



THE

PUBLIC-PRIVATE

Analytic Exchange Program

**Supply Chain Risks of SCADA/Industrial Control Systems
in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions**

Industry Background

The U.S. electricity industry is undergoing a rapid change in its operations and controls. These changes are driven by developing technologies, the convergence of information technology (IT) and operations technology (OT), and new business models. The traditional one-way electricity grid that produces electricity at generating stations, delivers via transmission and distribution networks, and measures consumption is transforming into a multi-directional network. Smart grid technologies are increasingly used to monitor, automate, and remotely operate the American power sector.

Supervisory Control and Data Acquisition (SCADA) systems are at the intersection of this power sector transformation. These systems are the industrial control systems (ICS) and operational infrastructure that can monitor, inform, and control the grid. SCADA systems are increasingly under attack, from both a cyber and operational perspective, illustrating a growing vulnerability in the electricity grid. To better secure the power sector, organizations must: 1) anticipate the evolution of SCADA functionality and deployment; 2) understand the supply chain risks they face; and 3) take proactive measures to mitigate these risks.

Report Objective

This report expands upon the effort of last year's Analytic Exchange Program (AEP) Electricity Grid Supply Chain team by focusing on man-made supply chain risks to SCADA systems in the electricity sector. It recommends risk mitigation strategies and measures that can be proactively incorporated into the industry's supply chain to secure the electricity sector rather than reactive responses to an emergency involving critical infrastructure. The report's goal is to highlight potential security risks to the SCADA supply chain in the current nascent stage to prevent an expensive, future retrofit of an established industry.

Report Organization

This report describes SCADA systems and functions operating in the power sector and how the industry's evolution is increasing the supply chain risk to these systems. It details the existing electricity grid, ongoing transformations, and potential vulnerabilities of the SCADA supply chain. Finally, the report provides recommendations to protect the U.S. electricity system from supply chain attacks to SCADA systems.

Acknowledgement

We acknowledge and thank the state and federal government agencies, companies, and academic institutions that supported the development of this paper.

We also thank the Office of the Director of National Intelligence and the Department of Homeland Security for the opportunity to have participated in the 2016 and 2017 Public-Private Analytic Exchange Program (AEP).

People and Organizations Consulted

We are grateful to the individuals and companies that provided their time to advise, answer questions, and assist in developing the information in this report:

- Energyzt Advisors, LLC
- Eversource
- GE Global Research
- Leidos
- National Grid
- New York Independent System Operator
- Schneider Electric
- State of Connecticut
- State of New York
- State of Rhode Island
- Xcel Energy

**2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions**

Team Members

Champion:

Joyce Corell, Assistant Director, Supply Chain Directorate, National Counterintelligence and Security Center, Office of the Director of National Intelligence

Project Manager:

Tomas J. Skucas, Senior Counterintelligence Analyst, National Counterintelligence and Security Center, Office of the Director of National Intelligence

Public/Private Participants:

- Tanya Bodell, Executive Director, Energyzt
- Nancy Checklick, U.S. Department of Energy
- Wes Lammers, Xcel Energy
- Jessica Mezzanotte, FBI
- Adam Zinger, National Grid

TABLE OF CONTENTS

EXECUTIVE SUMMARY..... ES-1

1. INTRODUCTION 1

2. USE OF SCADA/ICS IN THE ELECTRICITY SECTOR 2

3. IT/OT CONVERGENCE 4

4. HISTORY OF SCADA/ICS ATTACKS 6

5. SUPPLY CHAIN RISK 11

6. RISK MITIGATION 13

7. CONCLUSION AND RECOMMENDATIONS 15

TABLE OF FIGURES

Figure 1: Role of SCADA in the Power Sector 3

Figure 2: IT/OT Convergence..... 5

Figure 3: Threat Actors in Cyber and Operational Technology Attacks..... 7

Figure 4: Illustration of Selected SCADA Attacks World-Wide 7

Figure 5: Risk Drivers..... 11

Figure 6: Pathways to Risk Mitigation 13

EXECUTIVE SUMMARY

This report continues the effort of the U.S. Department of Homeland Security (DHS) to engage public and private sectors in analyzing and addressing risks to the country's critical infrastructure. It builds upon the 2016 report, which addressed risks to the supply chain of the electricity sector, by focusing on Supervisory Control and Data Acquisition (SCADA) systems—one of the increasingly exposed areas of the U.S. electricity sector. Of the sixteen critical infrastructure sectors identified by DHS, disruptions to the electricity sector could have the most extensive impact as all sectors rely on electric power for core operations.

SCADA systems are industrial control systems that monitor, report data, and can automate controls and responses. Large-scale use of SCADA systems in the electricity sector, along with smart meters and internet communications, are generally in the planning stage at large utilities; but, wide-scale adoption is near.

Other industries have also applied this technology and experienced how SCADA systems characterize the convergence of information technology (IT) and operational technologies (OT), realizing substantial gains in efficiency and lower costs. Such benefits, however, are not without associated risks, especially in critical industries such as electricity where system security, reliability, and resiliency are paramount.

SCADA systems create cyber and operational interdependencies, thereby magnifying vulnerabilities and increasing opportunity for cyber attacks that can have operational consequences. While distributed energy resources and automation of these decentralized systems decrease physical risk, the increased communications reliance via the Internet increase cyber and operational risks.

The security of SCADA systems in the electricity sector is increasingly at risk due to the:

- Convergence of IT and OT
- Optimization of the electricity sector with SCADA systems
- Increased cyber vulnerabilities resulting from use of SCADA and ICS
- Increasing frequency of cyber attacks targeting utilities in the United States and abroad

**2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions**

To address this growing risk, this report recommends the following:

- 1. Understand the problem landscape; recognize and respond to the varied risks confronting the electricity grid**
- 2. Improve information sharing among federal, state, and industrial organizations involved with the electricity grid**
- 3. Prioritize and apply resources to change business models to better protect the electricity grid**
- 4. Adopt industry guidelines and standards over regulations relating to the electricity grid**
- 5. Support science and innovation as it relates to defending the electricity grid**
- 6. Develop industry tools and avenues for testing IT/OT**
- 7. Promote education, training, and awareness relating to security of the supply chain for the electricity grid**

As is widely noted, “Security is a journey, not a destination.” As the electricity industry evolves, security measures need to evolve in tandem. As use of SCADA systems grows and is integrated into new technologies, supply chain controls need to be adapted. Increasing risks to the power sector infrastructure require greater awareness, understanding, and communication between industry and government.

The 2016 AEP study examined the supply chain of the “new grid” that is evolving with embedded smart technologies to improve resiliency and productivity of the grid. This report culminates two years of study of risks associated with the supply chain of the electricity grid – perhaps the most crucial of the U.S. critical infrastructure sectors.

Recommendations carried over from last year:

- Prioritize supply chain risk management at all levels
- Emphasize incentives for supply chain compliance
- Improve information sharing and business best practices

For further information, see the AEP 2016 white paper, *Identifying and Mitigating Supply Chain Risks in the Electricity Infrastructure’s Production and Distribution Networks*.

1. Introduction

This report examines evolving threats and vulnerabilities to the U.S. power sector from SCADA systems. It concludes with strategies and recommendations to mitigate the risks and minimize the impact of successful attacks on the integrity of power system controls and data acquisition resources.

For most people in the United States electricity is ubiquitous, expected, and central to almost every aspect of daily life, as can be seen in the scenarios below (each has occurred in some form, dating back to 2003).

- A sensor fails to identify and warn system operators about a system duress, resulting in a loss of power to 50 million people, 600 stranded trains, car accidents caused by inoperative traffic lights, and an inability to purchase gas or access cash from automatic teller machines across the entire Eastern Interconnect.
- An operator at a nuclear power plant watches his remotely accessed cursor scan across his computer screen and shut down controls in the nuclear power plant. The operator fears a nuclear core meltdown.
- 225,000 customers are denied power because adversaries accessed the IT networks, remotely controlled the SCADA distribution management system, and executed a telephone denial-of-service attack to prevent customers from reporting the situation.
- A ransomware attack infiltrates a company's network, encrypts files, and disables computers, causing utility services to be offline for 11 days.

Threats to the electricity grid are multiple and varied. New technologies create new vulnerabilities and adversaries develop new malware and other methods to exploit them. Currently, little incentive exists for industry to invest in measures to mitigate vulnerabilities associated with these new technologies. Cumulatively, this increases the probability and effectiveness of cyber and operational technology attacks on the electricity grid.

The following factors are considered in assessing the risk of SCADA and ICS to the electricity grid:

2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

- Convergence of IT and OT
- Users increasingly optimizing the electricity sector with SCADA systems
- Increased cyber and operational vulnerabilities resulting from use of SCADA and ICS
- New entrants and globalization making the supply chain a clear threat vector for SCADA and ICS
- Increasing frequency of attacks targeting utilities in the United States and globally

The combination of these trends points to an increased risk to the electricity industry with higher consequences of a breach of SCADA/ICS systems.

2. Use of SCADA/ICS in the Electricity Sector

The electricity industry is optimizing technology and processes in several ways. Through SCADA and ICS technology, industry can optimize processes, cost, efficiency, assets, and load management. Both IT and OT offer efficiencies to the electricity industry with software to manage energy costs and usage and to enhance automation. These capabilities also contribute to the resiliency of the electricity grid and security of electricity supply.

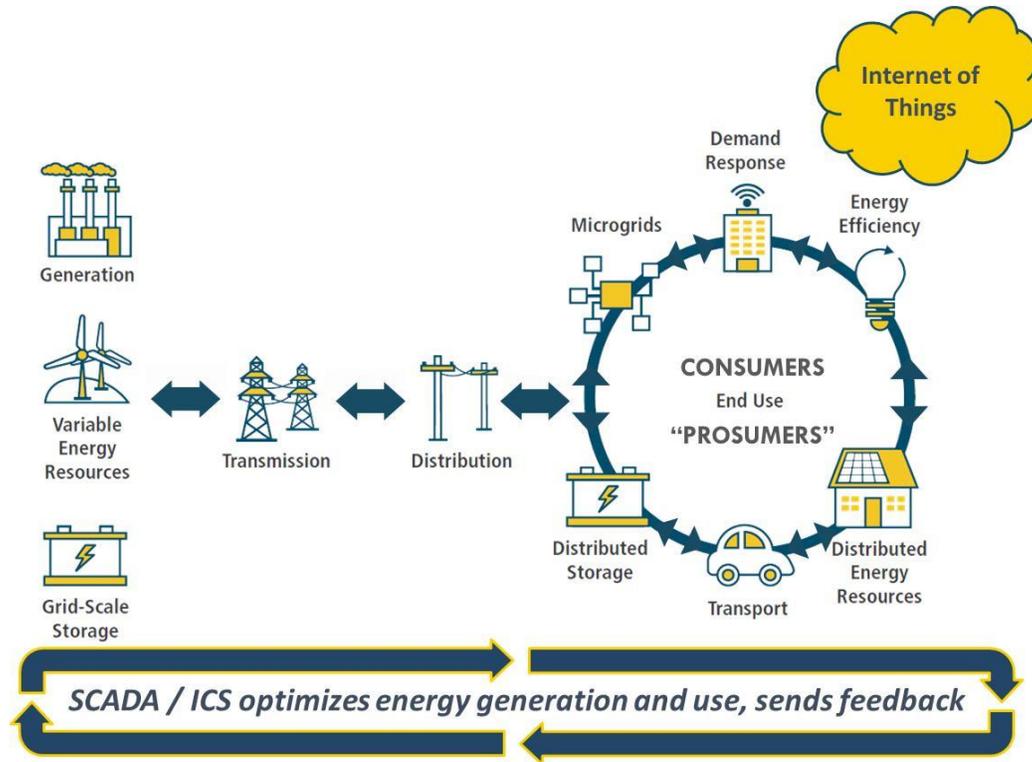
The power sector performs three primary functions:

- Generation
- Transmission
- Distribution

SCADA/ICS systems currently are embedded in these functions (Figure 1) and are anticipated to play an even greater role.

2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

Figure 1: Role of SCADA in the Power Sector



Electricity generation traditionally burns coal or gas or uses nuclear reactors. Public policies most recently have supported development and integration of intermittent renewable sources such as solar and wind. An ICS monitors the equipment and controls the environment of electricity generation facilities.

The transmission process transfers electricity from the power generation source across high voltage power lines. Considered one of the modern man-made wonders of the world, the bulk power grid delivers electricity via 283,000 miles of high voltage wires to distribution systems and end-users. SCADA systems monitor the transmission system, continuously sending data to the owner and operator of the transmission system (and in some markets to an independent system operator) regarding its functionality and ability to meet the demand of end-users.

Distribution systems are lower voltage networks of wires that deliver electricity from the bulk transmission system to consumers, such as individual businesses and homes. Local distribution companies also use SCADA systems to monitor and control the transmission of electricity from bulk transmission to end-users via low voltage systems. SCADA sends data back to generation utilities for system monitoring and demand side

2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

management. Currently, utilities mostly use SCADA systems for monitoring or remote control. As the industry evolves, utilities increasingly will begin using them for automated control.

Distribution systems are becoming increasingly complex as consumers adopt new technologies such as distributed energy resources, micro grids, demand response, and internet-connected devices. For example, a smart meter can allow a consumer to check electricity usage via a cloud-based application on a mobile device. These new technologies increase the importance of SCADA systems in the overall monitoring and control of the distribution grid to manage the two-way flow of electricity and information in a more dynamic environment. Since the main goal of these applications is to increase communication, feedback, and productivity, little attention may be paid to securing the technology and environment from cyber and operational technology attacks.

The Internet did not exist when SCADA systems were first developed for use in the electricity grid. Securing SCADA networks from Internet-based attacks or global supply chain infiltration was not originally considered when designing the network to support this critical infrastructure. In the past, SCADA systems operated on a separate operational network, segmented from the business network. With the introduction of external pathways to the Internet, these networks are converging, resulting in new vulnerabilities that did not previously exist.

As today's IT and OT systems become more integrated and complex, so have the vulnerabilities. For example, utilities introduce cyber vulnerabilities to generation and distribution systems when transferring control of equipment from internal networks to SCADA systems, which can be accessed through the Internet. As a result, SCADA systems could become more vulnerable to access through VPN connections, SAAS cloud-based applications bolted onto the system and sending data to an external datacenter, and Wi-Fi enabled devices that lack proper security settings.

3. Convergence of IT and OT

IT allows for the creation, storage, and exchange of information, usually via physical devices such as valves, computers, and storage, as well as software and networking equipment.

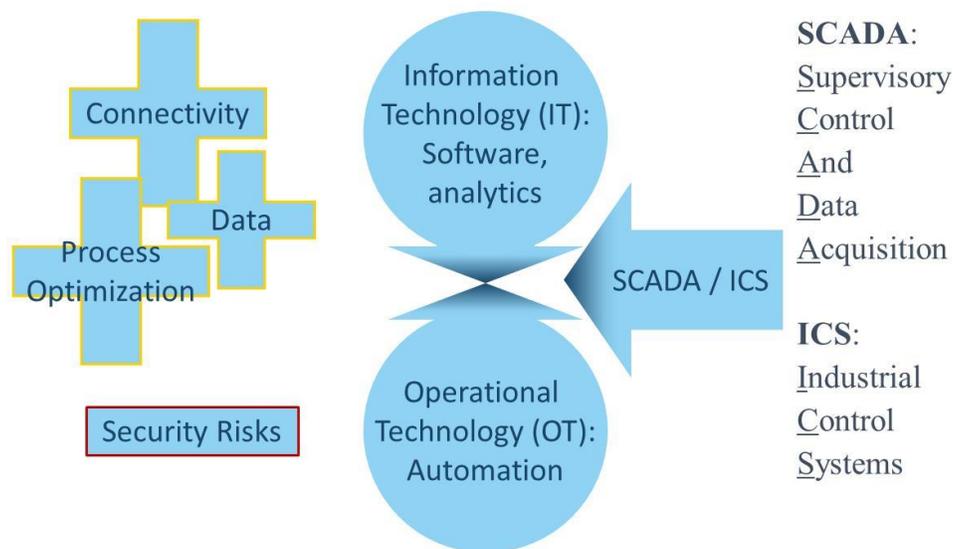
OT is a system (hardware, firmware, and software) that detects and/or causes change through direct monitoring or control of physical devices, processes, and events in the

2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

system. Most OT devices send commands with no expectation of a return acknowledgement; they do not store information and seldom exchange information. Examples of OT networks include power plants, nuclear systems, and water treatment systems.

IT and OT convergence refers to software and analytics combining with automation, resulting in increased connectivity. IT standard protocols are being implemented in traditional OT devices and systems to reduce complexity and increase compatibility with IT hardware (see Figure 2).

Figure 2: IT/OT Convergence



This shift to Internet-based data collection and control results from increased competitiveness in markets, requiring businesses to have greater data from OT environments to make more informed business decisions. This trend has accelerated over the past ten years due to the emergence of cloud computing and software-as-a-service applications. These new technologies allow mass data storage at a lower cost and automation of manually operated systems, reducing time and resources previously required. Firms also save money by integrating traditional OT networks with existing IT networks to leverage bulk pricing.

Convergence has introduced new security risks. Many OT network protocols are dated and did not include security considerations in their design. Connectivity of traditional OT devices and systems to the Internet introduces new vectors of vulnerability and opportunities to compromise systems (e.g., the ability to steal data and remotely

influence system control). Organizations recognize benefits afforded by the convergence of IT and OT systems; they do not always realize or respond to the risks or understand broader impacts of decisions.

This situation creates opportunities to innovate, improve data collection and analysis, and increase awareness of vulnerabilities of these systems which, in turn, will enhance grid security and encourage further partnerships and interface among industry, governments, and academia.

4. History of SCADA/ICS Attacks

Cyber threats to SCADA systems and ICS in the electricity sector originate from various sources, including nation states, terrorists, criminal groups, and hacktivists. Threat actors continue to adapt tactics, techniques, and procedures (TTPs) for cyber and operational technology attacks. Observed methodologies and TTPs can be applied in attacks against critical infrastructures worldwide; skills required to do so can be rudimentary.

Nation states pose the greatest threat to the critical infrastructure, although they differ in motivation, capability, and intent.¹ Russia's cyber capabilities are among the most sophisticated and are used to collect information and technology in support of its own economic development and security.² China also is sophisticated and aggressive in its cyber capabilities and collection, focusing on military, commercial, and proprietary information to support its economic growth, enhance technological capabilities, and achieve strategic advantage over other countries.³ Iran has recently expanded its cyber warfare capability and is suspected of engaging in numerous cyber campaigns against U.S. and foreign targets, compromising and destroying corporate infrastructures.⁴

Terrorists, criminal organizations, and hacktivists are also able to attack the electricity grid. Terrorists are ideologically motivated and less developed in their capabilities and may pose a limited cyber or operational technology threat.⁵ Criminal groups possess substantial capabilities and pose a medium-level threat; their motivation is financial.⁶ Cyber criminals are increasingly working with or for nation states, augmenting the threat posed by both groups.⁷ Hacktivists are typically politically motivated, possess varying capabilities, act alone or in a group, and pose a medium-level threat.⁸ A comparison of these players and their relative threat is summarized below (**Figure 3**).

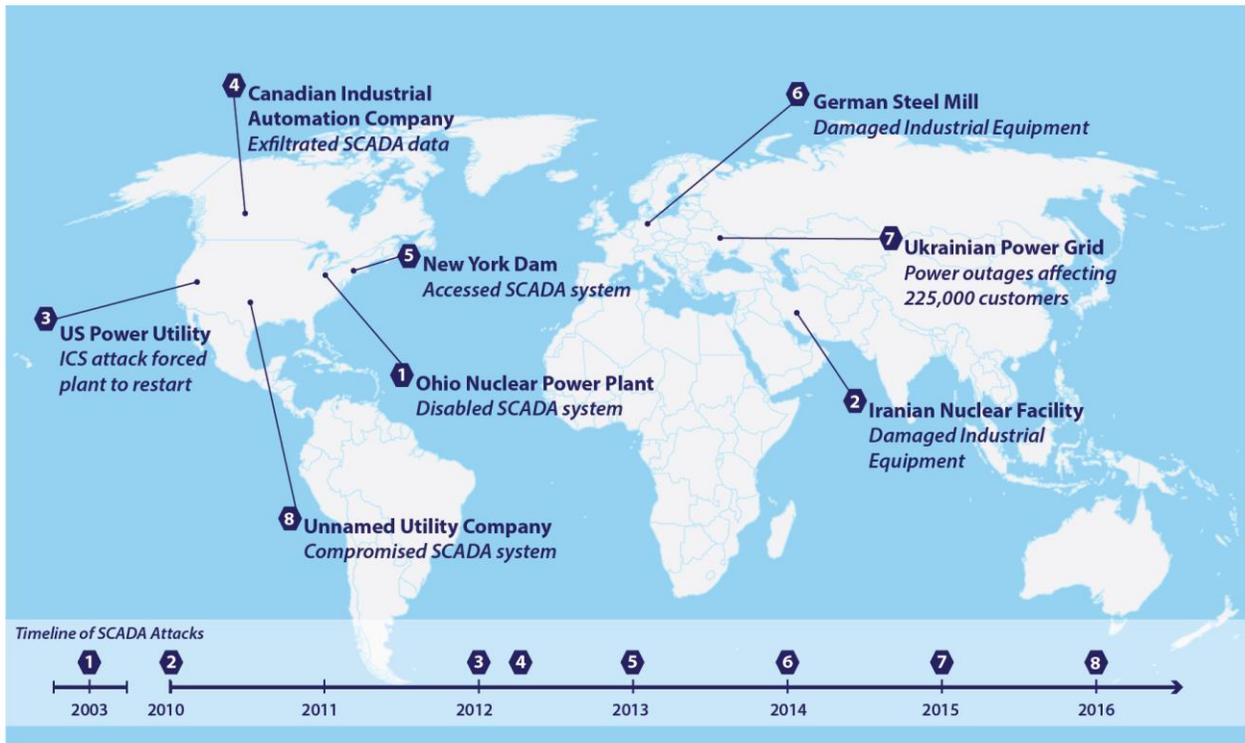
2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

Figure 3: Threat Actors in Cyber and Operational Technology Attacks

Threat Actor	Limited	Medium	High
Terrorists	✓		
Criminal Organizations		✓	
Hacktivists		✓	
Cyber Criminals			✓
Nation States			✓

These threat actors already have attacked SCADA systems worldwide. The case studies below offer valuable insights to successful SCADA-based cyber and operational technology attacks on electricity systems around the world (**Figure 3**).

Figure 4: Illustration of Selected SCADA Attacks World-Wide



(U) Source: Graphic created by Cyber Division

CYD224 Rev3 09-2017

1. Ohio Davis-Besse Nuclear Power Station, 2003

2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

In 2003, the Standard Query Language (SQL) Slammer worm, the fastest computer worm in history, attacked the private network at an idle nuclear power plant in Ohio, disabling the safety monitoring and display system for five hours and the plant's process computer for six hours. Slammer penetrated the unsecure network of a plant contractor, bypassed the plant's firewall, accessed the business network, and spread to the plant's network.^{9 10}

2. Iranian Natanz Nuclear Facility (Stuxnet), 2009-2010

Stuxnet is the first computer virus specifically targeting ICS; it allowed attackers to take control of the systems and manipulate real-world equipment without the operators knowing. The adversary targeted cascades and centrifuges at the Natanz uranium enrichment plant in Iran, manipulated computer systems that control and monitor the speed of the centrifuges, and reportedly destroyed roughly one-fifth of Iran's nuclear centrifuges by causing them to spin out of control. The attacker increased the pressure on spinning centrifuges while showing the control room that everything appeared normal by replaying recordings of the plant's protection system values during the attack.^{11 12 13}

3. U.S. Power Utility, 2012

A U.S. power utility's ICS was infected with the Mariposa virus when a third-party technician used an infected USB drive to upload software to the systems. The virus resulted in downtime for the systems and delayed plant restart by approximately three weeks.¹⁴

4. Canada Industrial Facility Telvent, 2012

Telvent, whose systems are used to remotely administer and monitor more than half of all oil and gas pipelines in North America and Latin America, was the victim of a cyber attack spanning its operations in the United States, Canada, and Spain. Threat actors breached Telvent's internal firewall and security systems, infiltrated portions of its network, installed malicious software, and exfiltrated data on customer projects. Threat actors stole OASyS project files, a product used to integrate energy companies' older IT network with more advanced "smart grid" technologies. If threat actors accessed these files, they likely gained access to project files involving other Telvent products used to manage oil and natural gas pipelines.^{15 16}

5. Bowman Avenue Dam, 2013

A threat actor accessed New York's Bowman Avenue Dam SCADA systems, repeatedly obtaining information on the status and operation of the dam, including information about the water levels, temperature, and status of the sluice gate, which controls water levels and flow rates. This access would allow the attacker to remotely operate and manipulate the dam's sluice gate. However, in this atypical instance, the gate had been manually disconnected for maintenance at the time of the intrusion.¹⁷

6. German Steel Mill, 2014

Threat actors targeted industrial operators at a German steel mill. Using spear phishing emails, they accessed the business network and then the production network. Demonstrating knowledge of the plant's ICS and production processes, they caused multiple components of the control system to become unregulated, resulting in physical damage to industrial equipment.¹⁸

7. Ukrainian Power Grid, 2015

The highly coordinated attack against three distribution companies in Ukraine is the first known attack to cause power outages, resulting in loss of power for 225,000 customers. Threat actors used spear phishing emails and BlackEnergy 3 malware to access the electricity company's IT networks. They then accessed the ICS network to remotely control the SCADA distribution management system. Threat actors used custom malicious firmware to damage field devices and prevent remote commands from being issued to substations, wiped devices to prevent automated recovery of the system, and conducted a telephone denial-of-service attack to prevent customers from contacting customer support. This is an escalation from past destructive attacks that impacted general-purpose computers and servers and is the first time the world has seen this type of attack against OT systems in a nation's critical infrastructure.¹⁹

8. Unnamed U.S. Water Utility, 2016

Threat actors accessed a water utility's business network by exploiting an unpatched vulnerability in the payment application web server and obtaining administrative credentials for the system that interconnected the IT/OT networks. They obtained control-level access to the SCADA system and altered settings that controlled the amount of chemicals used to treat tap water and water flow rates, disrupting water distribution. Alert functionality allowed the water utility to quickly identify and reverse the chemical and flow changes, largely minimizing the impact on customers. Had the threat actors been more familiar with the flow control system, the attack could have been far more consequential.^{20 21 22 23}

2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

These case studies illustrate that the risks described above are real and already occurring. Lessons learned include:

- **Global Exposure to Local Weaknesses:** Observed attack methodologies and TTPs are employable in critical infrastructures worldwide, but customized to the local environment.
- **Human Error:** TTPs used against the electricity sector include the targeting of specific individuals within an organization, the need to download files and/or perform software updates, and a company's trusted relationship with ICS and industrial suppliers.
- **IT/OT Convergence:** Business networks present a highly valued target for threat actors as they often have connections into or important credentials for the ICS network. Threat actors are able to attack business networks using traditional TTPs and then advance to a cyber physical attack to impact an operational environment.
- **Internet of Things:** Control systems are left vulnerable to cyber attacks as power companies transfer control of generation and distribution equipment from internal networks to SCADA systems that can be accessed through the Internet. SCADA systems increase efficiency at utilities because they allow remote operation of equipment; however, control systems were not designed with security in mind. Most modern power plants operate with a standardized ICS; if threat actors obtain control of one ICS, the attack can easily be replicated for other ICS.
- **Supply Chain Risks:** In addition to data exfiltration, threat actors can modify vendor software or potentially embed their own code or malware before it is distributed to other customers, providing a capability to manipulate and leverage malicious SCADA software to achieve a physical outcome.
- **Connectivity:** Threat actors can potentially infiltrate customer networks by taking advantage of the remote connectivity companies typically maintain with their clients.

5. Supply Chain Risk

Supply chain exploitation, especially when executed as a blended operation in concert with cyber intrusions, malicious insiders, and economic espionage, threatens the U.S. critical infrastructure. America's adversaries have augmented their traditional intelligence operations with nontraditional methods, including developing offensive capabilities that could be employed in a crisis or conflict to exploit, disrupt, and damage critical U.S. infrastructure.

When analyzing the components of risk, one must consider the combination a threat, vulnerability, and consequence. (see **Figure 5**).

- **Threats:** Understanding the adversary's intentions and capabilities is vital. Key here is applying the latest available threat information to determine if specific, credible evidence exists that the item or service might be targeted. While adversaries may aspire to harm the electricity grid, they can only do so if it is vulnerable to attack.
- **Vulnerabilities:** Weaknesses that are either *inherent* to the system or have been *introduced* by an outside agent create exposure. *Inherent* vulnerabilities result from things such as design oversights, poor quality control, or faulty processes and are normally not caused by malicious actions. Conversely, vulnerabilities that have been *introduced* are usually a result of nefarious activities from insiders or outsiders who have gained access to compromise some process along the supply chain lifecycle.
- **Consequences** of the risk must be considered. If the threat is realized and the system attacked and/or compromised, the outcome is either fixable or fatal.

Figure 5: Risk Drivers

Risk = f (threat, vulnerabilities, consequences)



2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

The electricity grid's supply chain is a growing concern as the IT/OT convergence within SCADA systems accelerates. As utilities modernize the embedded SCADA systems within the electricity grid, the cyber and operational technology attack surface increases as do the potential risks and consequences. The electricity sector has long recognized physical risks against the system such as natural events and kinetic attacks. Recent years have seen a shift in focus from physical to cyber security threats; it is time to focus on operational technology threats, as well.

An attack against a utility's supply chain will begin with a thorough reconnaissance of both its IT/OT infrastructure – as evidenced by the Ukraine electricity grid attack of 2015 – and gathering information about the physical components within the utility's infrastructure. The theft of proprietary information during the Telvent cyber attack illustrated how threat actors gathered product information that was later used in attacks – both cyber and/or the supply chain – against utilities using Telvent products across the United States.

Should cyber perimeter defenses be too strong, an attacker could still access the system via the supply chain. For example, the attacker could compromise software updates of either the IT or OT systems and achieve the desired goal when the utility either unwittingly uploads the malignant code into its system or the infected code is uploaded by an insider. A more capable actor could introduce malignant firmware into components – a back door – commonly used in the electricity grid for exploitation at a later date. This equipment compromise can occur during the design, manufacturing, or shipping stages.

The three main stakeholders involved with the electricity grid – utilities, industrial developers of SCADA technologies, and state regulators – are concerned with SCADA supply chains and engaged in strengthening their respective areas of responsibility. For example, utilities are proposing implementation of dedicated communication lines to bypass the Internet and create an "air gap." Some manufacturers have created multiple layers of security in purchased components with a combination of block chain verification with digital attestation to assure authentic parts, firmware, and software were used in their products. State regulators are creating agencies and appointing "cyber czars" specifically tasked with system security.

The most commonly expressed theme by all three stakeholders was the desire for more contextual information from the federal government. While all acknowledged the value

**2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions**

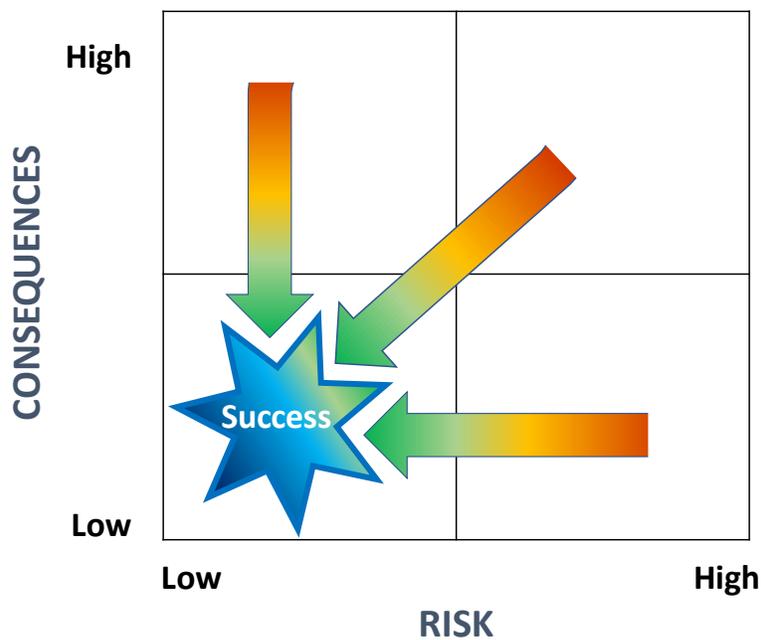
of information already received through programs such as the National Electricity Reliability Council's (NERC's) E-ISAC, they conveyed that the information was sometimes too generic or dated. Although information on cyber intrusions provided by private industry and the federal government was useful, they also wanted information on adversaries' TTPs to better understand the threat.

Two state governments also expressed frustration at what they perceived to be the federal government communicating directly with industry and utilities without including state regulators. State governments, they argued, are best situated to provide the information to all electricity grid entities as well as other critical infrastructures within their states. Additionally, few utilities employ individuals possessing security clearances and a national security background; employees may not understand the nuances of intelligence reporting.

6. Risk Mitigation

Risk mitigation includes: 1) decreasing the probability of risk; and/or 2) decreasing the consequences of risk.

Figure 6: Pathways to Risk Mitigation



2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

Multiple mitigation approaches are available to move from high consequences and/or high probability of occurrence to lower risk for SCADA/ICS in the electricity sector, including:

- Technology
- Policies and Regulation
- Process

Technology includes use of information and big data to perform testing, measurement, and detection of potential intrusions or counterfeits. For example, GE's research into the use of operational data to recognize anomalous patterns indicates that big data can be used to identify potential transgressions in operating controls. Networks should be segmented, monitored, and controlled. Limiting access to ICS and control network information that exists on the business network and implementing two-factor authentication, to include the VPNs into the ICS from the business network, are additional examples of how technology can be used to secure operations.

Policies include guidelines and standards for industry, as well as incentives. Regulations include legal requirements, audits, and penalties related to established requirements. NERC's efforts relating to cyber security in the electricity sector illustrate both the effectiveness and challenges associated with this mitigation strategy. Compliance

Government grants can provide the incentive for industry to direct its development efforts towards mitigating risks associated with IT/OT convergence. One example of this support is GE's "Digital Ghost" project. The U.S. Department of Energy (DOE) awarded grant funding to develop an automatic cyberattack detection and accommodation system for a power plant. GE developed, simulated, and tested this technology with over 99 percent accuracy. The Digital Ghost technology uses physics and operational knowledge of the power plant to detect anomalies and attacks within a framework of sensors. GE's goal is to move from incident detection, to containing the anomaly, and ultimately to neutralizing the threat. GE hopes to do this without downtime to the power plant by replacing the compromised sensor with a dynamic virtual sensor based on the remaining trusted sensors. Future enhancements could employ artificial intelligence (AI) machine learning with dynamic boundaries in a high dimensional space. If applied to the electric grid using existing data from the system, this technology could possibly be integrated with other detection systems. GE could not have developed this technology without DOE's financial support. Industry is unable to fund this type of project lacking a supporting business case.

2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

requirements serve to raise awareness but often require industry to stretch limited financial resources, thereby possibly harming the business they strive to protect. In contrast, industry often prefers its own guidelines and standards that it helped develop, contrasted with regulations created by other entities.

Processes include information sharing, developing active supply chain risk management measures, cyber defenses, incident response plans incorporating both IT and OT personnel, and resilient operations plans to survive cyber and operational technology attacks and restore the system. Information sharing is key in the identification of a coordinated attack and directing appropriate responses. The focus should be on maintaining and improving the information provided by asset owners and operators to enhance situational awareness within the sector, detect attacks earlier, and facilitate incident response. Active defense measures such as network security monitoring should be used to continually monitor networks and systems to identify abnormalities and detect exfiltration. Known vulnerabilities should be prioritized and patched regularly.

7. Conclusion and Recommendations

Use of SCADA/ICS in the electricity sector is evolving to reflect a number of external and internal trends, including emerging threats, development of new technologies and associated vulnerabilities, the convergence of IT and OT, and changing business models. Past attacks on the U.S. electricity system clearly convey potential repercussions of not protecting this critical operational technology. The following recommendations are provided to stimulate dialogue about increasing operational security measures to better defend the power sector's SCADA/ICS systems:

RECOMMENDATION 1: Understand the problem landscape; recognize and respond to varied risks confronting the electricity grid

Early recognition of the threat and proactive measures to address the evolving electricity industry and role of SCADA systems in the power sector. Attacks are likely to escalate as malicious actors, including state-supported hackers, continue to seek weak points of the power sector, including SCADA systems.

RECOMMENDATION 2: Improve information sharing among federal, state, and industrial organizations involved with the electricity grid

Knowledge is key to mitigating risks associated with an evolving set of technologies, supply chains, and the electricity industry's SCADA systems. Government and industry should increase communications channels and more freely share information. Examples include:

- White papers
- Information on attempted and successful attacks
- Data on operations to understand when deviations occur
- Analytics on collected data concerning SCADA security
- Peer information exchange
- Public to public information sharing between federal and state governments
- Coordination between state and federal intelligence
- Access to classified threat briefings and more context in unclassified reports
- More timely release of information from the federal government (e.g., warnings and intelligence)

RECOMMENDATION 3: Prioritize and apply resources to change business models to better protect the electricity grid

Encourage industry to make the business case for investment through:

- **Incentivizing pilot programs:** Fund demonstration projects and hack-a-thons to test accessibility and control of energy infrastructure.
- **Early stage commercialization:** Support new technologies to hasten commercialization of OT/IT grid security measures.
- **Improved risk valuation with insurance companies:** Educate insurance companies about risks and effectiveness of mitigation approaches to reduce insurance costs for companies that have installed industry-accepted security

2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

measures. This could incentivize energy businesses to adopt measures and receive lower premiums.

- **Wall Street risk assessments:** Encourage equity analysts to review security measures and supply chain processes as part of their business valuations.
- **Grants:** Provide the private sector funding to innovate supply chain risk management and security controls focused on OT/IT convergence.

RECOMMENDATION 4: Adopt industry guidelines and standards over regulations relating to the electricity grid

Minimize inefficiencies associated with heavy-handed regulations and look to industry to create guidelines and standards that are more adaptable across state lines for larger companies. Recognize that technology and the supply chain landscape change too quickly to be effectively regulated. Industry partners need guidance such as that provided by the Trusted Computing Group, an industry association focused on cyber security. Although the industry has begun to adopt cyber standards as part of the NERC reliability requirements, best practices should be defined and encouraged for adoption, including recognition of supply chain weaknesses. In addition, best practices should be developed for vendors to follow to strengthen every link in the supply chain.

RECOMMENDATION 5: Support science and innovation relating to the electricity grid

Due to the national security concerns with this issue, the federal government is uniquely positioned to support R&D initiatives relating to protecting the critical infrastructure. Given the global security implications, the case can be argued for advancing the technological edge of the United States and promoting global leadership and innovation in these areas.

RECOMMENDATION 6: Develop industry tools and avenues for testing IT/OT

Working with trusted industry and academic partners to test current and future grid components is key to integrating cybersecurity across the electricity supply chain. DOE should lead this collaborative work and include support for research, development, and deployment of tools and processes for testing system architectures and components. The goals include helping to identify and minimize cyber/operational technology attack surfaces, prioritize and isolate key elements of electricity generation and delivery from internal and public networks, and enable system recovery. While some programs exist

2017 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Mitigation Actions

to test and certify traditional IT components used in the industry, a considerable gap exists in the amount of programs available for OT equipment. For example, development of a testing program, possibly through DOE's national laboratories, could examine grid components, evaluate cyber malware impacts to components in a simulated environment, and assess the posture of the cybersecurity supply chain.

RECOMMENDATION 7: Promote education, training and awareness relating to security of the supply chain for the electricity grid

Developing an education, training, and awareness program for all actors within the electricity grid is a priority to ensure both cyber and supply chain security. Too often an employee has fallen victim to social engineering and inadvertently introduced malicious code or a virus to a company's IT systems. Those same social engineering skills could be used to affect SCADA systems with an assumed update or patch that actually contains malicious code from an adversary. A similar program is needed for individuals who acquire components or products for manufacturers and utilities. Regulators may be best poised to engage with both entities to develop a "best practices" guidelines that would ensure the authenticity of components being placed within the electricity grid.

In summary, the convergence of IT/OT expands both the surface area and consequences of cyber and operational technology attacks against SCADA systems. The electricity industry must recognize this and take steps to protect these systems. Miguel de Cervantes noted: "Forewarned, forearmed; to be prepared is half the victory." However, forewarned is insufficient. Attacks are already occurring.

2016 Public-Private Analytic Exchange Program (AEP)
Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector:
Recognizing Risks and Recommended Remedies
ATTACHMENT A: Case Studies of SCADA/Industrial Control System Attacks

¹ ICS-CERT; Online article; “Cyber Threat Source Descriptions”; <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>; accessed 6 June 2016.

² *Op. cit.*, endnote ii.

³ *Ibid.*

⁴ *Ibid.*

⁵ ICS-CERT; Online article; “Cyber Threat Source Descriptions”; <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>; accessed 6 June 2016.

⁶ *Op. cit.*, endnote iii.

⁷ *Op. cit.*, endnote ii.

⁸ *Op. cit.*, endnote iii.

⁹ <http://large.stanford.edu/courses/2015/ph241/holloway2/>

¹⁰ World Energy Council; Publication; “The Road to Resilience – Managing Cyber Risks”; https://www.worldenergy.org/wp-content/uploads/2016/09/Resilience_Managing-cyber-risks_Exec-summary.pdf; 6 September 2016.

¹¹ Norton; Online article; The Stuxnet Worm; <https://us.norton.com/stuxnet#details>.

¹² Wired; Online article; An Unprecedented Look at Stuxnet, the World’s First Digital Weapon; <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>; 3 November 2014.

¹³ Business Insider; Online article; The Stuxnet Attack on Iran’s Nuclear Plant Was ‘Far More Dangerous’ Than Previously Thought”; <http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11>; 20 November 2013.

¹⁴ *Op. cit.*, ii.

¹⁵ ComputerWorld; Online article; “Energy Giant Confirms Breach of Customer Project Files”; <http://www.computerworld.com/article/2491671/cybercrime-hacking/energy-giant-confirms-breach-of-customer-project-files.html>; 26 September 2012.

¹⁶ Krebs on Security; Online article; “Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent”; <http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/>; 26 September 2012.

¹⁷ DOJ; Press Release; Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector; <https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged>; 24 March 2016.

¹⁸ SANS ICS; Publication; “ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack”; 30 December 2014.

¹⁹ E-ISAC; Publication; “Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case”; 18 March 2016.

²⁰ Security Week; Online news article; “Attackers Alter Water Treatment Systems in Utility Hack: Report”; <http://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report>; 22 March 2016.

²¹ Softpedia; Online news article; “Hackers Modify Water Treatment Parameters by Accident”; <http://news.softpedia.com/news/hackers-modify-water-treatment-parameters-by-accident-502043.shtml>; 22 March 2016.

²² Belden; Online news article; “U.S. Water Utility Breach and ICS Cyber Security Lessons Learned”; <http://www.belden.com/blog/industrialsecurity/u-s-water-utility-breach-and-ics-cyber-security-lessons-learned.cfm>; 22 February 2017.

²³ *Op. cit.*, endnote xxxii.