-operational data, provide better access and bandwidth for protection data like phaser measurements, COMTRADE files, settings file management, or even firmware upgrades. It opens the door to the need for, and the ability to manage stringent higher level secure access control, logging functions, data security and record keeping. Coincidentally, these capabilities, common in IT networks (think email, corporate Intranets, online banking) are key elements of NERC CIP Cyber security.
manufacturers. Several functions in the communication architecture had some overlap, and not all functionality for interoperability had been completely incorporated. In effect, much of what had been hard-wired between devices in the conventional approach (e.g. between numerical devices and switches, or with auxiliary devices, and electromechanical relays) would now be managed through digital relays. However, there was still a fair amount of hard-wired status information that needed to be collected along with the information traveling from CPU to CPU in a purely software environment. In the first 4 years of MPAC projects being built and commissioned, both the data management requirements and the technology available proved to be areas of both challenge and opportunity.

F. Security Overlay

When a modular protection and control program was first conceived and discussed in the late 1990s, security – whether for data management or physical access to substations and control buildings, – was already one of the considerations for any automation and network or remote control application. The post 9/11 and post northeast blackout focus by FERC and NERC served to amplify and to a degree, formalize that consideration.

As implemented today, the integrated substation communications architecture developed by the power company is very close to plug-and-play for NERC CIP cyber security requirements, Table 1. With the addition of security management software, typically located outside the substation firewalls, determinations can be made as to whether the CIP standards have been successfully implemented. One of the questions concerns demarcation and boundaries, both physical boundaries and when discussing data management, virtual boundaries. To some extent the standards are open to interpretation. For example, per CIP-005, the utility must define an Electronic Security Perimeter (ESP) and develop actionable plans to address securing that ESP. Some of the questions facing the industry include:

- “Where should we as the industry draw the box?”
- Does cyber security stop at the router/firewall device?
- Does cyber security extend to the edge of the IP addressable network? Or even to the IED’s themselves at a peer to peer level? (Picture a Remedial Action Scheme project where peer to peer may be separated by significant distance)

Additionally, points of access to data create security concerns: what kind and how many paths can be supported out of a list that includes dial up, LAN and WAN access, leased lines, and ISO RTU links? These are among the topics the industry must consider in shaping the next iteration of protection, control, networking and substation automation design standards. Table 1 is a summary of which Network Device functions relate to which CIP sections.

| Managed Ethernet, Router, WAN and Serial Server |
| NERC CIP Compliance Solution Relationships |
| Electronic Security Perimeter – CIP-005 |
| WAN Firewall | • IP/ICMP Filters (address/port access control) |
| | • Policing, QoS, and packet marking |
| Ethernet Port Security | • Sniff MAC security |
| | • ISL or VLAN tagging |
| Serial Port Security | • Serial port IP and port filtering |
| | • Serial port SSL authentication and encryption |
| System/IED Access Control – CIP-007, 4, 5 |
| Individual Profiles | • Central administration of individual users |
| | • Authentication/authorization of permitted applications for end user access use |
| Strong Authentication | • Two-factor authentication via integration w. RBA and/or PAM, 2 step/multi-factor authentication systems |
| | • Strong authentication using PKI and/or smart cards |
| Session Logging | • Log of system activity and access authentication attempts |
| | • Log of system activity and access authentication attempts |
| Network Management Security – CIP-007 |
| | • Log of session access (application, device, and user) |
| Security Policy | • Security policy management |
| | • FTP access via SSL, IPsec |
| System Recovery – CIP-009 |
| Backup Networking | • Multi-socket, multi-client support for Serial SCADA applications |
| | • RASP and RATS for application security |
| | • RADIUS support for authentication |
| System Security | • Hardened systems, frame and packet filtering, dynamic IP routing and URRM, and Ethernet RSVP |
| | • Edge firewalling and configuration files |
| | • Scripting support for configuration management |
| Asset Classification – CIP-003 |
| | • Critical Asset and Transition Options |
| | • SCADA Forwarding options for non-critical alternative for remote SCADA consolidation |
| | • Provides transition planning option to avoid classification of Critical/Cyber Assets |

Table 1. – NERC CIP Compliance standards’ CIP 002-009 Relationships to Network Devices and Functions

G. IEC 61850 Overlay

The MPAC data network architecture supports 61850, however there is much more capability that has yet to be implemented. Physically, considering the availability of the Ethernet network and the capability of the majority of IEDs, there is not much to change, other than allowing more digital and analog status information to flow as pure data rather than hard-wired I/O. The utility is taking an incremental approach to this, in part because this helps the organization and various stakeholders become more comfortable with “trusting” automation, Ethernet substation networks and digital IEDs. There is also the consideration that utility stakeholders need to absorb the engineering, maintenance and operational impact of much more data being available, turning that into information or knowledge of practical use in real time.

The potential benefits of implementing more of IEC 61850 are further reductions in cost and increases in reliability. The choices made through consensus building, and the planning and selection of suppliers aligned PG&E with vendors that are industry leaders with their technology plans and migration paths in place. Using this process, the utility is in a position to work with and select from multiple 61850 compliant manufacturers, choosing best in class IEDs to suit their applications and establish substation network and data management standards that will be forward compatible. With the modular control building design paradigm, IEC 61850 compliance extends out to the network devices, some software applications and other ancillary IEDs.
This leads to a very logical question... what next?

**H. MPAC II, the next level**

Currently in discussion and early design stages, at both Distribution and Transmission levels, updated designs for the next generation of MPAC projects will address both 61850 and Cyber Security opportunities and challenges. Now that the utility has completed the development of the modular protection and control concept, proved it and implemented it at the transmission level, it can be refined and carried out to future transmission projects and to distribution substations and switchgear. This concept includes a lot of messaging (IEC 61850 for protection and control) that will apply to distribution switchgear. At the utility today, IEC 61850 is used for control and interlocking, a next step in implementing 61850 could be to utilize it at the automation level to replace the DNP protocol.

With the availability of substation hardened switches, serial servers, routers and WAN access devices, now available from some suppliers in one product) the data and network can have full intelligence. That is, the data and the network itself become critical assets, thus, there is an advanced IT-style look to the substation network, Figure 5.

Bandwidth is extended to the IED’s at the very edge of the network, in the substation, or in switchyard monitoring IEDs; IP addressability is maximized; hardened substation computers with all flash memory and no moving parts can provide additional data management or a “wide spot in the line” and local access to the system; data can be selectively channeled through the same “pipe” (think IP video for security, card access authentication, operational and non-operational data, and engineering access for protection information); data can be “pushed” to upstream clients further limiting required access and security risk; and full security (strong passwords, logging, access control) can be implemented and managed through one “fat pipe” into the substation, with very high security and redundancy as required. This network architecture allows maximum advantage for using best in class IEDs, and going back to the stakeholders (as data clients), they can receive data in formats and classifications relevant to their specific applications (EMS, OMS, Asset Management, predictive maintenance, ISO and NERC CIP requirements). Advanced function or capabilities in securing the network and the data may be utilized including VPN and encryption, Secure serial port and serial-IP management, strong passwords, SSL and static MAC addresses, Filtering and Firewalls.

**I. Conclusions**

For large, medium and small utilities this is a valid approach to solving several important challenges facing power utilities today – a modularized, scalable, standardized protection and control, networking and automation platform that meets the needs of today and tomorrow: Reliable operations, using best quality state of the art devices, systems and processes; Managing change, whether that is in personnel, business operations, technology or construction and project management; Compliance, for FERC, NERC-CIP and homeland security, and for regional or local regulatory bodies (ISO, RTO). As the technology and information age move ahead, data is transformed into information which yields knowledge. Facilitated by automation, intelligent devices and high speed intelligent networks, the “brains” of these intelligent systems - the software management, monitoring and analysis tools - will enable the engineers, technicians and managers in current and future operations to meet the needs of their internal clients, their actual customers and interested stakeholders with reliable, robust, efficient systems that will not become suddenly obsolete, but actually enable forward migration of technology and information.

**III. REFERENCES**


**IV. BIOGRAPHIES**

**Charles E. (Ted) Witham, PE, MBA,** director of International Business Development at GarrettCom, Inc., has 20 years experience in industrial measurement and control, with 15 years of specialization in power industry generation, transmission and distribution. In addition to GarrettCom, Witham has held technical and sales positions with companies including General Electric Company, Honeywell Industrial Automation and Control. He was licensed as a Professional Engineer in Control Systems in 1995 and is a member of BICSI, the National Society of Professional Engineers, Instrumentation Society of America and IEEE.

**Vahid Madani** is a Principal Protection Engineer at Pacific Gas and Electric Co. (PG&E). His responsibilities include 500kV transmission, reactive compensation, series capacitor protection and controls on EHV systems, single-phase tripping and reclosing schemes, transient and real time simulations, wide-area disturbance monitoring and prevention, protection and control equipment evaluation, substation integration and automation, and policies and standardization.

Vahid is a registered Electrical Engineer with more than 24 years of academic and utility experience and recipient of many honorary and distinguished awards, for his leadership and contributions to the power industry and education. Vahid is a Tau Beta Pi member and has a MS Degree in Power system from University of Idaho.

Mr. Madani has various technical, advisory, and leadership roles within the North America and Internationally. He is Chair of the Remedial Action Scheme Reliability Subcommittee in the Western Electricity Coordinating Council (WECC) and recipient of the outstanding Chair Person award from WECC. Vahid is also Chair of the IEEE Working Groups and member of CIGRE Study Committee (SC) B5 (Protection and Control) and C2 (Power System Operation).

Mr. Madani has contributed to the development of many advance applications (theory and implementation) in power system protection. Vahid has been an invited author, speaker and panelist at CIGRE, DistribuTech, EPRI, IEEE-PES, IREP (International Institute for Research and Education in Power Systems), and the World Energy Systems conference (WESC). He has authored more than 50 publications in system automation, protection & controls applications, and practical wide-area monitoring systems with advance warning and fast restorations. He is the Guest Editor of the 2007 Edition of International Journal of Reliability and Safety (IJS) for InderScience Publishing, published in UK and Switzerland.