Remote Operational Monitoring and Control of Auxiliary Process Units and Electrical Systems

Michael E. Rourke
Schweitzer Engineering Laboratories, Inc.

Presented at
AISTech 2012 – The Iron & Steel Technology Conference and Exposition
Atlanta, Georgia
May 7–10, 2012

Remote Operational Monitoring and Control of Auxiliary Process Units and Electrical Systems

Michael E. Rourke
Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, Washington 99163
Phone – (509) 332-1890
Fax – (509) 336-7955
Email: Michael_Rourke@selinc.com

Key words: Power Plant, Water Treatment, Pumping, Remote Monitoring, Security

INTRODUCTION

Auxiliary process units (APUs), such as power plants or water treatment facilities, serve key roles in supporting operations and maintaining regulatory compliance. Minimal staffing, remote locations, and harsh environments make the control and monitoring of these units even more challenging. This paper describes field-proven control technologies and methods to remotely control and monitor these units in order to improve process visibility, optimize staff deployment, increase monitoring equipment reliability, and maintain regulatory compliance. It includes a discussion of integrated web-based operator interfaces, the application of network security mechanisms, and appropriate control system environmental specifications.

Auxiliary Process Units

Consider the significant vertical integration in many modern industrial plants, such as steel mills. Well beyond the primary business purposes of the facility, owners and operators invest in capital equipment, expertise, and staff for APUs. In some cases, these facilities exist to increase direct control of operations and reduce costs. Electrical generating facilities, steam boilers, large-scale air compression and handling systems, and process water preparation equipment are all examples of this. The investment in this type of APU is dependent on improving operations and/or reducing costs. For example, the local electric utility might be an excellent source of high-quality bulk power for normal operations, but the mill may continue to experience occasional service interruptions that cause the shutdown of operational facilities. By operating a captive generating facility (either using mill waste streams as fuel or stored external fuel), the mill has the ability to continue operation of critical facilities during electrical service interruption and possibly add the surplus generation as a new revenue stream. Beyond the direct advantages, the operation of and information from these facilities provide plant operators with valuable knowledge related to the manufacture and supply of critical inputs to the steel-making process. This new expertise aids personnel in dealing knowledgably with external suppliers when issues arise.

Most mills also operate APUs installed for the purpose of maintaining regulatory and environmental compliance rather than reducing operating cost. Examples may include wastewater treatment plants, airborne emissions reduction units, or waste process fluid capture equipment designed to remove materials not treated as part of wastewater plants. Due to external oversight and auditing, high availability and continuous monitoring need to be part of these solutions. In some cases, operating mill facilities may need to be shut down if the operator cannot verify that environmental systems are working properly.

While they may be needed (or mandated), APUs designed to maintain regulatory compliance are not the primary facilities that managers consider when evaluating potential capital projects. Some plants have reported that many of these facilities continue to use control system equipment nearly as old as the original installation.[1] Two situations may arise that cause the facility and controls to undergo a modernization. The first situation occurs when the age and performance of the facility make it too costly to operate, requiring significant personnel. The second is when new regulations require performance beyond the capability of the existing equipment. For example, new environmental requirements enacted by the United States Environmental Protection Agency or other regulatory agencies may be unattainable with the installed equipment. In such a case, plant managers may be faced with a requirement to upgrade the capability of control systems before regulators will allow them to renew air or water discharge permits.[2]

Regardless of the need for or primary purpose of the APUs, they do not function as part of the primary plant operations. They are frequently staffed by a nonoperations support department and are commonly located well away from the mill. An illustration of this can be seen in Figure 1. Operating companies have significant incentive to minimize staff because APU operations are managed more like an overhead cost rather than a direct cost of production.

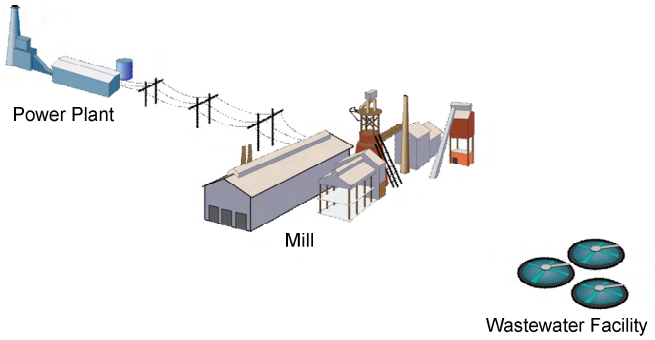

Figure 1. Remote APU locations impede the monitoring of system performance

In the end, though these ancillary APUs are not monitored or controlled by the plant control system, they have become a contingency for its safe and continued operation. Visibility and future control of these APUs are becoming essential to the control system because the failure of these APUs can force suspension of the control system application.

Operational Challenges

The combination of aging equipment, increasing regulatory requirements, and pressure to reduce support staff puts the plant managers in a difficult position. To make matters even more complicated, many APUs are exposed to harsh environmental factors because they reside outside the primary mill structures. These environmental factors may include temperature extremes and exposure to waste stream components, which can be very damaging to electronic components. Such exposures can add maintenance labor and repair costs to a facility that is already searching for labor cost reductions.

Cybersecurity is a relatively new concern for APU operators. In the past, the primary focus for control systems has been performance and reliability.[3] Stuxnet, Duqu malware, and other cyberattacks have made everyone aware that control systems are potential targets for hackers and other groups. We cannot safely and effectively deploy remote monitoring and control equipment without understanding the practices and technologies that promote secure operation as well as secure, dependable, and deterministic communications.

When considering control system upgrades or new installations, designers need to consider how to specify and deploy technology that meets the economic requirements of the project, performs the intended functions securely and reliably, and provides process visibility and staffing flexibility. This paper deals with the technology, testing, security, and performance of protection, control, and monitoring (PCM) equipment for a variety of APUs in iron and steel facilities.

TECHNOLOGY AND DESIGN METHODS

Automation system manufacturers offer a wide variety of equipment choices for remote control and monitoring devices. Device attributes related to environmental performance, security, and overall capability have a large impact on the long-term reliability of an APU control system.

Design and Testing Suitable for Harsh Environments

The intended operating location and environment are important design considerations for any control system. In the case of many APUs, there are physical characteristics that complicate installation and upgrade programs,[1] [2] including the following:

- APUs are located remotely from primary operating facilities, as shown in Figure 2.
- The control and monitoring equipment can be exposed to more harsh environmental conditions than the operations within the mill building complex.

Figure 2. Monitoring systems are exposed to diverse environments

One option for these types of installations is to install the electronic control devices in a cabinet that includes climate regulation accessories. However, the required heating and cooling equipment that is part of these types of installations increases the initial project cost and system maintenance costs. In actuality, this is an admission of design failure due to the fact that the equipment does not meet the specification. This is done when designers choose devices that are not acceptable for the application and then add environmental modification equipment to mitigate risk. This permits the control devices to work until the environmental management fails and disguises the design flaw of poor product selection. As with many similar design choices, when done frequently or because no better alternative is readily available, this improper product selection becomes common and even accepted. This practice disguises the fact that products will fail sooner and more often but after the designer is no longer responsible. Inopportune failure coinciding with a malfunction of an APU component can turn a simple issue into a catastrophe.

The other option is to specify hardware that is intended to operate over wide operating conditions. Manufacturers that specialize in hardened systems, such as PCM applications, understand that unique design and testing processes are needed to ensure that users experience reliable operations under difficult circumstances. Design considerations for extended temperature operation without the loss of reliability include the following:

- Self-tests and alarms
- Elimination of moving parts
- Use of appropriate components and design margins
- Heat reduction and addition methods

Many embedded control platforms provide continuous internal self-tests and performance monitoring. If the self-test identifies a problem, the device automatically signals the alarm condition via fail-safe contacts.[4] Monitoring these alarms dramatically improves overall system availability because operations and maintenance personnel receive immediate notification of system alarms and failures. The alarm pinpoints the root cause of the problem and facilitates immediate corrective action to limit system downtime.

An important design attribute of PCM devices is the operating temperature range. When installed, if the system is exposed to widely varied temperatures, then either the devices need to be rated to operate in those extremes or the installation needs to protect the electronics from the ambient temperatures. Cabinets with heaters and air conditioners not only add significant expense to the initial

project but also add more maintenance costs to the system over its lifetime. Therefore, the control equipment should be rated for operation at the needed temperature. These considerations have a large impact on long-term system reliability because the useful life of electronic components can be reduced by as much as 50 percent by even a relatively small violation of rated temperature.[5] Table I provides some commonly used temperature ranges for control devices. Devices designed to operate for a long useful life at high temperature ranges also exhibit much greater longevity than commercial and industrial devices in environmentally managed installations. Larger temperature ratings are one of the main attributes that help users predict life expectancy and reliability.[6]

Table I. Categories of temperature ratings

Category	Temperature Range
Commercial	0° to +50°C
Industrial	–20° to +60°C
Extended	–40° to +85°C

The methods used to remove heat from electronic instruments are also an important consideration. For instance, conduction and convection methods can effectively remove heat from an instrument chassis without introducing moving parts that can be susceptible to failure. On the other hand, many devices use forced-air methods, like fans, to remove heat from the chassis. Users need to consider the reliability of these components as part of the overall product evaluation.

In addition to temperature ratings, designers need to evaluate the electrical and mechanical specifications in order to provide the needed margin based on their operating environment. Important mechanical tests include vibration resistance, shock resistance, and seismic protection. Based on the geographic location of the installation and nearby equipment, such as gantry cranes, control equipment can be exposed to significant mechanical forces that can damage inappropriately hardened devices. Root-cause analysis of recent generator failures shows that severe apparatus vibration was present and would damage commercial and industrial control system components at the time they were most needed to operate properly.

IEC 60255 and other industry standard specifications define electrical standards used to describe the susceptibility of an instrument to applied aberrant signals, such as electrostatic discharge, surge withstand, and impulse resistance. Manufacturers must test their products in accordance with the tests defined in the standard in order to claim compliance with the standard. Some tests provide multiple severity levels, so two similar products may not provide the same protection even if both list compliance with the same portion of the standard.

Radio frequency immunity (RFI) and interference tests determine how an electronic device will operate in the presence of nearby radio signals. In a mill environment, these tests are particularly important due to the wide use of portable two-way radios by operations and maintenance personnel. Without proper immunity, an electronic device may shut down or misoperate if a nearby radio is transmitting.

The presence of corrosive materials in the APU process materials is very common[7] and can significantly reduce the reliability and longevity of electronic devices. Conformal coating is a flexible material that covers the components on a printed circuit board (PCB) and provides a barrier against airborne contaminants, such as hydrogen sulfide, chlorine, or salts. The coating also resists dendrite growth between conductors on the PCB and is moisture resistant.

Security and Remote Communications

The remote and varied locations of APUs also create networking and communications challenges.[8] In cases where directly connected networks are not feasible, wireless remote communications are an increasingly popular option. Within short distances, IEEE 802.11 Wi-Fi® communications for I/O networks are a viable option. For most APUs, the distance is too large to use these methods. Leased

cellular or microwave networks provide the needed distances but can be costly. Licensed and unlicensed radios can also be used to provide these links. Figure 3 illustrates the cost differences for a variety of communications mediums.[9] As we can see, unlicensed radio can be a very economical choice for these links, compared with the other options.

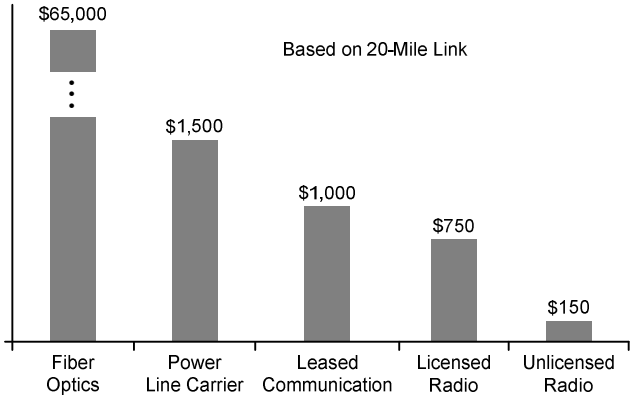

Figure 3. Comparisons of cost per mile for communication

When evaluating unlicensed radio purchases, users need to be aware of the allowed operating parameters for their region. There is no worldwide standard for operating frequencies; each country or region sets its own standards. For North and South America, the industrial, scientific, and medical (ISM) band at 915 MHz is commonly applied. Because these are unlicensed frequencies that are shared by multiple users, most radios operate with spread-spectrum or frequency hopping techniques in order to reduce interference.

These radios generally operate in line-of-sight applications over a maximum distance of 20 to 30 miles. For most plant locations, a range of less than 5 miles is sufficient. If the APU is not in direct line of sight due to local geography, system designers will install repeaters to support the communications link. As shown in Figure 4 and Figure 5, the radio links can be configured in a number of ways. Point-to-point links provide a channel between two locations, while point-to-multipoint configurations allow a master (M) site to communicate with multiple remote (R1 through R4) stations. Each wireless connection may support multiple serial communications connections, so an individual radio is not required for every end device in the field.

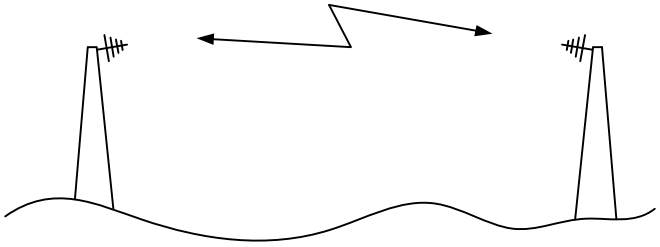

Figure 4. Point-to-point radio application

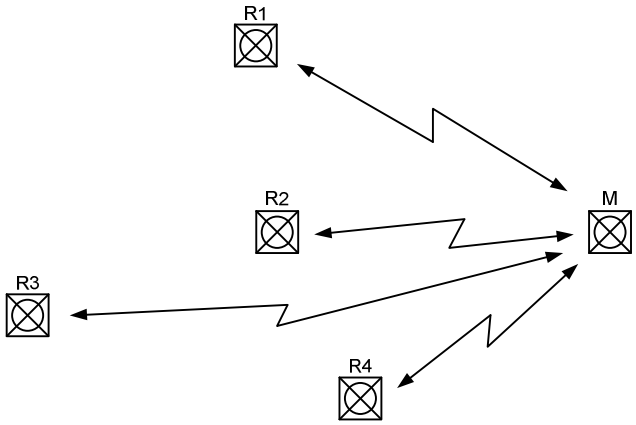

Figure 5. Point-to-multipoint radio application

While all communications and networks in a control system need appropriate security measures, radio links are an obvious application that needs rigorous security analysis because process data and control commands will be transmitted wirelessly. Industrial control systems have not been a major target of hackers or cybercriminals in the past. Business or commercial computing systems were the main targets and received most of the resources for cybersecurity. Attacks such as Stuxnet help us understand that industrial control systems are increasingly seen as a target for cyberattacks.[10] Disallowing remote connections to the control equipment (electronic barrier) is no longer a sufficient security measure; some of these attacks were initiated through portable Universal Serial Bus (USB) drives connected by employees or manufacturers who were not aware that their portable drive was infected. Serious, diligent, and mature enforcement of a policy that minimizes external device connections and requires prior scanning reduces the carry-in threat and is the responsibility of all designers, operators, and technicians—no exceptions. Encryption of process data that are transmitted over nonsecure networks, like radio, will further reduce the potential access points for cybercriminals. Insist on communications equipment that supports sophisticated encryption methods, such as the Advanced Encryption Standard (AES) algorithm. The United States government uses AES encryption for transmitting data up to the top secret level. A number of industrial radios and networking devices exist today that provide AES encryption as an option.

Electrical System

As on-site electrical generation becomes more common at iron and steel facilities, operating companies are becoming more aware of the cost and reliability advantages of modernizing the PCM and communications equipment related to electrical transmission and distribution within the plant.[8 11] Pumping stations, compressors, and other APUs use significant electrical energy and require reliable protective relay support. Many modern relays are specifically designed for operation in tough environments and secure, remote communications.

Highly accurate electrical meters have almost exclusively been used by electrical utilities in the past due to the cost of these devices. However, newer meters are available that are affordable for use at multiple locations in plants, include advanced metering capabilities, and provide simple integration and communications features.[11] Variable frequency drives and other switching power supplies commonly used in APU processes can create harmonic content in the electrical distribution network. This harmonic content needs to be monitored and managed. Local electric utilities may require industrial customers to maintain minimum harmonic feedback into their grid. Meters available today provide advanced harmonic metering that gives users the ability to identify sources of harmonics in the plant and reduce their overall impact, as needed. Distributed metering also provides visibility of the power consumption of each cell or operational bay within the mill to enable better process optimization and scheduling for efficient power consumption based on decision-making metering information.

Control and Monitoring Devices

Properly choosing control and monitoring devices for APU installations is a critical design step for any upgrade project or new installation. In this section, we discuss a number of control equipment categories and potential applications for each.

Remote terminal units (RTUs) and programmable logic controllers (PLCs) have been widely deployed as the primary control devices in APUs for many years. Improvements in processing power and flexibility in many RTUs and PLCs help users advance the reliability and stability of many processes. As discussed in earlier sections, the environmental design and secure communications capabilities of the controllers also need to be evaluated during the specification stage of new projects. Manufacturers of controllers for mission-critical industries, such as power system protection and control, have recently introduced PLCs that are designed to operate over extended temperature ranges, provide conformal coating for PCBs, and support the traditional IEC 61131 programming interfaces familiar to mill automation designers.

Because of tighter regulatory requirements for waste processing and recycling units, the installed PLC needs to enforce deterministic I/O processing and logic in order to maintain the mandated stringent process tolerances.[12] In some regions, the plant is required to provide accurate logging of waste processing as part of the permitting process. Some manufacturers provide the capability to synchronize the PLC system clock to satellite Global Positioning System (GPS) signals and thereby log process signals with precise time stamps. In this way, logs from multiple PLCs are automatically time-aligned without postprocessing. When required as part of a design, accurate time distribution and device clocks provide an accurate representation for forensic analysis of what happened and when. Further, accurately time-stamped and recorded change-of-state events serve to verify and document field commissioning tests for due diligence review and audit.

In addition to the data security discussed previously, engineers should also evaluate the access and user security provided in control devices. In order to reduce system administration tasks, look for PLCs that support central authentication for user accounts. This capability allows users to use one password for desktop and control system computers. Also, system administrators can manage user account policy changes from one server rather than traveling around to implement policy changes on multiple systems.

While RTU and PLC systems provide most of the I/O for APU controls in monolithic cabinets filled with field wiring termination panels, many installations have some I/O points that need to be connected to the control system via remote I/O modules. Also, distributed instrumentation and processing modules reduce cost and simplify installation of new and retrofit I/O. These modules generally have a small point count, standardized automation capabilities, and largely fixed functionality. Easy integration with the primary PLC, simple logic and scaling functions, and low cost per point are important considerations when choosing remote I/O.

Modern mill control systems employ equipment monitors to provide apparatus protection and decision-making information for asset management and predictive maintenance programs.[11] These specialized instruments help operators monitor the process, while, at the same time, evaluating the physical performance of actuators, motors, and other mechanical devices. For example, a pneumatic valve positioner might be monitored for movement initiation pressure and travel drift. Operations and maintenance personnel can use trends of these types of signals in order to diagnose pending equipment trouble well in advance of process upsets or failure.

Traditional human-machine interface (HMI) and supervisory control and data acquisition (SCADA) systems allow operators to monitor and alter process parameters in a very user-friendly format. However, flexibility and portable viewing were not strengths of these systems. Some manufacturers have added web-based clients to HMI software suites, but users need to have a complete HMI infrastructure in place before deploying these portable tools. New PLCs that directly provide fully customizable web-based HMI systems without the cost or complexity of installing a complete HMI network improve reliability and reduce complexity, which both increase availability. The central processing unit (CPU) of the PLC hosts the web sessions, screen graphics, and process values and/or statuses. Within the limits of the PLC, any accredited user with network access can monitor process functions. If operators have a concern about the performance of a particular piece of equipment, they can contact the maintenance department, who could remotely view the HMI screens and potentially resolve the issue without dispatching any personnel to the APU.

BENEFITS

With an understanding of the technologies and products that can support APU control and remote monitoring, we can now look at some expected benefits from the technologies and methods previously discussed. This section addresses how these technologies are used to improve process visibility, staff deployment, equipment reliability, and regulatory compliance.

Process Visibility

Standalone APUs without remote monitoring, such as a pumping station, often suffer from alarms or faults without initiating any response from maintenance or operations personnel. Secure radio connections and web-based HMI clients provide immediate notification and improved decision making. Additionally, process signals are integrated with production facilities in order to automate downstream responses to changes in APU status. For example, noncritical production could be temporarily stopped if there was a reduction in production of deionized water or compressed air.

Additionally, all the monitoring and alarm inputs that provide better visibility to the mill and APU processes also provide a well-documented audit trail of performance and maintenance.

Staff Deployment

As previously mentioned,[1] the combination of outdated automation systems and tightening of regulatory and operating requirements causes increases of operator intervention in an APU process, while the business need is to improve process performance and, at the same time, minimize operating staff for support facilities. The deployment of technologies such as those discussed in previous sections enables proper control and communication within and between APU sites that may be scattered around a facility. These modern solutions allow operating staff to be centrally located, maintain immediate visibility of several important processes, and minimize the need for direct operator control actions. Even when operator intervention is required, remote HMI systems allow operators to make process changes without traveling around the plant. This not only saves time and labor but also reduces safety concerns due to potentially bad driving conditions during inclement weather. The combination of more reliable systems and remote controls allows managers to optimize the deployment of support staff. As discussed previously, few APUs are profit centers for the mill. Any reduction of APU staff is a cost benefit for the overall operation. Using this field-proven technology allows skilled staff to focus on process improvements and mill profitability rather than tedious and repetitive monitoring and control, which are now automated. Additionally, PCM devices make skilled and automatic decisions based on field data and are not swayed by the emotional consideration of the consequences of the control decision. Emotion and indecision often delay and influence dramatic but important safety and availability decisions.

Manage Reliability and Regulatory Compliance

When evaluating new installations or upgrades, specifying control devices that are designed to operate in the APU environment reduces the installation cost and improves long-term reliability. As we have discussed, wider temperature ranges are one of the best predictors of equipment longevity in exposed and protected environments. Cybersecurity requirements, regulations, and auditing are happening now within industrial control systems, with the expectation to grow more comprehensive in the future. Electric utilities have already been declared critical assets and placed under significant regulation for cybersecurity. PCM products that serve this industry, and now industrial processes, have decades of successful cybersecurity management features embedded in the devices. While most industrial manufacturers are not presently subject to or acting on these regulations, the recent instances of cyberattacks targeted at industrial control systems make similar regulation more likely in the future. Regardless of compliance with regulation, strong cybersecurity performance is now a required design criterion for high availability.

SUMMARY

APUs are critical for the economical operation and regulatory compliance of steel facilities. Plant managers recognize that many of these units are operating with aging process equipment and obsolete control systems that cannot meet updated licensing requirements. Minimal staffing, remote locations, and harsh environments make the control and monitoring of these units even more challenging. This paper explains field-proven control technologies and methods to remotely control and monitor these units in order to improve process visibility, optimize staff deployment, increase monitoring equipment reliability, and maintain regulatory compliance. The discussion of integrated web-based operator interfaces, application of network security mechanisms, and appropriate control system environmental specifications illustrates the benefits to mill control centers and APUs. Although new to the instrumentation and control industry, technologies presented here have been used successfully in mission-critical power generation and delivery systems for years.

REFERENCES

1. M. Lamb, S. Adamowski, F. Jere, and C. W. Kiesling, “Biological WWTP for Coke Battery Wastewater Discharge: Design, Construction and Start-Up Challenges and Solutions,” *Proceedings of the 2009 Association for Iron & Steel Technology Conference*, Vol. 1, St. Louis, MO, May 2009.

2. G. Amendola, J. Flannery, and M. Olthof, “Upgrades to Process Water Treatment Systems for Hot End Operations at ArcelorMittal Indiana Harbor West,” *Proceedings of the 2008 Association for Iron & Steel Technology Conference*, Vol. 1, Pittsburgh, PA, May 2008.

3. R. M. Lee, “Cyber Warfare and the Control Systems Community,” *Control*, December 2011, pp. 14–16.

4. R. D. Kirby and R. A. Schwartz, “Microprocessor-Based Protective Relays Deliver More Information and Superior Reliability With Lower Maintenance Costs,” IEEE Industrial and Commercial Power Systems Technical Conference, Detroit, MI, May 2006.

5. F. Gutierrez, R. Moxley, D. Kopcynski, and D. Holmes, “Relays in the Hot Box,” proceedings of the 32nd Annual Western Protective Relay Conference, Spokane, WA, October 2005.

6. M. B. Watkins and M. Zeller, “Ensuring Recloser Control Compliance With IEEE C37.60-2003 Testing,” proceedings of the 5th Annual Power Systems Conference, Clemson, SC, March 2006.

7. D. Konaré, S. Pierre, J. Y. Weng, and E. Morand, “Real-Time Image Processing for Remote Sensing,” Canadian Conference on Electrical and Computing Engineering, Montreal, Canada, May 2003.

8. A. Kar, D. M. Chowdhary, and R. Jeloka, “An Industrial Power System Management for High-Quality Uninterrupted Power Supply at Tata Steel,” *Proceedings of the 2010 Association for Iron & Steel Technology Conference*, Vol. 2, Pittsburgh, PA, May 2010.

9. S. V. Achanta, B. MacLeod, E. Sagen, and H. Loehner, “Apply Radios to Improve the Operation of Electrical Protection,” proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

10. D. Dolezilek, B. MacDonald, J. Kraft, and P. Dolezilek, “In the News: Recent Security Failures Prompt Review of Secure Computing Practices,” proceedings of the Protection, Automation and Control World Conference, Dublin, Ireland, June 2011.

11. M. E. Rourke, “Innovative Methods for Integrating Utility and Production Automation Systems,” *Proceedings of the 2010 Association for Iron & Steel Technology Conference*, Vol. 2, Pittsburgh, PA, May 2010.

12. D. Dolezilek, F. Chumbiauca, and M. Rourke, “Application of Ethernet Fieldbus to Substation RTU and Automation Networks,” proceedings of the 13th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2011.