21, rue d'Artois, F-75008 PARIS
http://www.cigre.org

CIGRE US National Committee
2019 Grid of the Future Symposium

Recommended Solutions to Major Security Challenges Facing OT & IT Personnel within Smart Substation Environments

M. COLE
3 Phase Associates, LLC
USA

J. PACK
POWER Engineers, Inc.
USA

SUMMARY

The electric power industry has come a long way since the 1900s, with respect to evolving from legacy analog devices to new and advanced digital technologies. "Today, microprocessor devices used by power utilities have advanced into smarter and more intelligent devices, known as intelligent electronic devices (IEDs). These IEDs aid power operators, technicians, and engineers in better decision making, offering more tools for controlling and monitoring power flow that can perform routine maintenance testing 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 supervisory control and data acquisition (SCADA) functionality." [1]
As power control systems and operational technology (OT) systems continue to progress so does their dependence on information technology (IT) systems for communications and enterprise network connectivity. The OT world of SCADA and control systems for power substations continues to evolve with more influence, products and services from the IT world. The need for a unified cyber/physical security approach within the smart substation environment that protects the overall goal of safely delivering electric power to customers is not only a laudable goal, but an absolute requirement as the two traditional OT and IT environments start to become a single solution. The OT and IT convergence are a reality due to the integrated and complex computing e.g. networking and communications taking place within OT environments. This paper reviews some of the major security challenges facing OT and IT convergence with power utilities, particularly within smart grid (SG) and smart substation environments. Also, recommendations are provided for implementing and maintaining proper security controls in the new combined OT/IT environment.

KEYWORDS

Security, SCADA, OT, IT, convergence

jeff.pack@powereng.com

INTRODUCTION

Decades ago, "cyber-crimes were minor and reduced to stealing identities, credit card fraud, long distance calling or corrupting personal computer (PC) hard drives with viruses and malware. These crimes have intensified over the years to attacking public infrastructures such as banks, businesses, government, and other entities including utilities." [2]
These adversaries are applying more sophisticated tactics by attacking a nation's critical infrastructure. Since almost everything depends on electric power to function, it makes the electric power grid and its systems one of the top critical infrastructures to protect. There have been cyberattacks and cyber attempts on power grids in the past. Two successful and most devastating attacks affected Ukraine's power systems. "The first cyber-attack on Ukraine's power grid in December 2015, for the most part, infiltrated a legacy SCADA system (via spear phishing emails) that allowed full access to the operation of 30 substations via remote terminal units (RTUs), ultimately de-energizing power circuit breakers that killed the power to over 250,000 users for up to six hours. The second cyber-attack against Ukraine, which happened approximately one year later, had a similar and more severe penetration but surprisingly caused fewer outages and affected less customers." [3]
Evolving technologies used by electric utilities continue to increase into major data driven, data intensive, and connected devices that present enormous challenges for protecting power grids. "In light of the increased cyber threats facing electric utilities today, SCADA systems are the greatest threats." [3]
Protecting the bulk electric system (BES) and its critical cyber assets (CCAs) against cyberattacks remains a great concern since some of the first NERC CIP standards were approved in 2007. [4]

OT AND IT SUBSTATION CONVERGENCE OBSTACLES

Over the last few decades, communication devices and information technologies have advanced in terms of power, control, bandwidth, automation, monitoring, etc. These advancements in technology have also benefited the power utility industry by providing them with better IEDs. IEDs and SCADA systems have been grouped together in harmony providing real-time control and functionality paving the way for SG. SG has greatly improved power system reliability by implementing many more monitoring capabilities, automation, and system data points. Although vast improvements with system reliability have been recognized, the required remote communications and monitoring has presented major security risks for power utility owners and operators.
As the number of internet of things (IoT) devices increase with new substation devices that can communicate remotely over the Internet using the Internet Protocol (IP) and Ethernet, major security challenges continue to grow for power utilities.
One of the main obstacles today is that power substations and associated electronic security perimeters (ESP) are equipped with connectivity of both OT system devices and IT network components, adding major security vulnerabilities.
Due to the convergence of OT and IT systems within smart substations, cybersecurity threats are increasing, creating a larger cyberattack surface for hackers and adversaries. An important example is the attack that took down Ukraine's power grid, which began as an infiltration in their IT corporate networks that quickly spread to their OT systems putting customers in the dark. Malicious attackers are also using vendors, such as maintenance companies and other poorly defended OT/IT systems as penetration points for breaching both OT and IT networks and systems of much larger entities. "Since power utilities are not in the business to manufacture equipment, they rely heavily on hundreds of suppliers and vendors to carry out

their mission. If the third-party vendors' physical and cybersecurity policies and procedures lack proper scrutiny and robustness or do not match the level of security of the T&D utility, how can the utility be resilient to an attack if the supplier is considered the weakest link? This question proves to be especially pertinent in light of Target Corporation's November 2013 cyber intrusion caused by malware infection to Target's HVAC vendor." [5]
The roles of OT and IT are now extremely important considering this ever-increasing attack vector facing power utilities.

ROLES OF OT AND IT WITHIN POWER SUBSTATIONS

OT within power utility substations consists of systems, including both hardware and software, for controlling, monitoring, and detecting changes with components such as SCADA, RTUs, IEDs, etc. OT systems are used by operators, technicians, engineers, and other utility personnel for properly delivering electric power to their customers and end users. [6]
IT uses microprocessor-based systems, that include both hardware and software, in order to manipulate both data and information for storing, retrieving, and transmitting for corporate enterprise systems and OT networks. [7]
OT and IT hardware and software systems, for the most part, perform very different functions. OT systems focus primarily on delivering electric power to customers safely, reliably, and economically, whereas IT systems focus primarily on corporate functions that support day-to-day enterprise. With OT and IT personnel having diverse backgrounds, OT and IT departments also have separate management structures with different goals and visions. In the past, OT was less concerned about security and more concerned about safety, reliability, and the availability of operational systems. OT systems were isolated from IT infrastructures and corporate networks, where today this is not the case.
Likewise, in the past, IT personnel have always been concerned with the security, protection, and the availability of corporate data information, financial, customer records, etc., including remaining up-to-date with the latest hardware and software systems. Today, IT systems are used in power substations for network connectivity to OT systems such as SCADA, RTUs, IEDs, human machine interfaces (HMIs), smart meters, and providing bi-directional external routable connectivity (ERC).

MAIN DIFFERENCES WITH OT VERSUS IT ENVIRONMENTS

The functional requirements for OT systems are quite different from traditional IT systems. In general, OT systems are focused on safety for people and equipment, controlling and monitoring industrial processes, and automating manufacturing or commodity delivery systems. IT systems are focused on managing information associated with businesses and consumers, such as Google or Facebook. Since these functions are so different, the associated risk management, performance, communications, and hardware are all similarly different [8].

In the past, the differences in OT systems were easy to determine. The hardware and software were all isolated systems with largely proprietary solutions from a single vendor. However, the market has changed. Introduction of economical and flexible Ethernet communication systems and powerful, low cost hardware computing platforms for the IT market have taken over much of the OT market. In addition, software is now the focus for many OT systems, which reflects the need to add additional security controls, such as intrusion prevention systems/intrusion detection systems (IPS/IDS) to maintain the design goals of OT systems.

The following table summarizes many of the differences in design and implementation between the two types of systems.

Element	OT Focus	IT Focus
Personnel	Engineering	Computer Science
Risk and Security	Integrity and Availability	Confidentiality
Communications Time and Performance	Real-Time Data Acquisition	Bandwidth
Computing Resources	Limited on specialized devices	High performance on general purpose hardware
Environment	Ruggedized Hardware for Remote Locations with minimal HVAC	Data Center
Patch Frequency	Minimize downtime – schedule patching during system outage	Patch as soon as possible and as often as needed
Device Lifetime	10-20 years	3-5 years

The technical advances in hardware, software, and communications have fostered the notion of "IT-OT Convergence" that is seen in many publications [9]. "OT must keep up with the rapid increase of networking features, capabilities, and standards. These are being introduced at a speedy pace to an IT industry exploding with new mobile communications, consumerization of IT, virtual desktops, cloud computing, and new computing/communication platforms such as tablets and smartphones. It's no longer feasible to effectively scope, architect, design, build, and maintain operational systems in groups of silos using ad-hoc approaches." [10]

The convergence between OT and IT systems and personnel within the power utility sector must happen for success and is not avoidable. If OT and IT departments and their personnel are not on the same page and cannot find common ground, major vulnerabilities, breaches, and attacks may occur causing power disruptions and outages to customers while leaving utility owners and operators hopeless. Likewise, operating utility OT systems and IT networks with legacy hardware and software systems also presents major cyber vulnerabilities and increases the threat risk due to vendors no longer supporting or supplying security patches.

The following sections discuss the inevitable convergence of these system designs and provides suggestions to maximize the benefits and resolve the associated security challenges.

IMPORTANCE OF BOTH OT AND IT ROLES IN SMART SUBSTATIONS

The core function for both OT and IT systems in a smart substation is based on the absolute requirement to facilitate the safe, secure, and reliable delivery of electric power to the customer. This function is performed through the use of a protection scheme for power delivery using protective relays, fault recorders, communications equipment, and other devices to protect people and equipment from damage due to electrical faults, etc. There is also a secondary function to protect the devices and communications equipment from unauthorized access or compromise via vulnerabilities in hardware or software.

In order to perform the protection scheme and the unauthorized access or compromise protection, security controls are required to enforce access controls (for both the physical security perimeter (PSP) and ESP), system integrity via configuration and patch management

and event monitoring. These security controls require networking and communications systems to authorize individuals, provide engineering access for configuration and patch management, including logging, and monitoring to provide visibility into these systems.

Even though there are differences in design and implementation for OT and IT systems, management and staff must recognize the need to support the core function of the substation. They will need to understand the importance of each system and determine the best way to secure and maintain their co-located systems at each substation [11].

As software and virtualization technologies become the dominant systems for both OT and IT, the engineering and computer science disciplines will also start to merge into an application-driven solution. The line between OT and IT will continue to blur – mainly split on the vendor of the applications.

MAJOR SECURITY OBSTACLES FACING OT AND IT

(1) Roles and Responsibilities

Poor understanding of roles and responsibilities leads to chaos when working in the substation environment. In the worst-case scenario, injured people and damaged equipment happen when protection systems are modified without notification or approval [12].

Employees who have the role or responsibility to make specific decisions but haven't been held accountable for making effective decisions or don't have the authority to actually make those decisions become ineffective and bottleneck the organization.

(2) Training

Personnel training is important across the board, and NERC CIP considers training so important that they require it for all employees who have access to high and medium impact BES cyber assets (CAs). Staff members for both OT and IT also need to have a good understanding of the entire system for troubleshooting and efficiency.

(3) Processes and Procedures

From an operational perspective, effective and efficient processes and procedures are very important to an overall security program. An organization needs configuration management, access control, network monitoring, and restoration/recovery efforts in place. Both OT and IT need to work together so their processes are complementary and aligned with their roles and responsibilities [13].

(4) Software

The increased dependence on software in both OT and IT environments necessitates an increased focus on software security. The traditional patch cycle for OT environments of only patching when absolutely necessary and during a scheduled outage will need to change.

(5) Hardware

Equipment life cycles in OT environments are typically much longer than those in IT environments. OT equipment is normally expected at a minimum to be installed in service for ten (10) years and is designed to last well beyond the warranty period. Even so, with the advances in security controls, technology and communications, utilities may want to consider replacing equipment much sooner, similar to IT systems; to gain the advantages of better security access controls and logging, faster processing power, increased capabilities, and advanced communications.

RECOMMENDED SOLUTIONS FOR BOTH OT AND IT TO ACHIEVE CYBER RESILIENCY

(1) Roles and Responsibilities

Having both OT and IT functions in a smart substation require a clear understanding of who's responsible, accountable, consulted, and informed (a RACI chart) or other similar mechanism to define the roles and responsibilities for the organization. The RACI chart also outlines accountability and authority that drive decision-making and expectations within your organization. Verify that all team members have a good understanding of the decision matrix for your organization. Figure 1 shows an example of a RACI chart for power substations.

Figure 1 – RACI Chart

Services	Engineering	Relay Techs	IT Networking	IT Applications
SCADA Ops	R, A	C	I	I
SCADA Comms	A	I	R	C, I
Electrical Protection	A	R	C, I	I
HVAC	A	I	C, I	R
Maintenance	A	R	C, I	C, I

(2) Training

Cross-training between OT and IT staff helps everyone during troubleshooting or incident response activities. The training doesn't have to be extensive or overbearing, but at a minimum needs a lunch and learn session every month to keep everyone up to date on the system including any changes that may have been introduced since the last session.

(3) Processes and Procedures

Mature organizations have key performance metrics and indicators in place for each process. IT has had an advantage in this space due to Sarbanes Oxley requirements (for US public-owned companies) and audits associated with financial systems. OT is catching up on the compliance side with NERC CIP and additional review from management due to the publicity associated with the Ukraine power grid attacks.

Both OT and IT need to work together so their processes and procedures are complementary and aligned with their roles and responsibilities.

(4) Software

OT software vendors will need to develop a way to patch software without requiring an outage, or at least minimizing the downtime associated with patching. This issue becomes

easier to resolve in a virtual environment, where an additional virtual instance of a device or function can be brought online and stand in for the primary while it is being patched.

(5) Hardware

In order to gain modern communications and capabilities, utilities should develop and implement both OT and IT equipment replacement schedules that provide secure Ethernet connectivity and modern automation standards such as IEC-61850. This will allow power utilities to utilize modern SCADA and protection systems as well as updated security controls such as access control, network monitoring and event logging.

CONCLUSION

“Cybersecurity Protection will continue to rise due to increased threats facing the utility industry with enemy state actors and other acts of terrorism turning to cyberspace for disrupting critical infrastructure. Utilities and governments will continue increased spending for cyber protection in future years due to many more internet and Ethernet connected devices expected, thereby creating a greater cyberattack surface.” [14]
In smart substations, as OT and IT systems merge, OT and IT personnel must also converge in order to successfully achieve cyber resiliency. Both OT and IT must actively understand and pursue their roles and responsibilities of securing and protecting the power grid and its substation critical assets. Additional training and modifications to processes and procedures will need to realign to bring the two groups together for maintaining and securing the smart substation’s hardware and software systems within the PSP/ESP. This paper recommends some solutions to aid power utilities that are being faced with security challenges of OT and IT convergence within smart substation environments.

BIBLIOGRAPHY

[1] J. Cole, "Major Components for Improving Power Distribution Reliability." 3 Phase Associates, LLC – White Paper, June 20, 2019. https://www.3phaseassociates.com/major-components-for-improving-power-distribution-reliability/

[2] J. Cole and N. Wallace, "Applying NERC CIP Standards to Power Distribution Utility Control Centers to Enhance Cybersecurity within a SMART and Automated Environment." CIGRE US National Committee, 2016 Grid of the Future Symposium, Minneapolis, MN, October 30-November 1, 2016.

[3] J. Cole, "Is Your Legacy SCADA System Secure?" 3 Phase Associates, LLC – White Paper, October 7, 2018. https://www.3phaseassociates.com/is-your-legacy-scada-system-secure/

[4] J. Cole, "Challenges of implementing substation hardware upgrades for NERC CIP version 5 compliance to enhance cybersecurity." (210 IEEE, Power Engineering Society Transmission & Distribution Conference, pp 1-5).

[5] A. Aksoy, J. Bridges, J.M. Cole, F. Napier, "Methods for Reducing Cybersecurity Vulnerabilities of Power Substations Using Multi-Vendor Smart Devices in a Smart Grid Environment," CIGRE US National Committee, 2017 Grid of the Future Symposium, Cleveland, OH, October 22-24, 2017.

[6] Wikipedia, "Operational Technology," https://en.wikipedia.org/wiki/Operational_technology

[7] Wikipedia, "Information Technology," https://en.wikipedia.org/wiki/Information_technology

[8] National Institute of Standards and Technology, "Guide to Industrial Control Systems (ICS) Security," SP 800-82, Revision 2, May 2015. https://doi.org/10.6028/NIST.SP.800-82r2

[9] Sundblad, William, "How Manufacturers Can Get IT And OT To Work Together", Forbes, December 5, 2018, https://www.forbes.com/sites/willemsundbladeurope/2018/12/05/how-manufacturers-can-get-it-and-ot-to-work-together/#2817702c69ff

[10] The Digitalist Magazine, "Convergence of IT and OT In Energy and Manufacturing," November 5, 2018. https://www.digitalistmag.com/author/mohamedbabikir

[11] Harp, Derek and Gregory-Brown, Bengt, "IT/OT Convergence – Bridging the Divide," https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf.

[12] Brocklehurst, Katherine, "IT/OT Convergence Needs Conflict Resolution from Both Sides," June 21, 2017, https://www.controleng.com/articles/it-ot-convergence-needs-conflict-resolution-from-both-sides/

[13] Utilities Technology Council, "IT/OT Convergence Issue Brief," September 2018, https://utc.org/wp-content/uploads/2018/09/2018_9_IssueBrief_IT-OT.pdf

[14] J. Cole, "Some Strong Utility Trends for 2019 and Beyond." 3 Phase Associates, LLC – White Paper, January 8, 2019. https://www.3phaseassociates.com/some-strong-utility-trends-for-2019-and-beyond/