WGCPARIS2015
WORLD GAS CONFERENCE
"GROWING TOGETHER TOWARDS A FRIENDLY PLANET"

26th World Gas Conference | 1-5 June 2015 | Paris, France

Smart Energy Future – Cybersecurity & Resilience

Table of Contents

Background

The exponential growth of activity around smart energy grids and the deployment of technological innovations in support of this have resulted in the automation of energy delivery control systems, monitoring, and metering equipment. Additionally, smart energy solutions place energy decisions in the hands of the consumer. While all this results in a long list of positives, such as increased reliability, it also expands the cyber risks for energy systems. This expansion of risks is commensurate to the present day interconnectivity of infrastructures such as natural gas, electric, water, and thermal. This places more pressure on the energy operator to take a more holistic and strategic approach.

There is a compelling vision of smart energy infrastructure that integrates natural gas with electric from multiple sources. Natural gas is an abundant, low-carbon, strategic, generating resource for electricity and a wise source for homes and businesses. Fundamentally, natural gas is a smart energy enabling smarter electric grids. This irrefutable pairing is driving a market for smart grid technologies that increase the interdependency between natural gas and electricity systems and increase the dependency on reliable telecommunications and control technologies.

Smart energy implies more system-wide reliability and security. However, this increase in integration can result in unintended risks. Smart energy technology depends on timely communication and intelligent field devices, such as sensors with two-way communications and automated or remote-control responses, which can be inherently vulnerable to cyber abuse. This change from mechanical and pneumatic controls to digital has drawn the attention of smart energy experts who are noting the need to expand beyond the sole focus of reliability to also include robust cybersecurity considerations and modern comprehensive emergency planning.

Recognizing the impracticality of monitoring and defending individual intelligent field devices, such as advanced metering infrastructure and those associated with Home Area Networks,

operators need to increase their vigilance beyond the network perimeter of the control system and further utilize a d*efense in depth* strategy, with a focus on monitoring, detection, response capabilities, and data analytics. Ideally, the objective would be to evolve into an intelligence-driven organization supporting timely response.

Aims

Natural and emerging man-made threats should be considered to inform secure infrastructure for a smart energy future. Cyber risks associated with integration of smart grid technologies and increased interdependency between natural gas and electricity systems must be considered in greater depth in corporate risk management assessment and planning activities. America's natural gas utilities and government regulators work in partnership to address constantly changing threats to the natural gas industry. Many of these programs can be applied to secure smart energy grid operations. Further, increased frequency of unprecedented natural events, such as *Superstorm Sandy* which overcame portions of the North Atlantic United States, have incited a paradigm shift among natural gas operators in their approach to emergency and business continuity planning in light of smart energy options, which minimize system-wide impacts and localize severe outages should they occur.

Methods/Results

Industrial control systems were deployed in the latter part of the twentieth century for the purpose of increasing system reliability. At that time, operating requirements and automation were of utmost importance, while cybersecurity took a backseat or was not considered for this internet-based technology. Internet risks were not foreseen, and from a corporate risk tolerance perspective, the threats and accompanying risks were considered low or not well understood. This coupled with the boom of computing, business networks, and the interconnected world in which we live, multiple vectors have been introduced for exploitation by adversaries. This has left the operators in a position where cybersecurity has to be retrofitted without impacting operations or data flows.

A significant benefit of smart energy systems is the ability to localize outages as opposed to system-wide incapacity of the grid. Reliability planning generally focuses on maintaining continuity of service in response to various contingencies. By localizing an outage, restoration becomes more manageable with less customer and safety impact. Recently, utility planners have begun to focus not just on reliability, but on resilience – the ability of a system to withstand an event and quickly restore service after a disruption. In February 2013, President Barack Obama issued *Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience*. This directive acknowledges the need for a comprehensive approach for cyber and physical infrastructure resiliency, which encourages the evaluation of infrastructure resilience from an all-hazards perspective, i.e., man-made and natural. Natural gas is identified as a critical infrastructure, and as natural gas is increasingly used to generate electricity, the interdependency between the natural gas and electricity systems in the smart energy future model requires that system planners also take an all-hazards approach to resiliency.

Man-Made Hazards – Cybersecurity & Resilience

Over the course of the past few years, there have been active series of successful and attempted cyber intrusions targeting control systems associated with natural gas pipeline sector companies. The attacks used basic exploitation techniques and readily available online tools to gain network access. In at least one case, the attackers successfully accessed the corporate environment and obtained all information needed to access the industrial control systems environment.

The awareness and reporting of incidents of internet security breaches and threats against the energy sector have increased measurably. In 2012, attacks against the energy sector comprised over 40% of all incidents as reported to the U.S. Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT). ICS-CERT reported an increase to 59% in the energy sector in 2013 but a substantial decrease to 32% in 2014. Yet, even with a reduction in 2014, the U.S. energy sector continues to lead all other sectors with the number of reported incidents. Many of these incidents targeted information pertaining to the industrial control system and Supervisory, Control, And Data Acquisition environments, including data that could facilitate remote access and unauthorized operations.

Natural gas utilities across America have been assessing cyber-related control system risks, vulnerabilities, threats and consequences, and are developing cybersecurity management programs that align with the changing risk landscape. These programs are built on a foundation of basic cybersecurity hygiene, best practices for defending against cyber attacks, and threat/vulnerability awareness; all of which may also be applied in the operation of smart energy grids. Further, these programs are layered on an extensive system of operational redundancies and fail-safes (e.g., separate and/or agnostic safety controls), which support service reliability, system resiliency, and the mitigation of catastrophic consequences.

Cybersecurity Assessment

The first steps in an effective cybersecurity program include identifying threats, evaluating vulnerabilities, weighing risks against potential consequences from a successful cyber event, and assessing the corporate risk tolerance. This can be achieved by leveraging threat models to determine the best way to minimize exposure. The American Gas Association's (AGA) Cybersecurity Strategy Task Force identified multiple leading cyber threats to America's natural gas utilities and communicated them to the membership and AGA's Board of Directors. Among these are two threats applicable in the smart energy environment, *Cybersecurity Breach of Critical Natural Gas Infrastructure* and *Dependency on Telecommunication Infrastructure*. Understanding these threats means developing the threat descriptions and listing the target types, threat actors, attack vectors, and consequences associated with a successful compromise. Attack vectors observed in the natural gas sector include malware (e.g., Conficker worm and Shamoon), spear phishing, backdoors, and brute force intrusions. Target types are evolving beyond attacking the

operator directly to compromising the information technology suppliers. This was demonstrated in 2014 with the Energetic Bear campaign, which used malware known as Havex that was inserted into the ancillary control software unwittingly sold by third-parties to hundreds of energy providers.

In addition to encouraging natural gas operators to conduct a cybersecurity risk assessment to identify the most critical functions and components of their companies used for operations, operators are encouraged to identify mitigation actions for each phase of threat management, i.e., Prevention, Preparedness, Response, and Recovery. Another grouping of informative threat management categories includes Identify, Protect, Detect, Respond, and Recover. Extrapolating a similar approach beyond cyber to all-hazards threats allows the operator to identify risks and gaps and to develop contingency plans in advance of incidents, regardless of the cause.

Public/Private Partnerships

Critical infrastructure in the U.S. is largely owned by the private sector; while government agencies have access to critical threat information. Each group controls security programs, research and development, and other resources that are more effective if discussed and shared in a partnership setting. These joint programs follow a public/private partnership model based on coordination and joint initiative planning. These programs can be used to bridge cybersecurity gaps between smart energy supply and delivery operations.

President Obama, in a speech given on January 13, 2015 at the DHS National Cybersecurity and Communications Integration Center (NCCIC), noted that protecting the nation's critical infrastructure is essential to public health and safety stating that, "Neither government, nor the private sector can defend the Nation alone. It's going to have to be a shared mission -- government and industry working hand in hand, as partners." Utilities are already partnering with Federal and State governments on initiatives intended to strengthen existing cybersecurity programs.

Some leading initiatives follow.

> *Oil and Natural Gas Cybersecurity Capability Maturity Model*. The U.S. Federal Department of Energy (DOE) worked with industry in the development of the *Oil and Natural Gas Cybersecurity Capability Maturity Model* (ONG-C2M2). The ONG-C2M2 is comprised of three parts: a maturity model, an evaluation tool, and self-evaluations. The maturity model is a common set of industry-vetted cybersecurity practices, grouped into domains, and arranged according to maturity level. The evaluation tool allows organizations to assess their cybersecurity practices against ONG-C2M2 identified cybersecurity practices. Based on this comparison, a score is assigned for each domain that is compared with a desired score, as determined by the organization's risk tolerance for each domain. This model, which was originally developed to improve cybersecurity capabilities for the

electricity subsector (*Electricity Subsector C2M2*), is being applied widely across natural gas and electric utilities to internally evaluate their cybersecurity posture. In fact, companies are being asked by their Boards for updates on their C2M2 scores.

Framework for Improving Critical Infrastructure Cybersecurity. Recognizing the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*, in February 2013. It directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary cybersecurity framework – based on existing standards, guidelines, and practices – for reducing cyber risks to critical infrastructure. NIST released the first version of the *Framework for Improving Critical Infrastructure Cybersecurity* (Framework), which was created through collaboration between industry and government and consists of standards, guidelines, and practices to promote the cybersecurity protection of critical infrastructure. NIST also issued a companion Roadmap that discusses NIST's next steps with the Framework and identifies key areas of cybersecurity development, alignment, and collaboration. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps operators of critical infrastructure to manage cybersecurity-related risk.

Energy Sector Cybersecurity Framework Implementation Guidance. DOE, in collaboration with the energy sector, released the *Energy Sector Cybersecurity Framework Implementation Guidance* (Guidance). The overall objective of the voluntary Guidance is to aid those operators with cybersecurity programs in their infancy stages as well as assist operators with well-established programs. AGA was an active contributor in the creation of the guidance document and has strongly encouraged all member utilities to review the Guidance and consider how it may be used to advance a company's cybersecurity program.

DHS Assessments. ICS-CERT provides a self-assessment tool known as the Cyber Security Evaluation Tool (CSET) that allows critical infrastructure asset owners to evaluate their cybersecurity posture against numerous standards. The tool identifies security gaps and provides recommendations for improvement. ICS-CERT also deploys assessment teams to an owner's facilities to assist with assessments, analyze network architectures, and provide detailed recommendations for improving cyber defenses.

Information Sharing. On February 13, 2015 President Obama signed a new executive order, *Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing*, aimed at improving cybersecurity information sharing between government and private industry. The executive order is designed to encourage more companies and industries to set up organizations, or hubs, known as Information Sharing and Analysis

Organizations (ISAO), where information may be shared securely. The goal is to ensure that the government can share threat information with these pre-established ISAOs more efficiently. With these functioning hubs, it will also make it easier for the government to provide companies with classified cybersecurity threat information they need to protect their networks.

Natural Hazards – Continuity Planning & Resilience

Severe storms, weather events and natural disasters continue to stress natural gas utility infrastructure and cause significant damage. A recent example was *Superstorm Sandy* in October 2012, which struck the American northeast coast disrupting electricity and natural gas service to millions of customers, with estimates up to $65 billion in damages. Natural gas distribution systems in some areas had to be completely rebuilt.

Such natural disasters do not discriminate between conventional energy systems and smart energy grids. Some smart grid technologies, such as microgrids, have an advantage in quicker restoration. For example, during *Superstorm Sandy*, some distributed generation systems, e.g., combined heat and power units, withstood the storm or were restored much more quickly compared to the rest of the electric grid. Greater continuity planning on the part of the operator underscores the outward resilience of these technologies.

As a result of events associated with extreme winds, ground movement, waves, and ice, America's 200+ natural gas utilities are adjusting their emergency response, recovery, and business continuity plans to better prepare for these extraordinary strains on operating infrastructure and service reliability. This includes participating in regional and national mutual assistance programs, which provide emergency support as needed in the event of service disruptions beyond the recovery capacity of the impacted natural gas utility and the region to assist.

There is a multitude of reference materials and tools available to assist the operator in continuity planning. AGA hosts the online *Emergency Planning Resource Center*, which serves as a springboard to the AGA Mutual Assistance Program, situation reports, and government and private sector links to support all-hazards response, recovery, and restoration. The American Petroleum Institute developed the widely referenced *Oil & Natural Gas Industry Preparedness Handbook* (Handbook), a strategy document to ensure roles, responsibilities, and needs of the oil and natural gas industry are clearly identified prior to events that may affect the integrity of oil and natural gas systems. The Handbook provides a game plan for how corporate and Federal relationships and capabilities can facilitate efficient response and recovery at the local level. Preparedness and response are approached from the local level, acknowledging that events impact workers, businesses, and communities first and foremost. While resources and information are often held at the regional or national level, it is the facility operators and those on the ground who will have the best ability to assess their systems, identify needs, and perform the work needed to restore services.

Further, because the vast majority of critical infrastructure in the U.S. is privately-owned and/or operated, during an event, the Federal government hosts timely situational awareness teleconferences with impacted critical infrastructure sectors in order to garner

and provide a larger outlook on the national, regional, and local impacts and needs. These assessment teleconferences are jointly coordinated among various Federal government agencies in a concerted effort to minimize interference with operator response and recovery.

Summary/Conclusions

Whether threats to utility systems are man-made or occur naturally, utilities must remain vigilant and comprehensively assess threats to system resiliency. Smart energy technologies are subject to both the cyber and physical threats faced by conventional energy systems. The electric industry has progressively embraced grid modernization and is leading the charge with vendors to provide more accurate real-time measurement and control systems. The natural gas industry lags behind in this initiative to modernize and automate but is making progress, learning from the experiences of the electric industry. They further gain from the resilient systems demanded, pioneered, and tested by the electric industry in response to the need for enhanced cybersecurity in remote operating technologies.

America's owners and operators work collaboratively with each other and with government agencies to share threat information to exchange mitigation practices and to jointly develop products that address the cyber risks. These cooperative relationships strengthen system security and lay the groundwork for mutual assistance during unprecedented circumstances. These lessons and programs can be applied to smart energy grid management.

References

Kimberly Denbow, Director, Engineering Services and Andrew K. Soto, Vice President, Regulatory Affairs, American Gas Association, United States.