The Demands and Implications of IT and OT Collaboration

Mohamed Moussamir and David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
PAC World Africa Conference
Cape Town, South Africa
July 30–August 2, 2013

Originally presented at the
Power and Energy Automation Conference, March 2013

The Demands and Implications of IT and OT Collaboration

Mohamed Moussamir and David Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

Abstract—**Traditionally, companies have developed, implemented, and supported operational technology (OT) separately from information technology (IT). However, as OT continues to evolve, its underlying platforms, software, security, and communications are becoming increasingly similar to those of IT. Also, the data within OT devices are a rich source of nontraditional decision-making information for IT processes. As a result, there are clear and growing benefits for an IT and OT collaboration.**

The separation was mainly imposed by how IT and OT defined their business strategies and capabilities and how both worlds govern their organizations. Clear governance, decision-making authority, and strategic direction dictate that the investments in each one produce value for the business and shareholders. Achieving clear smart grid governance requires access to the impacts of processes and standards for both IT and OT. A smart grid network management system enables clear governance by providing an understanding of the smart grid network health, as well as impacts to the business and customers.

IT is the common term for the entire spectrum of information processing, including software, hardware, communications technologies, and related services. OT is a general term that refers to several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems, and other control system configurations, such as programmable logic controllers (PLCs), often found in the industrial sector and critical infrastructure.

In general, IT does not include embedded technologies that do not generate traditional data for enterprise use. The purpose of IT is to capture, retain, manage, and present business information. Previous terms used for IT were management information system (MIS) and business information system (BIS).

OT refers to communications network projects undertaken by groups outside of the IT department and encompasses the use of technology associated with the management and operation of physical assets. OT systems are typically used for the protection, control, and monitoring (PCM) of industries such as electrical, water and wastewater, oil and natural gas, chemical, and transportation. OT has the machine world at one or both ends of the input and/or output spectrum. In other words, OT is fundamentally about information and control technology (ICT) networks of embedded computers interacting with machines. IT has the human world at both edges. IT is about computers interacting with people.

This paper focuses primarily on describing the OT world for those familiar with IT and presents the major OT requirements, security concerns, and the ramification of an impaired OT system compared with an IT system. OT operations and engineering management recognize that it is very crucial to not only define the OT business model environment for a potential IT and OT collaboration but also make sure IT management understands the challenges for this collaboration in order to define the right strategies and employ the right capabilities.

I. Introduction

Business system experts have collaborated over the last two decades to create a set of services to support the software and communications needs of businesses, generically referred to as information technology (IT). The Information Technology Infrastructure Library (ITIL®) is a set of practices for IT service management (ITSM) that describes procedures, tasks, and checklists that are not specific to an organization, but are used by an organization for establishing a minimum level of competency.

In electric power systems, operational technology (OT) networks are specialized networks that include intelligent electronic devices (IEDs) that perform protection, control, and monitoring (PCM) applications.

Ethernet has emerged as a popular message transport method across many industries, including those considered mission critical, such as electric power, water and wastewater, data centers, and many others. In some instances, protection, control, automation, monitoring, and communications experts at electric utilities and product manufacturers have collaborated over the last two decades to create a set of services to support the information and control technology (ICT) needs of OT systems. The electric power industry continues to participate in standards organizations to create OT practices for successful ICT in electric power systems. Mission-critical OT operations, especially those required to prevent potential loss of life, often require true deterministic delivery of every message, every time, on time.

To date, Ethernet in OT networks has been most widely used for communications with relaxed class of service requirements, such as supervisory control and data acquisition (SCADA) and configuration access. These data exchanges are similar to IT tasks within OT networks. Meanwhile, the mission-critical protection-class OT messages, which have traditionally been transported over direct serial links, are now being delivered over Ethernet. These messages are published after a fault or event malfunction and used in high-speed automation, interlocking, or teleprotection functions. Protection-class digital messaging requires more deterministic message delivery than IT does and must meet internationally standardized requirements for message delivery, dependability, and security. OT PCM devices apply IEEE 802.1p and Q parameters to published messages to improve the ability of the network to provide OT behavior.

In order to transport protection-class messages over Ethernet, IT and OT network engineers must collaborate with protection experts to design the communications to meet OT requirements based on IEC 60834-1, which specifies performance and testing requirements for the teleprotection equipment of power systems. After the successful collaboration of business experts to create IT best practices and process experts to create OT best practices, we recognize the need for these two groups to collaborate. Important technical designs are required to move OT information into IT networks to improve business decisions without adversely affecting OT system performance.

II. Operational Technology

Previously, OT had little resemblance to IT systems in that OT consisted of isolated systems running proprietary control protocols using specialized hardware and software with predominantly Electronic Industries Alliance (EIA) serial connections. OT systems include IEDs with computer processing and digital memory and communications, essentially embedded rugged computers without monitors, mice, or keyboards, with both EIA serial and Ethernet connections. These PCM OT networks automatically control the power system apparatus that generate, transmit, distribute, and consume energy. They also allow users to operate the apparatus manually. IEDs in these networks generate, transmit, distribute, and consume information associated with control and operations processes [1]. Perhaps most important to understand is that OT Ethernet relies on multicasting of messages, or Ethernet packets, for mission-critical protection functions. These OT messages require specific IEEE Ethernet frame components, such as Ethertype and quality tags, which are different than those in any other industry. IEEE assigned unique Ethertypes to IEC 61850 Generic Object-Oriented Substation Event (GOOSE) and Sampled Value (SV) messages for use in power system OT, specifically because GOOSE and SV performance must be more precise than IT methods.

PCM OT networks are local or wide area. Local substation networks support the substation and possibly nearby distribution circuits; wide-area networks (WANs) connect several substations. Fig. 1 shows several local OT networks communicating information over wide-area OT networks. OT networks are the traditional way of transporting this information, which includes teleprotection signals, synchrophasors, and SCADA data [2] [3]. Wide-area OT methods, such as time-division multiplexing (TDM), provide the determinism and high availability needed for mission-critical electric power system applications.

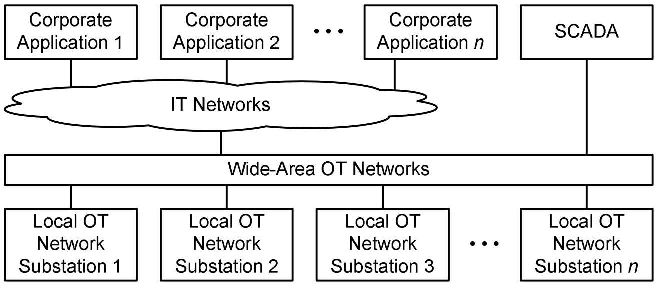
Corporate Application 1
Corporate Application 2
• • •
Corporate Application *n*
SCADA
IT Networks
Wide-Area OT Networks
Local OT Network Substation 1
Local OT Network Substation 2
Local OT Network Substation 3
• • •
Local OT Network Substation *n*

Fig. 1. Application example of OT and IT networks in an electric power system.

The management of the intricate balance of electric power supply and demand, protection of the delivery apparatus, and preservation of the safety of the public requires the constant, vigilant, sophisticated, and reliable exchange of information among parts of the grid. The additions of distributed and renewable generation, microgrids, two-way power flows, automatic network reconfiguration, and changes in load profiles have required advances in protection and control systems as well [4]. By and large, these advances in real-time information exchange and automatic control within the grid go unnoticed by all but a select few who are aware of high-speed automation, digital teleprotection, and interlocking. High-speed communications among devices performing PCM are largely invisible to the general public—especially if the lights stay on—and even to the utility staff responsible for asynchronous SCADA, energy management, and automation. Unaware that protection-class communications are working in the background of the grid, IT experts often make statements like: "The way we generate and distribute electricity today is essentially the same as when Thomas Edison built the first power plant well over 100 years ago. All we have to do is collect and move the associated information into the enterprise." In fact, tens of thousands of PCM IEDs are sharing information using ICT and making millions of decisions every millisecond of every day to control the health and performance of the grid. Although the underlying principles of generating electricity have not changed, the generators, loads, and digital control systems have changed dramatically. It is the responsibility of all the members of the power industry to maintain and improve service to the public, remain informed of new technologies, and prevent uninformed decisions about grid communications from jeopardizing the delivery of safe, reliable, and economical electric power. Modern PCM digital control systems rely on rapid and deterministic transport of commands via digital messages to avoid potential loss of life, equipment damage, and blackouts by mitigating power system malfunctions and preventing them from creating a man-made technical disaster.

III. Information Technology

IT refers to the devices and methods used to transport information between people and processes. IT networks move information from the source to a remote person, process, or network. In Fig. 1, IT networks collect information from OT networks and distribute this decision-making information for corporate applications, such as planning, asset management, and billing. IT networks are shown as a cloud because their structure and behavior are variable, adaptable, and nondeterministic. These characteristics are acceptable for IT convenience and flexibility because the information is for less time-critical business processes.

The electric power industry has begun using specialized applications of generic IT devices (such as Ethernet switches and routers) and methods (such as Internet Protocol [IP] communication) to move data within PCM OT networks. These devices and methods are adaptable and flexible. However, their variability and nondeterminism, while acceptable in business applications, are detrimental to mission-critical OT applications. Although the power industry has created specialized Ethernet methods for a few critical applications, these methods are unique to PCM OT networks and are difficult to use within IT devices. Therefore, most IT devices and methods in power systems are relegated to nonmission-critical data flow, such as engineering access and data archiving.

IV. IT Impact on the Power Industry Infrastructure

Due to this recent IT influence, widely available, low-cost IP devices are now replacing proprietary solutions. This increases both interconnection flexibility and the possibility of cybersecurity vulnerabilities and incidents. As OT networks change to include IT solutions to promote corporate connectivity and remote access capabilities and are being designed and implemented using industry standard computers, operating systems, and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for OT from the outside world than previous systems did, creating a greater need to secure these systems. Perhaps more important is that the underlying performance requirements of mission-critical OT systems are not recognized or satisfied by IT governance.

The National Institute of Standards and Technology (NIST) special publication *NIST Framework and Roadmap for Smart Grid Interoperability Standards* includes IEC 61850 protocols for protection-class communications [5]. The IEC 61850 protocols GOOSE and SV are Ethernet messages used for peer-to-peer data exchange for protection, automation, interlocking, and teleprotection. SV messages are published at a fixed frequency, often 4,800 messages per second. GOOSE messages are published by IEDs constantly at a configured time between messages. GOOSE messages are also published in a burst mode after a change is detected in the power system. The first message of this burst mode must travel through the network without delay to accomplish mission-critical protection. Guaranteeing undelayed first response of these Ethernet messages requires a revisit to the first principles of network design.

Delayed, dropped, or overcommunicated messages are unavoidable consequences of using Ethernet technology and are considered acceptable, even expected, for IP applications. Essentially, this behavior has become the new normal because communications designers accept occasional failed message delivery. These delays are not analyzed as true failures and actual catastrophic near misses. The unintended consequence of the new normal nondeterministic Ethernet is that it is only a matter of time before such a failure occurs, delaying a message burst that is reacting to a change of state in the power system and attempting to perform a protection function.

Near misses are misunderstood, ignored, or, worse, tolerated and accepted because they do not appear to cause immediate harm. The sole purpose of these communications is to move information instantly after a power system event, and the communications network needs to be designed for that purpose. PCM engineers are obligated to educate end users, consultants, designers, manufacturers, integrators, technicians, and maintenance staff about the expected behavior of communications within protection-class applications. It is imperative to do so because degraded behavior is essentially invisible within the network and others may not grasp the significance of delayed messages. Even when deviations are noticed, network designers, consultants, and integrators often obscure the effect of the symptom, such as by promoting asynchronous instead of synchronous client/server applications, rather than find root cause.

Present smart grid designs and proposals that focus on smart metering and other smart grid accessory applications use bandwidth-sharing IP protocols and IT methods. Some activities also promote greater use of IT technologies in PCM OT networks. However, the industrial OT networks that successfully use bandwidth-sharing IP protocols and IT methods do not have the same performance requirements as power industry networks. Other industries do not share the need of the power industry for real-time PCM applications and mission-critical communication. PCM OT networks must be designed to perform both nonessential smart grid data acquisition, such as metering, as well as essential smart grid actions, the activities that automate the generation, delivery, and consumption of electric energy.

The power industry in all its forms has been going through many changes compared with the way the industry used to function a couple of decades ago. This change was triggered by the pressure to drive maximum operational efficiency, increase reliability, and, at the same time, reduce cost. The management at utilities is under constant pressure to adopt new strategies to accommodate the new business environment. These strategies include difficult decisions related to determining which proprietary assets be kept inside the walls of the organization and which will be leveraged on the outside. Once strategic positioning and direction have been defined and strategic goals have been set, the next step is to assemble the resources and build the capabilities required to achieve those goals. OT and IT collaboration must be looked at as a new business. Building a successful OT and IT business in these challenging times requires that executives understand how to define and execute strategy, develop and leverage capabilities, and create value for all stakeholders. When strategy, capability, and value are aligned with the goals of an organization and with the external environment, the business model creates what economists call a virtuous cycle of innovation, productivity, and increasing return.

V. The Need for IT and OT Collaboration

In order to understand the best method for collaboration between OT and IT, the differences between IT and OT must be defined and managed. Traditional IT systems are seen differently from OT systems. IT refers to areas like supply chain, asset management, mobile workforce management, human resources, accounting, and finance. The main purpose of OT resides in physical and critical asset SCADA, process control, metering and protection, device-to-device communication for teleprotection and automation, server-to-device communication for monitoring, data archiving, and commanded or automatic control. The OT operating environment exists in substations, field equipment, and control centers, manipulating data coming from transducers and sensors via remote terminal units (RTUs) and programmable logic controllers (PLCs). Data are also collected from IEDs, relays, and meters. These data reflect the status, health, and performance of the underlying primary power system. Data being sent out into the field (output data) result in device and control actions, human-machine interface (HMI) updates for displaying statuses and alarms, and operating logs. From an ownership standpoint, OT owners are the operations and engineering managers, line-of-business managers, and maintenance and engineering services departments. Mission-critical requirements have driven OT solutions to use different ICT acceptance criteria and therefore different networks. Therefore, the most important differentiator that greatly sets OT apart from IT is connectivity for device-to-device communication and client/server communication.

OT is very important for managing, monitoring, and reporting on the health and performance of the network of machines and devices that it is operating. However, more often than not, new operations networks are being designed from an IT perspective and the use of OT acceptance criteria is limited to engineering operations management and the control room of the utility. SCADA is the primary OT used to monitor the health of an electric power network under a given situation because it is most similar to an IT network monitoring system (NMS) of operator supervision. However, the true power of modern OT systems is that the IEDs perform the role of human operators to constantly observe, decide, and act. OT device-to-device communications allow the IEDs to accelerate automation actions by rapidly sharing decision-making information among themselves. This capability, which includes telecontrol and teleprotection, provides the largest benefit over traditional IT methods and is unfortunately the least understood by IT professionals. *Tele*, from the Greek *telos*, refers to accomplishing goal-oriented processes over long distances from a remote location. To do this, IEDs in mission-critical communications act on the data to perform the goal objective. IT networks exist to move information about the results and effectiveness of the OT processes. Perhaps the most important technical hurdle for collaboration is the lack of visibility of the existence, importance, and performance requirements of OT multicasting for teleprotection and telecontrol among IT professionals.

VI. Proposed Method for IT and OT Collaboration

The most important element of collaboration is recognizing that it is necessary. Over time, IT and OT teams have developed very different strategies, predominantly because they have a need to accomplish very different things. This paper addresses the subset of IT functions that require the acquisition and processing of data from OT networks. For an IT engineer, the solution seems simple—extend the IT network to connect to the OT data source. However, this adversely affects the other communications functions required of that OT data source. IT and OT engineers must meet and discuss the requirements of the OT and IT applications and how to work together to support them.

The second most important element is that OT engineers are not being asked to be OT engineers in an IT environment, but rather to design OT networks based, in part, on Ethernet. They need to understand and embrace the performance requirements of OT and the term *OT engineering*. Over the years, all of the utility business information systems have converged onto the IT network. Therefore, regardless of the business application, IT networks are designed by IT engineers to satisfy themselves. Today, many utilities name groups *substation engineering*, *protection and control*, *substation automation*, and other terms. Therefore, regardless of the substation application, OT networks are designed by OT engineers to satisfy themselves.

The third most important element is for end users to work to remove the silos that different groups have built around themselves. When no data are passed outside of the substation except command and control to a remote SCADA computer, IT and OT can remain separate. The advancement of ICT and the availability of business decision-making information in the substation mean that those silos must come down. Utilities can no longer afford to have IT communications and OT automation groups isolated from one another. The digital communications links between their equipment requires that they understand one another and how to satisfy applications at each end of the cable.

As [6] and [7] illustrate, the successful merger of protection, control, and monitoring into one network of IEDs requires collaboration among operators and protection, communications, and automation engineers; now they are OT engineers. Challenges must be expected when a new design is developed. The OT challenges are not always technical; some are procedural. For instance, how do test technicians selectively block signals communicating over Ethernet? To address these and other important issues, one utility created a project team consisting of representatives from engineering, operations, standards, and electrical testing. Issues were discussed at length, and the system was designed to accommodate concerns associated with testing, scaling and expanding, and maintaining the design [6]. Over time, they also identified a new engineer, the OT network communications engineer.

The collaboration process starts by building the right team and putting together a group of employees with the right skills, chemistry, and motivations. They must agree to work together to create a joint solution and communicate effectively as a team without silos to identify the following:

- A project plan
- Key dates
- Network communications requirements
- Clear acceptance criteria
- Team member skills and experience

- Team member responsibilities and deliverables
- Potential road blocks
- A budget

VII. IT and OT Have Very Different Information Flow Standards

Direct purpose-built digital protocols, including Mirrored Bits® communications, the IEC 61850 communications standard, Ethernet switching, multicast Ethernet packets, and IP communications, are among the most widely accepted standards and technologies today for providing the underlying framework for a strategic integrated substation network in an OT system. They have evolved to address the needs and requirements of the substation environment in a way that will support long-term growth and performance needs in an organized and cost-effective manner. Today more than ever, IEC 61850 and other initiatives identify IP and multicast Ethernet as the basic networking technologies upon which to build multipurpose integrated substation network architecture and facilitate data exchange with other groups or organizations. Therefore, an OT and IT collaboration is important. Collaboration must carefully support performing OT communications among IEDs, as well as transporting IT traffic to the OT perimeter for secure and dependable delivery to the IT network. In this way, the two systems share information through a well-designed, safe, and secure intersection where the perimeters intersect rather than sharing the same resources.

VIII. IT and OT Have Very Different Acceptance Criteria

The aim of this new communications framework is to close the gap between OT and IT systems for strategic collaboration and sharing capabilities. However, data and network security through the lens of IT and OT are very different. Within the collaboration infrastructure, those differences are often blurred. IT security usually stops at the firewalls of the corporate local-area network (LAN) and focuses on IP, while a large part of OT security exists in the field and needs to satisfy unique characteristics, such as multicasting. Utilities have found that simply extending IT security to cover the OT needs for the smart grid is not sufficient or practical technologically or operationally. Meeting the security needs for IT and OT requires bridging this gap with a security framework that ties both together. As stated previously, the communications capabilities are already in place and shared between IT and OT in the form of IP and multicast Ethernet frameworks. Furthermore, a security device used as the demarcation point between IT and OT networks, such as an OT firewall and router, will help ensure end-to-end security between the smart grid systems and endpoints, while not compromising the underlying security requirements of each organization. OT-aware smart grid network management systems provide capabilities that secure network devices and data transmission between smart grid endpoints (sensors, relays, meters, and so on) and the utility data center.

While security solutions have been designed to deal with security issues in typical IT systems, special precautions must be taken when introducing these solutions to OT environments. In some cases, new security solutions are needed that are tailored to the OT environment.

OT networks have many characteristics that differ from traditional IT systems, including different risks and priorities. Some of these include instantaneous and significant risk to the health and safety of human lives, serious damage to the environment, and financial issues, such as production losses and negative impacts to the economy of a nation. OT systems have different performance and reliability requirements and use operating systems and applications that may be unfamiliar, such as multicasting of IEC 61850 GOOSE and SV protocols, or unconventional, such as User Datagram Protocol (UDP) multicasting of synchrophasor messages, to typical IT support personnel.

Furthermore, the goals of safety and efficiency can sometimes conflict with security in the design and operation of control systems. As an example, enabling Manufacturing Message Specification (MMS) services requiring password authentication and authorization should not hamper or interfere with emergency actions for OT. The following are some IT and OT acceptance criteria concerns for various network communications requirements:

- Performance requirements. While IT systems typically require high throughput and can withstand some level of delay and jitter, OT applications are generally time-critical, with the criterion for acceptable levels of delay and jitter dictated by the individual installation. Some systems require deterministic responses in less than 3 milliseconds 99.99 percent of the time, regardless of distance, with never more latency than 20 milliseconds.
- Message throughput. High throughput is typically not essential to OT. A more recent and useful OT metric common to other industries and newly recognized by electric power system OT engineers is *goodput* [3]. Goodput is the amount of useful data, user data, or payload that can be processed by, passed through, or otherwise put through a system and received at the correct destination address. It is actually application information throughput, a measure of the amount of information exchanged between devices participating in an application, as opposed to traditional communications message throughput. Goodput is a ratio of the delivered amount of information and the total delivery time minus any packet headers or other overhead and minus any information lost or corrupted in transit. In contrast, IT systems typically require high throughput, and they can typically withstand some level of delay and jitter.
- Message delivery speed. Each mission-critical OT machine-to-machine, peer-to-peer multicast message defined as IEC 61850 Protection Class 2 or 3 needs to be delivered in less than 3 milliseconds, regardless of

quantity, frequency, or network configuration [4]. No similar requirement or measurement exists for IT systems.

- Message delivery latency. Permissible latency referenced by the IEC 60834-1 standard, which describes performance requirements for teleprotection systems within the smart grid, includes 20-millisecond maximum latency for the permissive tripping teleprotection function and 30-millisecond maximum latency for direct tripping. No similar requirement or measurement exists for IT systems.
- Message delivery dependability. Dependability defined by IEC 60834-1 indicates the acceptable number of unwanted messages because they may cause unwanted operations. For a GOOSE exchange between devices every second to support the intertripping teleprotection function, the requirement is that each IED receive less than nine unwanted messages in a 24-hour period. No similar requirement or measurement exists for IT systems. In fact, IT systems routinely buffer and resend packets, which improves IT dependability but reduces OT dependability.
- Message delivery security. Security defined by IEC 60834-1 indicates the acceptable number of dropped messages because they may prohibit communications-assisted operations. For a GOOSE exchange between devices every second to support intertripping, the requirement is that less than one (essentially zero) message be undelivered or delivered late to each IED. No similar requirement or measurement exists for IT systems. In fact, IT systems routinely drop or delay individual packets, which improves IT security but reduces OT security.
- Availability requirements. Many OT processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Outages often must be planned and scheduled days or weeks in advance. Exhaustive predeployment testing is essential to ensure high availability for OT. Also, many control systems cannot be easily stopped and started without affecting production. In some cases, the products being produced or equipment being used is more important than the information being relayed. Therefore, typical IT strategies, such as rebooting a component, are usually not acceptable solutions due to the adverse impact on the OT requirements of high availability, reliability, and maintainability. Some OT employs redundant components, often running in parallel, to provide continuity when primary components are unavailable.

  As mentioned previously, each mission-critical OT function requiring machine-to-machine, peer-to-peer messaging defined as permissive tripping or direct tripping must operate end to end in less than 20 and 30 milliseconds, respectively [4]. Other more stringent functions require even faster operation. Therefore, network outages must be resolved in a matter of a few milliseconds in order to support these operations should they occur simultaneously. No similar requirement or measurement exists for IT systems.
- Risk management requirements. In a typical IT system, data confidentiality and integrity are the primary concerns. For an OT system, the primary concerns are human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or lost or damaged products. The personnel responsible for operating, securing, and maintaining OT must understand the important link between safety and security.
- Architecture security focus. In a typical IT system, the primary focus of security is to protect both the operation of IT assets, whether centralized or distributed, and the information stored on or transmitted among these assets. In some architectures, information stored and processed centrally is more critical and is afforded more protection. For OT, edge devices (e.g., protective relays, PLCs, operator stations, and distributed control system controllers) need to be carefully protected because they are directly responsible for controlling the end processes. The protection of the central server is still very important in an OT system because the central server could possibly adversely impact every edge device. An IT edge device has been considered a physical device that can pass packets into enterprise or service provider core networks. These are routers, switches, and multiplexers that use the routing information within the network layer addressing to route messages. When positioned at the intersection of OT and IT networks, these devices act as intersection devices. An edge router is an example of an edge device that can act as a perimeter intersection device.
- Physical interaction. In a typical IT system, there is no physical interaction with the environment. OT can have very complex interactions with physical processes and consequences in the OT domain that can manifest in physical events. All security functions integrated into OT must be tested (offline on comparable OT) to prove that they do not compromise normal OT functionality. The required environmental ruggedness and reliability of communications networking devices installed in OT networks are dictated by standards such as IEEE 1613. This and other standards set stringent temperature, electric shock and noise, and vibration survivability standards that the devices must meet. These standards are dramatically more severe than those that IT devices must satisfy.

- Time-critical responses. In a typical IT system, access control can be implemented without significant regard for data flow. For some OT, automated response time or system response to human interaction is very critical. For example, requiring password authentication and authorization on an HMI must not hamper or interfere with emergency actions for OT. Information flow must not be interrupted or compromised. Access to these systems should be restricted by rigorous physical security controls. As mentioned previously, each mission-critical OT commanded control function must be delivered in a timely manner. IEC 60834-1 identifies the OT requirement that 99.99 percent of all command messages must be delivered in less than 10 milliseconds [4]. No similar requirement or measurement exists for IT systems.
- System operation. OT operating systems and applications may not tolerate typical IT security practices. Legacy systems are especially vulnerable to resource unavailability and timing disruptions. Control networks are often more complex and require a different level of expertise (e.g., control networks are typically managed by control engineers, not IT personnel). Software and hardware are more difficult to upgrade in an operational control system network. Many IT systems may not have desired features, including encryption capabilities, error logging, and password protection.
- Resource constraints. OT and its real-time operating systems are often resource-constrained systems that usually do not include typical IT security capabilities. There may not be computing resources available for OT components to retrofit these systems with updated security capabilities. Additionally, in some instances, third-party security solutions are not allowed due to OT manufacturer license and service agreements, and loss of service support can occur if third-party applications are installed without manufacturer acknowledgement or approval.
- Communications. Communications protocols and mediums used by OT environments for field device control and intraprocessor communication are typically different from those in the generic IT environment and may be proprietary.
- Change management. Change management is paramount to maintaining the integrity of both IT and OT systems. Unpatched software represents one of the greatest vulnerabilities in a system. Software updates on IT systems, including security patches, are typically applied in a timely fashion based on appropriate security policies and procedures. In addition, these procedures are often automated using server-based tools because their potentially negative impact on network and device availability is considered acceptable. Software updates on OT cannot always be implemented on a timely basis because these updates need to be thoroughly tested by the manufacturer of the industrial control application and the end user of the application before being implemented. OT outages often must be planned and scheduled days or weeks in advance. The OT system may also require revalidation as part of the update process. Another issue is that many OT systems use older versions of operating systems that are no longer supported by the manufacturer. Consequently, available patches may not be applicable. Change management is also applicable to hardware and firmware. The change management process, when applied to OT, requires careful assessment by OT experts (control engineers) working in conjunction with security and IT personnel.
- Managed support. Typical IT systems allow for diversified support styles, perhaps supporting disparate but interconnected technology architectures. For OT, service support is usually via a single manufacturer, which may not have a diversified and interoperable support solution from another manufacturer. Further, service contracts for constant and automatic patch management are popular for IT devices but not present in the OT environment. OT devices are deployed without annual service contracts, so adding IT technology with service contracts is unfamiliar and unwelcome to OT operations staff.
- Component lifetime. Typical IT components have a lifetime on the order of 3 to 5 years, with the brevity due to the quick evolution of technology. For OT, where technology has been developed, in many cases, for very specific use and implementation, the lifetime of the deployed technology is often in the order of 15 to 20 years and sometimes longer.
- Component access. Typical IT components are usually local and easy to access, while OT components can be isolated and remote and require complicated physical effort to gain access to them. OT devices are often embedded within the OT process environment, so access may require that the processes be stopped or that appropriate OT personnel make arrangements well in advance and observe stringent safety precautions.

IX. IT AND OT MUST INTERSECT BUT NOT OVERLAP

The single largest communications technology challenge facing the power system industry today is the inappropriate use of IT methods in OT networks. Therefore, OT and IT networks must be built and managed separately and a careful intersection be designed to move information between the two.

Ethernet is essentially synonymous with IT in many industries and is chosen without regard for support of the underlying applications and, in some cases, contrary to the needs of those applications. This is further complicated by the fact that the power industry, like others, has migrated toward the use of a single Ethernet connection on computers and IEDs to support numerous simultaneous IT and OT conversations.

PCM IT began when ICT moved into the grid as electromechanical devices (which are based on the physics of electromagnetism causing metal platters to spin) were replaced with smart devices with onboard computing for conversion of analog signals to digital measurements, memory, and communications. Since 1984, digital communications with PCM IEDs have allowed people or programs to act as clients of data being served from the IED. People began sending and extracting settings and retrieving disturbance records (similar to oscilloscope captures stored during a power system event) and reports that gave a calculated distance to the fault and information about the health and behavior of power system apparatus. Soon after, PCM IEDs were enhanced to support operator client/server OT communications, via an operator console, to exchange information with PCM IEDs to perform remote control.

These OT client/server applications were designed to survive the asynchronous nature of historically poor characteristics of client/server request-and-response data acquisition, including the following:

- Variable message response and delivery latency and asynchronous server data due to the lack of time synchronization of the IEDs.
- Occasional loss or corruption of messages.
- Incoherent data due to the lack of orderly continuity, organization, and perhaps relevance—information simultaneously presented to the client is actually created and collected from the servers at very different times. A Boolean change of state updates more quickly than analog voltage and current measurements.
- Incoherent wide-area data due to locations responding at different times—locations update in a round-robin poll-and-response scheme, so some data are recent while others are at least as old as the time duration of the polling sequence, which is often several minutes.

Operators today still experience infrequent and unsynchronized updates from field devices. Users have been trained to overlook incoherent information that results from asymmetric acquisition of analog versus digital data and from near and far source locations. During this continual asynchronous data acquisition, the control system is constantly attempting to represent the present state of the power system. However, this representation is never the actual state of the power system, but rather it is the most recent update of each element, and data are often mismatched and reflect measurements from different points in time.

In the past, IT applications benefited from sharing the deterministic communications previously installed for OT applications and perhaps enjoyed a higher quality of service than absolutely necessary.

Because convenient Ethernet IT satisfies legacy client/server OT requirements, it is often used without consideration of improved client/server performance or wide-area, peer-to-peer applications. Once in place, poorly designed Ethernet and IP ICT systems prohibit innovation, such as synchronous SCADA and stability controls, including real-time synchrophasors and wide-area IEC 61850 GOOSE.

X. IT and OT Intersection Examples

In this section, we consider various designs of OT and IT intersection within a typical substation, while providing guidance for defining points of interest from the OT point of view. The most successful method for securing an OT and IT collaboration is to gather industry-recommended practices and engage in a proactive, collaborative effort between management, control engineers and operators, the IT organization, and trusted automation and technical professional advisors.

This section covers details specific to OT. However, it can also be helpful for system administrators, engineers, and other IT professionals who administer, patch, or secure OT systems.

Fig. 2, Fig. 3, and Fig. 4 depict, at a high level, the network connections and components typically found in control houses. Protocol converters are used to accept and forward commanded controls from a remote SCADA center, as well as acquire, store, and report substation data to remote users. They often act as a gateway to convert data from one group of message protocols inside the substation to another for outside the substation. HMIs act as the operator interface in the substation, with visualization on a monitor and local operator control available via a keyboard and mouse. The type and quantity of PCM IEDs largely depend on the type of substation and the applications that the utility chooses to perform. In between the controllers and the IEDs are the LAN Ethernet switches or information processors. Between the controllers and remote users are the WAN communications devices. Cybersecurity must be present within every device, but a physically separate firewall and password manager must exist between the WAN and LAN and again between the WAN and remote control center. In this way, the connection between the substation and control center becomes a virtual private network (VPN). When necessary, this same VPN technology is used between the parts of the LAN. Aside from the SCADA server and HMI, an OT system consists of both hardware and software. Hardware includes communications equipment (radio, telephone line, cable, or satellite), engineering workstations, synchrophasor processors, real-time automation devices, switches, Ethernet-to-serial gateways, clocks, RTUs, PLCs, and IEDs that control various devices, such as actuators and/or sensors. These physical devices are installed in control houses and cabinets in the substation.

Fig. 2 illustrates an OT substation LAN with local and remote IEDs connected via direct serial links.

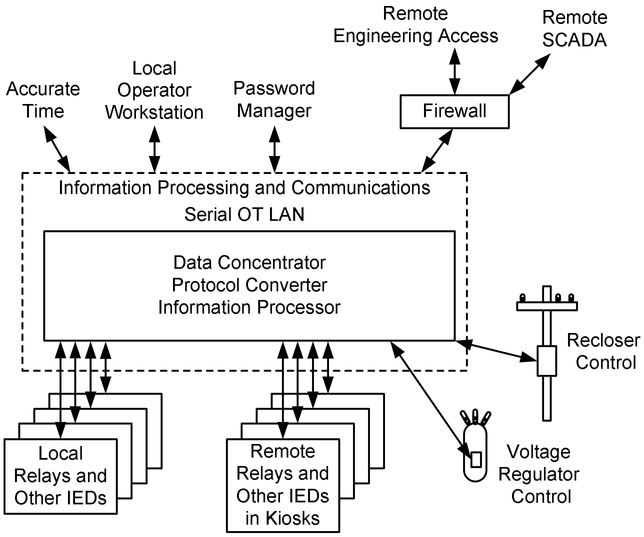
Remote Engineering Access
Remote SCADA
Accurate Time
Local Operator Workstation
Password Manager
Firewall
Information Processing and Communications
Serial OT LAN
Data Concentrator
Protocol Converter
Information Processor
Recloser Control
Voltage Regulator Control
Local Relays and Other IEDs
Remote Relays and Other IEDs in Kiosks

Fig. 2. Serial OT LAN with direct connections and nonroutable protocols.

Fig. 3 illustrates an OT substation LAN with local and remote IEDs connected via indirect Ethernet links. The remote connections may support both routed and multicast protocols or be restricted to multicast protocols exclusively to meet cybersecurity requirements.

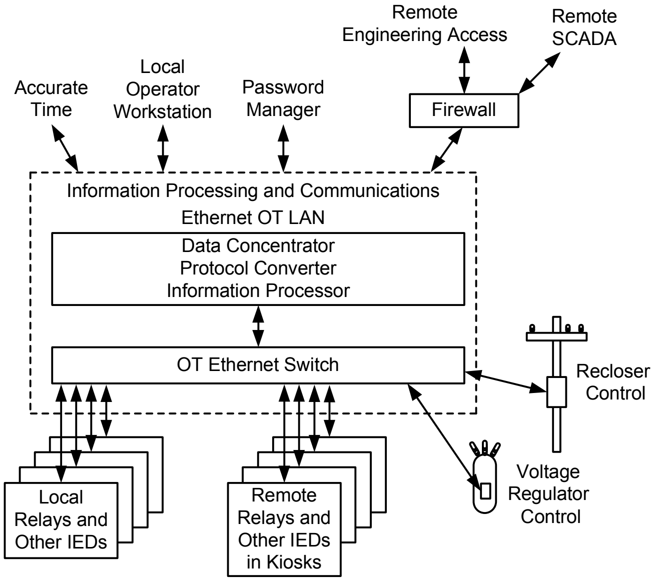
Remote Engineering Access
Remote SCADA
Accurate Time
Local Operator Workstation
Password Manager
Firewall
Information Processing and Communications
Ethernet OT LAN
Data Concentrator
Protocol Converter
Information Processor
OT Ethernet Switch
Recloser Control
Voltage Regulator Control
Local Relays and Other IEDs
Remote Relays and Other IEDs in Kiosks

Fig. 3. Ethernet OT LAN with indirect connections and routable and multicast protocols.

Fig. 4 illustrates an OT substation LAN with local and remote IEDs connected via indirect Ethernet links, with additional cybersecurity provided by intrastation VPNs.

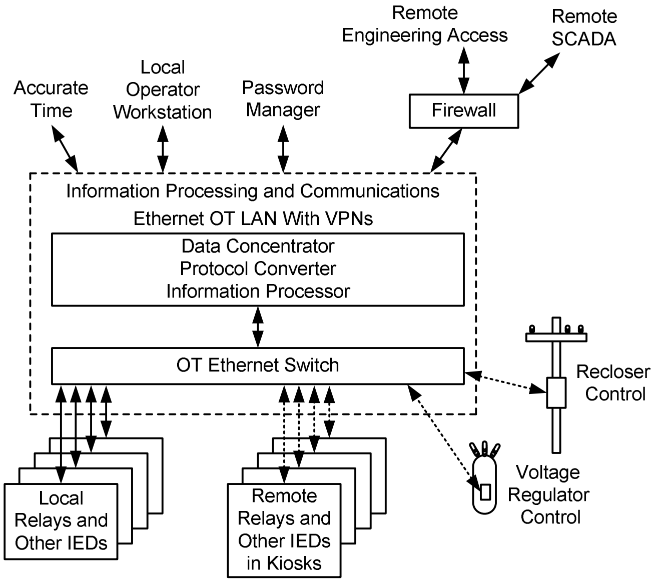
Remote Engineering Access
Remote SCADA
Accurate Time
Local Operator Workstation
Password Manager
Firewall
Information Processing and Communications
Ethernet OT LAN With VPNs
Data Concentrator
Protocol Converter
Information Processor
OT Ethernet Switch
Recloser Control
Voltage Regulator Control
Local Relays and Other IEDs
Remote Relays and Other IEDs in Kiosks

Fig. 4. Ethernet OT LAN with indirect connections and routable and multicast protocols plus VPN connections to remote IEDs.

Fig. 5 illustrates a completely vertical OT system from sensors to SCADA. Communications performance is designed to serve the OT applications, but the OT information is only available to business IT applications via the SCADA database. This substation LAN is based on dedicated serial connections and information processors that manage most of the network communications.

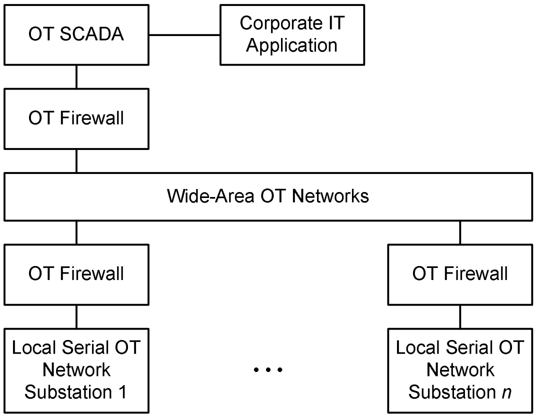

Fig. 5. Completely vertical OT networks for protection through SCADA.

Fig. 6 illustrates a completely vertical IT system from sensors to SCADA. Communications performance is nondeterministic and variable, which jeopardizes the ability of PCM systems to perform closed-loop control and rapid automation to protect personnel and equipment.

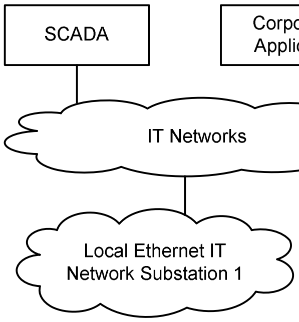
SCADA
Corporate IT Applications
IT Networks
Local Ethernet IT Network Substation 1

Fig. 6. Data acquisition based on nondeterministic IT methods.

Fig. 7 illustrates a local serial OT substation with an IT connection to SCADA. An evaluation of the issues presented in this paper demonstrates that it is not a best practice to interface between the OT LAN and IT WAN inside the substation because of poor message delivery performance and increased cost and unwieldy frequent maintenance associated with IT device service contracts.

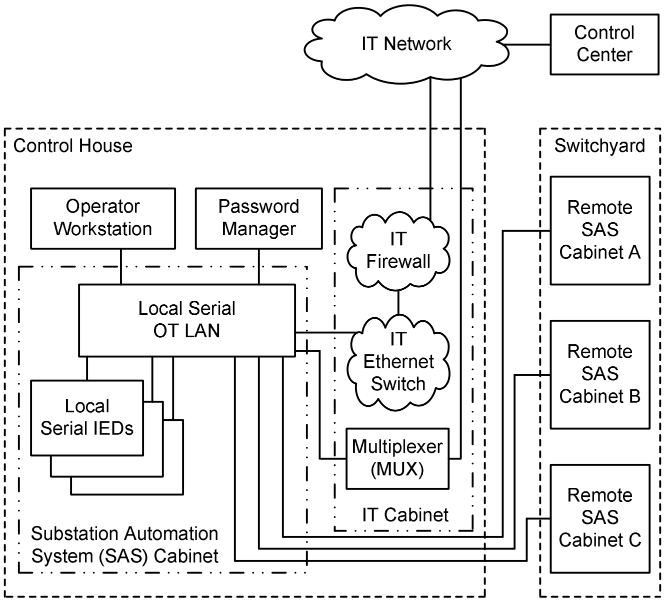

Fig. 7. OT serial LAN with IT WAN interface inside the substation.

Fig. 8 illustrates a local Ethernet OT LAN substation with an IT connection to SCADA. An evaluation of the issues presented in this paper demonstrates that it is not a best practice to interface between the OT LAN and the IT WAN inside the substation. Doing this prevents OT performance for delivering data from the substation to the control center and between substations. Inappropriate demarcation between IT and OT is often illustrated by physically duplicate WAN interfaces in the substation managed by separate groups operating in silos of responsibility and often without collaboration. Some asynchronous and nonmission-critical applications can be performed in this manner. However, mission-critical PCM applications cannot be performed. Therefore, the intended purpose and future capabilities of the substation system are restricted. These restrictions are preordained by inappropriate physical and professional separation of the process system experts and those responsible for the communications infrastructure. Clearly, this presents a problem because communications-assisted applications require careful management of the IEDs and the communications between them.

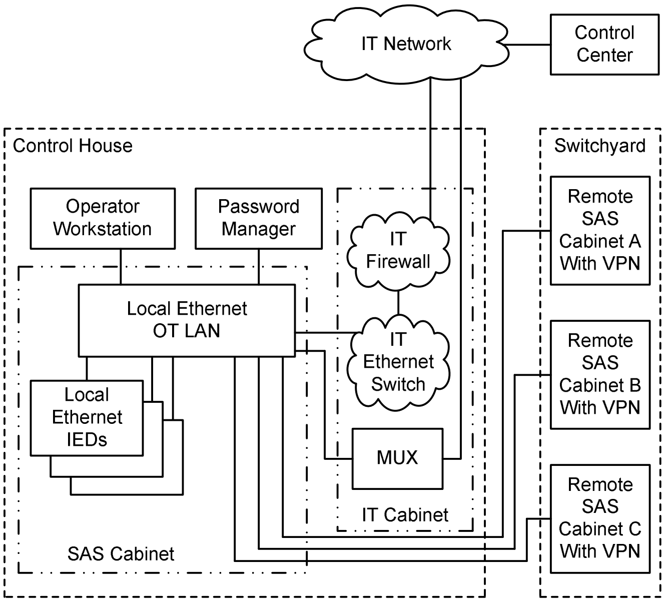

Fig. 8. OT Ethernet LAN with IT WAN interface inside the substation.

Fig. 9 illustrates a completely vertical IT system from sensors to SCADA. This preserves the performance of OT applications in the substation, between substations, and to SCADA. OT information is forwarded to IT applications via the OT firewall and router, acting as a demarcation point in the control center.

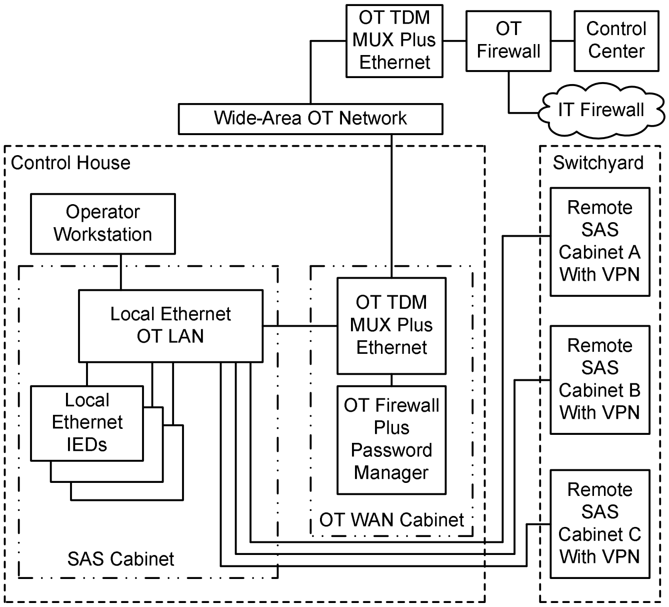

Fig. 9. Best practice OT substation LAN with OT WAN and IT interface at the control center.

This paper illustrates that the OT system is an isolated interconnected system where OT managers and engineers apply their own strategies and capabilities for a secure mission-critical environment. Further, appropriate collaboration between IT and OT personnel and products is done via a physical OT firewall and router, acting as a demarcation point best installed at the control center. Therefore, each control house should have its own communications cabinet for OT system Ethernet connections. However, substation OT and corporate IT systems are often incorrectly interconnected as a result of several changes in information management practices and operational and business needs. The demand for remote access has encouraged many organizations to establish connections to the OT system that enable OT and IT engineers and support personnel to monitor and control the system from points outside the control network. Many organizations have also added connections between corporate networks and OT networks to allow the decision makers of the organization to obtain access to mission-critical data about the status of their operational systems and to send instructions for the manufacture or distribution of product. Often, these connections were implemented without a full understanding of the corresponding security risks, which are out of the scope of this paper. In addition, IT networks are often connected to strategic partner networks and the Internet. OT systems also make more use of WANs and IP to transmit data to their remote or local stations and individual devices. Incorrect integration of OT and IT networks increases the vulnerabilities of OT systems due to the following:

- The majority of business unit managers believe their OT system is not connected to the IT or corporate network.
- The majority of OT systems are connected in some way to the IT system.
- The IT network is only secured to support general business processes and not mission-critical systems.

XI. Evaluating IT and OT Leadership and Governance

Success over time demands strong leadership. Effective leaders use governance structures and systems to balance the creativity and vision needed to set goals and prioritize investments with the discipline needed to execute and deliver results. Governance systems include strategic controls (scanning the environment, defining a strategic position, setting goals, and prioritizing projects and investments), operating controls (defining short-term objectives and controlling current business operations and projects), effective risk management (identification and management of key risks), and effective development and management of the shared values and culture that guide decisions and actions.

One of the consequences of IT and OT collaboration is the need to define a new strategy that will unify the strategies of the two departments. This collaboration brings many benefits, but it also brings many challenges. In the business context analysis, several questions have to be addressed to create and successfully execute the new strategies to be deployed. Sample questions for defining new strategies for IT and OT collaboration are the following:

- How favorable (or unfavorable) is the business context within which we operate today, and what changes do we anticipate?
- Are there disruptive changes on the horizon that would signal entry opportunities or threats to the two separate strategies? Can IT and OT management disrupt the industry and create new opportunities as a result of IT and OT collaboration?
- Which factors in the business environment help or hinder the achievement of IT and OT collaboration goals?
- What must be done well to succeed? What are the key failure factors?
- There are employees from both departments behind IT and OT collaboration. Did management communicate the range of opportunities that employees should pursue and, most importantly, which opportunities employees should not pursue?
- Are future opportunities identified as a result of an IT and OT collaboration?

XII. Conclusion

In summary, the operational and risk differences between OT and IT systems create the need for increased sophistication in applying cybersecurity and operational strategies. A cross-functional team of control engineers, control system operators, and IT security professionals needs to work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation. IT professionals working with OT operations and engineering management need to understand the reliability impacts of information security technologies before deployment. Some of the operating systems and applications running on OT systems may not operate correctly with commercial-off-the-shelf IT cybersecurity solutions because of specialized OT environment architectures. The following four immediate and important steps must be taken as collaboration between IT and OT continues to evolve:

- IT designers, analysts, and consultants must acquaint themselves with the underlying requirements of the OT applications and industry standards for behavior and performance, such as the IEC 61850 communications standard and IEC 60834-1.
- IT designers, analysts, and consultants must acquaint themselves with the unique requirements for message and packet delivery between devices to meet acceptable levels of availability, dependability, and reliability in mission-critical OT applications.

- IT and OT network designers, analysts, and consultants must recognize the importance of separate but compatible networks. Performance requirements dictate that OT networks remain separate and designed to support mission-critical and time-sensitive applications. OT data and information must flow to and from an IT network via a carefully designed perimeter intersection device. Though IT processes do exist in the OT network, the most stringent applications require OT performance and so IT and OT networks must remain separate and not merge.
- IT and OT network designers, analysts, and consultants must collaborate to benefit from the differing knowledge and experience for specific and unique ICT network acceptance criteria and best engineering practices.

XIII. References

[1] H. J. Altuve Ferrer and E. O. Schweitzer, III (eds.), *Modern Solutions for Protection, Control, and Monitoring of Electric Power Systems*. Schweitzer Engineering Laboratories, Inc., Pullman, WA, 2010.

[2] D. Dolezilek, "IEC 61850 GOOSE and IEEE C37.118 Synchrophasors Used for Wide-Area Monitoring and Control, SPS, RAS, and Load and Generation Management," proceedings of the CIGRE Monitoring of Power System Dynamics Performance, Saint Petersburg, Russia, April 2008.

[3] D. Dolezilek, N. Fischer, and R. Schloss, "Improvements in Synchronous Wide-Area Data Acquisition Design and Deployment for Telecontrol and Teleprotection," proceedings of the 14th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2012.

[4] D. Dolezilek, "Ethernet Design for Teleprotection and Automation Requires a Return to First Principles to Improve First Response," proceedings of the 14th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2012.

[5] NIST Special Publication 1108R2, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0*, February 2012. Available: http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf.

[6] H. Fischer, J. Gilbert, G. Morton, M. Boughman, and D. Dolezilek, "Case Study: Revised Engineering and Testing Practices Resulting From Migration to IEC 61850," proceedings of the DistribuTECH Conference and Exhibition, Tampa, FL, January 2008.

[7] D. D. Bekker, P. Diamandis, and T. Tibbals, "IEC 61850 – More Than Just GOOSE: A Case Study of Modernizing Substations in Namibia," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

XIV. Biographies

Mohamed Moussamir is an associate integration and automation engineer in the transmission group at Schweitzer Engineering Laboratories, Inc. (SEL) in Pullman, Washington. He has nine years of experience developing and testing products in research and development. For the past two years, he has been researching ways to validate system reliability, stability, behavior, and performance with all supported communications protocols, such as IEC 61850, synchrophasors, MIRRORED BITS® communications, DNP3 clients, File Transfer Protocol, Telnet, and SEL protocols. Mohamed is an MBA candidate at Eastern Washington University, with anticipated graduation in spring 2013. The focus of his research is the operational technology environment and security, including machine-to-machine exchange of messages among intelligent protection, control, and monitoring devices in the power system.

David Dolezilek received his BSEE from Montana State University and is a research and development technology director at Schweitzer Engineering Laboratories, Inc. He has experience in electric power protection, integration, automation, communication, control, SCADA, and EMS. He has authored numerous technical papers and continues to research innovative technology affecting the industry. David is a patented inventor and participates in numerous working groups and technical committees. He is a member of the IEEE, the IEEE Reliability Society, CIGRE working groups, and two International Electrotechnical Commission (IEC) technical committees tasked with the global standardization and security of communications networks and systems in substations.