WHITE PAPER

SECURING SCADA NETWORKS

Industrial control systems deliver valuable capabilities, but energy organizations must protect them from attack.

EXECUTIVE SUMMARY

Supervisory control and data acquisition (SCADA) networks play a crucial role in managing and monitoring the complex infrastructures that comprise the energy and utility industry. From monitoring power production equipment to controlling the flow of chilled water, SCADA networks perform functions that optimize performance, manage consumption and protect equipment and human lives.

The nature of those functions makes SCADA systems attractive targets for hackers, particularly those associated with nation-states or with quasi-governmental links. Cyberattacks are today's emerging front for warfare, and SCADA systems are among the most attractive targets. In recent years, such attacks have moved from the world of theoretical risk to practical danger as firms throughout the energy sector experienced attacks against their systems.

As governments issue warnings about SCADA-focused attacks, energy and utility companies must prioritize network security. Fortunately, policies and technologies are available to help firms protect SCADA networks and, more generally, the industrial control systems (ICSs) that manage manufacturing and other industrial processes. Energy sector organizations should conduct careful risk analyses to identify any potential missing controls and implement or enhance controls to fill those gaps.

What Are SCADA Networks?

SCADA networks form the communications, control and monitoring backbone of critical facilities supporting the energy industry. The highly specialized networks consist of sensors, controllers and communications links that allow facility operators to monitor a wide range of activities and control the operations of systems from a central facility. They allow an operator to sit at a centralized console and monitor the activity of equipment elsewhere in a building, across a campus or on the other side of the world. SCADA systems dramatically reduce manpower requirements while simultaneously increasing the ability to monitor and actively manage infrastructure components.

SCADA systems are found throughout the energy industry in applications ranging from the production of raw materials to the generation and distribution of power. Such systems are found deep below the earth in coal mines, where they link together sensors designed to ensure that the facility remains a safe operating environment. The systems continuously monitor air quality, providing safety officials with early warning of potentially unsafe conditions that might lead to an explosion, toxic environment or other hazards. At the production end of the industry, SCADA systems link complex monitoring systems found in nuclear power plants, allowing operators to monitor conditions in real time and make adjustments without exposure to hazardous conditions. SCADA systems also improve the efficiency of electrical generation plants by carefully controlling water flow to cooling systems, allowing operators to keep the plant running under optimal conditions.

Energy and utility companies derive tremendous benefit from the data-driven insights powered by SCADA networks. The emergence of the Internet of Things has dramatically reduced the cost of sensors, increased our ability to connect those sensors and made it inexpensive to retain large quantities of data for extended periods of time. SCADA networks provide the mechanism to collect data from throughout the energy production cycle and deliver it to data warehouses that power analytics. Data-driven companies may mine those databases to gain a competitive advantage in a highly competitive industry by detecting opportunities to increase production, reduce waste or otherwise optimize operations.

SCADA systems fit into the broader category of industrial control systems. While SCADA systems specifically focus on the technology that allows operators to monitor and manage processes, ICSs have even broader applications and may include components that provide a human-machine interface, distributed control systems (DCS) and programmable logic controllers (PLCs). They are often used in applications that require remote control of servo motors, such as hydroelectric dams, gas flow systems, pipelines, irrigation systems and wastewater treatment systems.

The nation's energy industry is a critical infrastructure component, driving economic productivity, industrial production, government operations and every other sector of national importance. That interdependence makes the energy industry a single point of failure for the nation's economy and, therefore, an extremely attractive target for foreign military planners and

SCADA Attack: A False Alarm

As the world awaited the transition to 2017 on New Year's Eve, *The Washington Post* ran a story that set the energy industry on edge. The ominous headline, "Russian hackers penetrated U.S. electricity grid through a utility in Vermont, U.S. officials say," sparked fear among executives and facility operators.

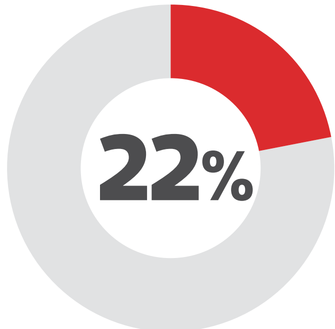
When this news story attracted the world's attention, cybersecurity professionals pointed out that the story lacked fundamental technical details that would normally be expected in such a dramatic announcement. Shortly after the story broke, Burlington Electric, a utility in northern Vermont, issued a statement acknowledging that it was the organization described in the story, but clarified that the scope of the attack was dramatically overstated. The utility had simply discovered a single laptop infected by malware, and the laptop was not connected to any elements of the electrical grid.

While the attack was a false alarm, it highlighted the fact that government agencies are paying careful attention to foreign threats targeted against the energy sector, and exposed vulnerabilities of the nation's electrical grid. The recent uptick in reported hacking attempts against utilities makes many cybersecurity professionals believe that, if foreign governments do not already have access to sensitive components of the electrical grid, it is only a matter of time before they obtain this access.

An FBI report on Russian cyberattacks against U.S. targets highlighted several areas where organizations can take measures to prevent and mitigate against attacks. These include:

- Backup of critical information
- Risk analysis
- Staff training
- Vulnerability scanning and patching
- Application whitelisting
- Incident response
- Penetration testing

other entities that may wish to undermine national security. Energy companies and the SCADA systems that control crucial processes are prime targets. In recent years, energy companies have seen a dramatic increase in foreign-originated attacks against critical infrastructure, and there is no reason to believe that increase will abate. Two emerging technology developments also increase risk to SCADA systems: cloud computing and mobile devices. While both promise tremendous financial and operating efficiencies, they also present challenging problems for SCADA cybersecurity planners.



The percentage of ICS infections that arrive via the internet[1]

Cloud computing provides organizations with flexible, scalable and cost-effective access to computing and storage, and energy companies are eager to take advantage. Cloud solutions are optimal when firms may experience spikes in demand, allowing the flexible renting of computing assets by the hour and avoiding costly capital investments. The cloud also provides an attractive opportunity for disaster recovery, sitting idle without incurring costs during periods of normal operation but allowing rapid activation of systems in the event of a disaster.

While the opportunities for cloud computing in the energy industry are extremely attractive, any move to the cloud for SCADA systems should be pursued cautiously. Companies should carefully screen cloud providers to ensure that they clearly understand the unique security needs of SCADA systems and are prepared to rise to those challenges. Companies should also fully understand the scope of service offered by the provider and how those services will fit into the organization's existing IT infrastructure, as well as how the company will retain ownership and control over data stored and processed by the cloud provider.

Mobile devices also are used widely in the energy sector. Engineers in the field use smartphones and tablets not only for personal productivity but also to interact with SCADA systems and obtain data from equipment that they are inspecting or maintaining. With that access comes a variety of new security concerns. Cybersecurity professionals must ensure that mobile access to SCADA systems is tightly restricted and carefully controlled to prevent unauthorized access to the network, disclosure of sensitive information or the transmission of illegitimate commands to SCADA devices.

Threats to Industrial Controls

Attacks against industrial control systems are on the rise and present a significant risk to energy and utility companies. A 2017 analysis by Kaspersky Lab revealed some sobering statistics on ICS attacks. In "Threat Landscape for Industrial Automation Systems in the Second Half of 2016," based on analysis of traffic to the networks of Kaspersky's own customers, 39 percent of ICSs worldwide were attacked during 2016, and more than 20 percent of industrial control devices are attacked *each month*. Threats come from many different sources using a variety of attack techniques. While some may be attributable to attackers randomly scanning networks in search of vulnerabilities, others are certainly targeted attacks on ICS technology by knowledgeable attackers.

Major sources of risk to ICSs and SCADA systems have a common root cause: The systems typically were designed more than a decade ago, when security was not a top concern for system designers. Many ICS technologies were planned to run on closed networks within a power plant or other controlled facility without any connection to the internet. The design assumption was that every other device on the network was friendly. As architects extended SCADA and ICS designs to include broader network connectivity, they attempted to add security functions onto existing products to meet a changing threat environment. Unfortunately, that "bolt-on" approach is rarely effective, making securing legacy systems and ICSs a real challenge.

Ukrainian Power Grid Under Attack

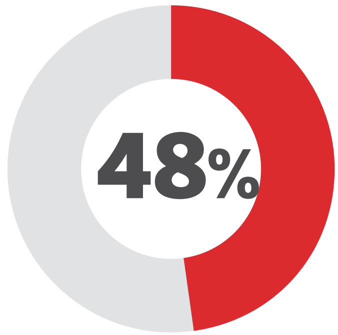
On Dec. 23, 2015, more than 200,000 Ukrainians suddenly found themselves without power in a blackout that confused officials at energy distribution companies. As they began their investigation, it appeared that 30 power substations had simply shut down, creating blackout conditions.

After performing a more thorough investigation, Ukrainian officials determined that they had been the victim of a cyberattack launched from within Russia. The attack began as early as March 2015, when attackers launched a spear-phishing campaign to gain initial access to systems. They then installed specialized malware on energy company computers. This malware, dubbed BlackEnergy, was specifically designed for use against ICSs and SCADA systems.

Once attackers gained access to the SCADA systems, they exploited vulnerabilities to take full control of the environment and gain administrative operator privileges. With this access, starting the blackout was a simple task. They simply logged in as administrators and shut down the grid using that administrative access.

Source: [1]Kaspersky, "Threat Landscape for Industrial Automation Systems in the Second Half of 2016," March 2017

The threats facing industrial control systems and SCADA systems are similar to those facing other technology devices. Cybersecurity professionals typically categorize threats as posing risks to the confidentiality, integrity or availability of systems and information. SCADA and ICS threats also fall into those categories. Confidentiality threats may expose sensitive information to unauthorized disclosure, such as allowing attackers to retrieve sensitive sensor information. Integrity threats present the risk of unauthorized alteration of information or systems. For example, attackers might alter the configuration of an ICS to present operators with false information about a system's status, potentially leading to disastrous consequences, such as building up pressure in a boiler until it reaches the point of explosion.



The percentage of IT and ICS security practitioners who map their security practices to NIST's Cybersecurity Framework[2]

Availability threats prevent authorized access to systems and information. In a critical infrastructure scenario, loss of availability may leave thousands or even millions of customers without access to essential services.

A Variety of Attack Vectors

Malware is a primary risk to all IT systems, and ICSs and SCADA are no exception. Viruses, Trojan horses, botnets and other malware seek to gain a foothold by exploiting common vulnerabilities and then using that access to perform unauthorized activities. Malware might steal sensitive information and transmit it to an attacker, provide backdoor remote access to alter the configuration of an industrial control system, or interrupt service availability by disrupting critical system components. While many attacks use automated techniques that prey on existing system vulnerabilities, others depend on human-centric vulnerabilities. Social engineering attacks manipulate legitimate users into taking actions that are detrimental to system security. For example, a social engineer might use a spear-phishing email that sends a highly targeted message to employees of an energy or utility company, informing them that they must complete their performance review by clicking on a link. When they click that link, they see a login screen that appears authentic, and they log in with their username and password. Unfortunately, the system is run by an attacker, who then captures the username and password for use in an attack. Other spear-phishing attacks may prompt users to install malware on critical system components.

Social engineering attacks prey on the susceptibility of well-meaning users to psychological tricks. Other legitimate users may have nefarious intent, deliberately seeking to use their privileged positions to undermine system security. Known as the insider threat, it's particularly dangerous because users already have a legitimate foothold in enterprise systems and then use that access to carry out malicious activity.

Brute-force attacks also are an effective way for attackers to gain access to user and administrative accounts. If a SCADA/ICS system allows unlimited incorrect login attempts, an attacker can simply try common username and password combinations until he or she stumbles on a legitimate account. Successful password-guessing attacks rely on the use of common passwords, such as names of local sports teams, common pet names, the first names of spouses or partners, and variations on those themes. Brute-force attacks target common default username and password combinations, such as "admin/admin," "default/default" or "administrator/secure," in an attempt to find systems using insecure default configurations.

SCADA systems and ICSs may contain flaws in their code, allowing attackers to take advantage of vulnerabilities. For example, attackers might insert instructions directly into the memory of an

Intentionally Attracting Attacks

While security professionals typically find themselves trying to *avoid* attacks, there is one case where they might try to intentionally *attract* attacks. That might seem counterintuitive at first, but there's a method to the madness.

Honeypots are systems that are carefully designed to attract attackers. They may seem like lucrative targets for attack with obvious vulnerabilities, but they are actually carefully instrumented environments designed to monitor attacker activity to gain insight into hacker tools and tactics. Energy and utility companies may even install SCADA software on a honeypot to further the illusion of an attractive attack target without actually connecting the SCADA system to any real control hardware.

One word of caution: An energy company shouldn't attempt to build a honeypot unless its IT leaders are very confident in their ability to create a controlled environment. It's especially important to ensure that the system is isolated so that an attacker can't turn the tables and use the honeypot as a jumping-off point to attack real production systems.

Source: [2]SANS Institute, "Securing Industrial Control Systems 2017," June 2017 industrial control system by using a buffer overflow attack that provides the system with more input than was expected.

Similarly, an attacker might execute database commands through a SCADA system by carrying out an SQL injection attack. Those vulnerabilities are extremely common in legacy systems designed and coded before developers were aware of such attack vectors, but they continue to persist in modern code.

ICSs and SCADA systems may also become the targets of distributed denial of service (DDoS) attacks, which are particularly insidious because attackers do not require system access for the attack to be successful. Instead, they use large numbers of systems under their control around the internet to send massive quantities of network traffic to a SCADA system. The goal is to bombard the system with so much network traffic that it cannot carry out its intended function or communicate on the network, leaving administrators powerless to reconfigure the system and jeopardizing the availability of system functions.

Protecting ICSs and SCADA Systems

The ever-increasing threat of attacks against ICSs and SCADA systems makes building a strong, layered defense critically important for energy and utility companies. A layered defense should consist of a combination of security frameworks, security technology solutions and security services designed to provide an overlapping set of controls that protect against risks.

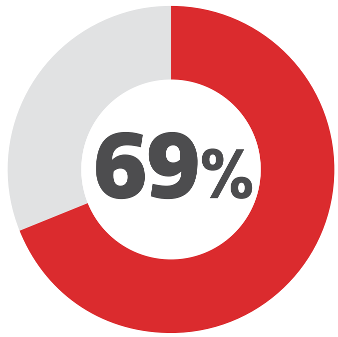
Security Frameworks

Security frameworks offer guidance for organizations seeking to design a comprehensive set of security controls. They provide best practices and advice that companies can customize for a specific operating environment. An excellent source for framework standards is the National Institute of Standards and Technology (NIST), a federal agency that produces cybersecurity standards for use in government and industry.

The NIST Cybersecurity Framework (CSF) is a wide-reaching set of materials that provides advice on five core activities in the cybersecurity realm. The CSF helps organizations adopt a risk-based approach that balances the costs and benefits of specific security controls. The five activities include:

- **Identify** core risks to an organization's systems, assets, data and capabilities.
- **Protect** systems and data to limit or contain cybersecurity incidents.
- **Detect** occurrences of cybersecurity events.
- **Respond** appropriately to detected events.
- **Recover** from the impact of cybersecurity incidents.

While the CSF is designed to be used across industries, NIST also provides specific guidance for energy and utility companies operating SCADA and other ICSs. "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security" provides detailed information on ICS threats, vulnerabilities and security controls.



The percentage of security practitioners who consider the threat to industrial control systems to be high or severe/critical[3]

Security Solutions

SCADA and ICS cybersecurity programs use a variety of technical solutions to meet the confidentiality, integrity and availability requirements of these critical infrastructure systems. Controls include multifactor authentication, firewalls, mobile device management, anti-virus, security information and event management systems, virtual private networks and patch management technology.

Multifactor authentication adds enhanced security to access control systems. Rather than simply relying on an easily stolen password, multifactor authentication supplements "something you know" authentication with an additional requirement based on either something users possess, such as a smartphone or token ("something you have"), or user's biometric feature, such as a fingerprint or voice ("something you are"), to verify identify. Multifactor authentication should always be used to protect access to sensitive SCADA systems, even if it's not required to access a wider enterprise network. Firewalls segment networks from each other, carefully restricting traffic that may flow between them. They are commonly found separating internal networks from the internet, but they can also be used internally to segment sensitive networks from general-purpose networks. Many energy and utility companies use firewalls to separate their SCADA networks from their general productivity networks.

When technology professionals use firewalls to separate networks, they must also provide authorized users access to those networks remotely. Virtual private networks (VPNs) provide an ideal solution. Authorized users employ a VPN client to create a secure, encrypted connection to the SCADA network, where they may access infrastructure. VPN access is typically restricted using multifactor authentication.

Both SCADA systems and the workstations that engineers use to access those systems must have carefully monitored configurations. Patch and configuration management solutions allow cybersecurity professionals to ensure all devices on SCADA/ICS networks are configured according to the organization's security standards, and that patches are up to date. If users access SCADA systems using smartphones, tablets or other mobile devices, specialized configuration management is often required. Mobile device management (MDM) or enterprise mobility management (EMM) solutions allow administrators to manage configurations, security patches, applications and other settings on devices, and also remotely lock or wipe devices reported as lost or stolen.

Anti-virus software is standard on almost every enterprise system, from laptops to servers, and that should also be true in a SCADA environment. Devices capable of running anti-malware software should run it at all times and be configured to receive automatic signature updates on a daily basis, if not more frequently.

Finally, organizations should prepare for the eventuality that

Source: [3]SANS Institute, "Securing Industrial Control Systems 2017," June 2017 they may experience a security incident on their SCADA/ICS networks. Security information and event management (SIEM) solutions act as a collection and correlation point for log and event information from every cybersecurity technology deployed systemwide. Security professionals use SIEM as a centralized monitoring dashboard and the jumping-off point for security incident investigations.

As organizations design their SCADA security programs, they may wish to begin with industry standard frameworks, such as those available from NIST. Those frameworks offer guidance to help energy and utility companies select the security technology that best meets their needs.

Security Services

In addition to building a strong set of cybersecurity technology controls, energy and utility companies should also consider security services from third-party vendors with specific expertise in SCADA and ICS technology. Vendors offer a wide variety of security services, including implementation and management of security controls.

Many organizations use third-party assessors to conduct testing on security controls. That approach is widely considered a best practice in cybersecurity circles because it introduces a degree of independence into the assessment process by using personnel who did not design the controls to perform the evaluation.

Vulnerability testing services conduct automated and manual scans of SCADA and ICS networks to detect the presence of known vulnerabilities that require remediation. Penetration testing services go a step further by attempting to exploit vulnerabilities to gain access to the ICS network, demonstrating the potential effects of a malicious attack.

CDW: An Energy Partner that Gets IT

CDW provides energy and utility companies with a wide variety of products and services designed to protect SCADA systems against emerging threats. The CDW team is able to draw on its extensive vast experience in the sector to customize solutions that meet the unique needs of utility and energy firms. As companies consider the security of their SCADA, ICS and IoT deployments, CDW stands ready to provide services such as:

- Framework Gap Analysis services help firms assess the maturity of their existing security programs and identify gaps requiring remediation.
- Comprehensive Technical Assessments perform more involved testing procedures that identify specific vulnerabilities in existing systems and help IT and business leaders prioritize risk remediation activities.

CDW account managers and engineers assist customers at every phase as they select and implement SCADA security products and services. CDW's team of technology professionals takes a comprehensive approach to identifying and meeting the needs of every customer.

Are your industrial control systems secure? Request a free security scan at CDW.com/threatcheck

The CDW Approach

ASSESS

Evaluate business objectives, technology environments, and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services, document technical architecture, deployment plans, "measures of success," budgets and timelines.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.