IT and OT Convergence - Prepare for the Inevitable
by Jeff Pack, POWER Engineers, Inc.  jeff.pack@powereng.com

Introduction
The electric power industry has used automated systems for many years. The concept of a master station in a supervisory control and data acquisition (SCADA) system began in the 1920s when substations adjacent to power plants started to be monitored and controlled from the power plant’s control room. The industry has continued to add automation in all areas of power generation and delivery, with the terms Operational Technology (OT) and “Smart Grid” dominating recent discussion of automation.

Advanced intelligent electronic devices (IEDs) provide power operators, technicians, and engineers better information for decision making and offer more tools for controlling and monitoring power flow via remote control and automated functions. IEDs can detect and protect against various power fault and system disturbance scenarios along with providing power flow waveforms, metering data, and SCADA functionality.

On the information technology (IT) side, there has been a tremendous amount of automation and standardization. Perhaps the best example of standardization is the Internet and its associated communications protocols. Prior to the 1960s, computers were standalone devices that did not communicate among each other. With investment help from the U. S. Department of Defense, research companies developed the Advanced Research Projects Agency Network (ARPANET) and the associated protocols to enable packet-based communications. Through the 1970s and early 1980s the ARPANET started its evolution out of the research labs and into universities and commercial firms. In 1982, the TCP/IP protocols were finalized as the standard communication protocols for “connected internets” and the rest is history. The TCP/IP protocols are still the backbone protocols of the Internet.

Since that standardization of the Internet communication protocols, nearly every aspect of modern life is affected, including our power control systems and OT systems and networks. The benefits of a standards-based approach in the Internet are driving similar benefits in the IT world for software and hardware platforms. A powerful general-purpose computer coupled with virtualization and/or container software can provide many more functions and services with better security than a traditional server environment.

This paper presents several areas of interest where continued IT/OT convergence will provide similar benefits for the electric power industry, and steps that organizations can take to prepare for the bulk electric system evolution towards a majority share of distributed energy resources and a more competitive market.

Data Analytics
Most can agree in general that the more information gathered and analyzed regarding a process or problem will result in a better decision or solution. Data analytics attempts to make
this process easier and more accurate by using specialized systems and software.\textsuperscript{6} As the electric power industry expands the use of renewable and distributed energy resources, the associated tasks of efficiency of operations, resource management and security risk management all become more dependent on the ability to gather and process information and develop intelligence for actions, decisions and process improvements.

One example of efficiency improvements is the application of machine learning algorithms to wind farms and their ability to make power delivery commitments.\textsuperscript{7} Using a neural network trained on weather forecasts and historical wind turbine data, the algorithms were able to predict wind power output thirty-six (36) hours ahead of actual generation and provide scheduled delivery commitments, which are normally more valuable.\textsuperscript{8} Integrating the weather forecasts from the IT world with the wind turbine information from the OT network allows the owner and operator to increase the overall value of the wind farms.

Another example is resource management. After losing $10M due to an extensive power failure, a major utility designed and implemented an initiative to improve its equipment and infrastructure with sensor data to better prevent future failures.\textsuperscript{9} After implementing the upgrades and applying equipment monitoring, predictive analytics and diagnostics infrastructure, the utility estimates that an additional 384 potential issues were identified, saving the utility $31.5M in repair costs. Utilizing the computing resources available on the IT side with sensor information from the OT side has allowed the utility to make significant advances in remote equipment monitoring, smart diagnostics and prognosis and data integration and visualization.

One area that shows significant progress with even more promise to reduce cybersecurity risk for OT systems is the area of autometrics or acting involuntarily. The Autonomic Intelligent Cyber Sensor (AICS) was recognized at the 2018 R&D 100 Awards, an international competition that annually recognizes the 100 most promising innovations in science and technology.\textsuperscript{10}

Using artificial intelligence algorithms, the AICS can look holistically at an array of interconnected systems, including the electrical grid, and adapt continually as attacks are attempted. It is inspired by the body's autonomic nervous system – the largely unconscious functions that govern breathing, circulation and fight-or-flight responses. Once installed, the sensor acts as a similar “nervous system” for a power grid, silently monitoring all its components for unusual activity—and learning to spot threats that were unknown when it was first installed.\textsuperscript{11}

**Protection and Control**

One of the main categories of IEDs are protective relays. These devices are critical to power generation and delivery and have been around in one form or another since the late 1890s.\textsuperscript{12} The industry has evolved from mechanical to electromechanical to digital relays as the technology has advanced to improve performance and safety. The digital protective relay has been the choice for protection and control of the electric grid since its commercial availability in the early 1980s.\textsuperscript{13}
The next step in the evolution of protective relays was enabled with the development of the IEC-61850 Standard in the 2000s and the use of sampled values services to replace the conventional CT/PT wiring in high-energy instrument transformer interfaces.¹⁴ There are many benefits of using IEC-61850 in substation automation besides decreased wiring and operating costs. Personnel safety, increased system flexibility and strategic positioning for additional automation also are major reasons to deploy a fully digital substation.¹⁵

By using the Ethernet interface (which was originally developed for IT systems) as the communications standard for all devices in the IEC-61850 Standard, all participating devices have access to all GOOSE messaging and sampled value information at the same time. Combining the digital protective relay algorithms with the information available via the Ethernet interface allows the protective relay to be completely implemented in software.

With the introduction of redundant networking architectures like parallel redundancy protocol (PRP) and high availability seamless redundancy (HSR) and highly accurate time services such as precision time protocol (PTP), all the required pieces are in place for the digital substation.¹⁶ There is no longer a need to have a separate physical device to provide the protective relay function – all protective relay functions can be provided with virtual or containerized servers, all residing on a single powerful general-purpose hardware platform. This architecture is very similar to the current IT-based server virtualization and may be the strongest example of the IT and OT convergence – to the point where all the OT information obtained from the electric grid is utilized by IT-based technology.

Substation Design
The concept of an electrical substation hasn’t really changed since the days of Westinghouse and Edison, but the details in designing and implementing a substation have taken a similar path as many other industrial infrastructure efforts.¹⁷ Gone are the days of spending many hours at a drafting table drawing individual components of each substation. Technology-enhanced engineering has replaced many of the manual processes used in the past, but many of these tools are standalone and not integrated for maximum benefit. For example, Bill of Materials (BOM) development can be automated with spreadsheets and backend databases of substation components. Computer aided design (CAD) tools can have libraries of diagrams that can be reused, but they may not be tied to the BOM created with the spreadsheet. Analytical models that help design the electrical functions of the substation are yet another standalone tool that require integration with the physical design from CAD.¹⁸

By using sophisticated CAD models and visualization capabilities developed using various IT-based tools, several software tools are enabling the next level of substation design. 3D design based on the Building Information Modeling (BIM) philosophy has the potential to improve every aspect of the lifecycle of utility assets. BIM is an intelligent, model-based process that gives professionals the tools to more efficiently plan, design and construct facilities and infrastructure.¹⁹ This IT-based technology is revolutionizing the way that OT infrastructure is designed and constructed.
Preparation for the Future

With these few examples of IT and OT convergence and many other areas not discussed here, it may seem like IT systems and people are poised to take over all aspects of the future electric utility. However, there are many aspects of OT that remain critical for electric utilities to continue innovating and improving along with all the new IT-based technology. For example, the fundamental goal of OT systems is to control the physical world and the associated risks and priorities. Electric power generation and delivery is subject to the laws of physics and electromagnetism. Due to the extreme hazards associated with generating and transmitting high-voltage electric power, OT systems are always focused on safety first, and that mindset and approach should not be diminished as IT tools and techniques become more prominent in new OT systems.²⁰

Another significant difference in OT systems is security design goals. The standard triad of information security deals with protecting confidentiality, integrity and availability of the overall system.²¹ IT systems are primarily information processing systems and tend to focus on protecting the confidentiality of the information. OT systems are more concerned with protecting the integrity and availability of the system, and the associated security controls reflect this focus.

Finally, OT operations are significantly different than IT operations. Many IT operations have a scheduled weekly downtime that is used for system maintenance and patching. Because of the availability requirements of OT systems, any changes required due to system software or firmware updates, including security patches, require significant planning, testing and scheduling to implement on production environments. In many cases, a scheduled maintenance period or electrical outage for a location is required to complete the installation.²² In addition, some OT processes may require revalidation or recertification when updates are applied to the system. In short, OT operations require significant lead time and effort prior to system changes.

Organizations should take advantage of the benefits of IT and OT convergence without losing the core values and principles that define decades of successful electrification of the United States. Review the following suggestions for strategic planning, risk management, industry engagement and resilient operations.

1. Strategic Planning – Control Systems for DER
As the growth of distributed energy resources (DER) continues to dominate new power generation sources, the number of SCADA systems required to manage these new sources also will increase. This growth will increase the complexity of the overall grid control system.²³ Meanwhile, the market will be extremely competitive for SCADA engineers who understand the communications and protocols associated with IT and OT convergence for DER integration and management.

Automation of new and existing SCADA systems will help maximize the engineers available for DER tasks. Utilities will need to develop a SCADA Architecture Roadmap that provides guidance for scaling and efficiency as the SCADA systems increase in number, size and complexity.
Organizations also need to develop strategies for investment in training, recruiting and retaining staff to be competitive as more DER is added to the grid.

2. Risk Management – Changing Priorities
The amount of IT and OT convergence and DER available in the next 30 years is expected to dramatically increase. This increase shifts risk management issues from internally to externally focused threats because of the number of independent power producers, independent transmission companies, and new DER-based companies. Much of this risk concerns cybersecurity issues commonly seen in IT and OT convergence areas such as access control and ownership, but there are other risks associated with DER. There are business risks in dealing with new issues such as storage and complex interconnection agreements. Electric utilities also need to address indirect risks from higher DER, including resource planning associated with forecasting load and load shapes as well as financial planning for rate design and cost recovery.

Organizations need to perform an overall risk assessment related to the anticipated changes of DER, SCADA systems and the various organizations that will require contractual and interactive access to OT systems.

3. Engage in Technical Standards
Many of the communications protocols and standards used in both IT and OT are developed and enhanced by professional associations such as IEEE and CIGRE. There are always opportunities for interested individuals to participate at different levels of the association and meet other like-minded individuals who have a deep understanding of the subject. Many of the meetings are held via web conferences and can be attended without travel and associated costs. The overall technical understanding of staff members can be significantly increased by having one or two individuals participate in one or more standards processes.

4. Resilient Operations
One of the most important metrics used in the electric utility industry is reliability. In fact, other industries use the term “keeping the lights on” as a measurement of how well they maintain their operations. The ability to maintain the same level of availability across the service area will become harder to do as the complexity of DER and SCADA systems increases. Utilities will need to increase the level of automation at the distribution level to maintain an acceptable level of reliability, using technologies such as outage management systems (OMS) and automated distribution management systems (ADMS) – modular systems with OMS, distribution SCADA and other modules. Of course, these systems add to the overall level of IT and OT convergence and complexity, but they also bring a tremendous amount of new capabilities to maximize efficiency and have a detailed operational view of the distribution system.

Summary
The age of OT systems being custom hardware and software are largely in the past. The ability to standardize on the TCP/IP communication protocols prepared IT systems for their tremendous impact on the world over the past 30 years. Similar advances in OT system communications, specifically DNP3 and IEC-61850 for electric power SCADA systems, have
brought similar standardization to OT systems. With the advent of additional digital systems to replace the CT/PT wiring for protective relays, the scalability of general-purpose computing hardware can replace many hardware components with equivalent software functions.

The future of higher DER penetration will increase the amount of information available for data analytics, another IT-centric function that is poised to provide significant benefits to OT systems and operations. Finally, the ability to bring a BIM model to 3D substation design provides significant safety and efficiency benefits for all involved parties.

Electric utilities need to prepare for IT and OT convergence by implementing a strategic roadmap for SCADA architecture that reflects the digital substation as well as the anticipated growth of DER in the energy market. Engineering staff also will need to learn how to design and manage OT systems in this new environment and stay engaged with the standards development processes.

Risk management needs to account for more external risks as the number of potential business partners increases due to DER interconnection. OT systems also will need to look at additional automation from OMS and ADMS to handle the increasing complexity of the distribution grid.

---