WHITE PAPER

THE CONTINUING EVOLUTION OF SCADA NETWORKS

As industrial control systems become more powerful and more externally connected, energy and utility companies must be sure to address security concerns, networking investments, edge computing and other challenges.

EXECUTIVE SUMMARY

When it comes to networking physical assets securely and reliably, the energy and utility industries have been leaders for many years. Organizations in these sectors, which often maintain remote networks of physical equipment, have long relied on technologies such as supervisory control and data acquisition (SCADA) networks and industrial control system (ICS) technology to monitor, manage and automate their critical infrastructure.

Over time, these networks have increasingly used digital technologies. This presents an opportunity for oil and gas companies to explore emerging technologies that can lead to new applications, such as predictive maintenance, which can help reduce downtime, increase the useful life of equipment and support human safety. However, increased digitization of operational technology networks can also lead to an expanded surface for cybersecurity vulnerabilities. It is essential for energy and utility companies to design their SCADA networks with security in mind, and to enforce policies that prevent employees from exposing their organizations to attacks.

A strategic approach to operational technology can both maximize business benefits and minimize the threat of cyberattacks. A trusted third-party partner can help organizations develop and implement their SCADA strategies.

The Changing Demands on Industrial Networking Technology

Decades before cities rolled out smart lighting systems and homeowners installed thermostats and televisions connected to their wireless networks, energy companies were already connecting physical assets to their IT networks. In fact, the term SCADA dates to the 1970s, and the use of computers for industrial control purposes dates all the way back to the 1950s. Very early in the history of computing, leaders in sectors such as energy, oil and gas, transportation, utilities and manufacturing recognized the potential for connected physical assets to improve efficiency and help organizations keep tabs on their operational environments.

Historically, SCADA systems and other networks that connect operational technology (OT) have helped organizations monitor, manage and automate equipment in the field. The ability to monitor physical assets without human involvement is critical, especially if equipment is spread over a wide geographical area that may include inhospitable terrain. This monitoring function also makes it possible to better manage equipment through automated alerts that are sent if something goes wrong. For instance, a supervisor might get a notification that pressure on a certain valve has increased or decreased — an issue that might lead to production delays or potentially even create safety or environmental hazards. By relying on a SCADA system for this information, human operators can quickly respond to such issues *before* they result in a major problem. Finally, advances in technology have enabled automation through SCADA networks. By automating production processes, SCADA systems can eliminate problems associated with human limitations, such as fatigue.

Today, the SCADA landscape is growing and evolving. According to one report, SCADA became a $30 billion worldwide market in 2019, with a projected annual growth of 7.5 percent between 2020 and 2026, when the global SCADA market is expected to hit $50 billion. A number of factors are driving this growth, including the robust outlook of the global oil and gas industry, rising adoption of automation in the utility sector, increasing investments in smart city projects and the growing popularity of automation technologies.

Grid modernization efforts also have an effect on the need to maintain and secure SCADA networks. Placing new equipment on the energy grid has the potential to improve reliability and performance, but it can also increase the attack surface available to cybercriminals. Even the COVID pandemic has had an impact on SCADA adoption, in much the same way the coronavirus crisis drove the adoption of tools that facilitate remote work in other industries. With more people working from home, organizations in industrial sectors have relied more heavily on technologies such as SCADA that allow human workers to monitor physical assets from a distance.

Meet Industry 4.0

One of the most important drivers of industrial networking is the rapid adoption of what are commonly called Industry 4.0 technologies, including the Industrial Internet of Things (IIoT) and public cloud resources. Coupled with the emergence of widely available, lower-cost wireless sensors and connectivity, these technologies are changing the way businesses look at the convergence of their IT and OT environments. In the past, SCADA networks were largely analog. Increased digitization will both expand the number of potentially transformative applications available to an organization and reveal new security concerns.

The percentage of security professionals who said they had encountered challenges in securing their organization's IoT devices[1]

Organizations that invest in SCADA and other industrial control systems are typically looking to enable critical business

Source: [1]securityinfowatch.com, "Survey: 99% of security pros struggling to secure their IoT and IIoT devices," March 30, 2021

outcomes such as reduced costs, heightened productivity and reduced demands on personnel. SCADA networks can also provide benefits such as greater reliability and efficiency, improved maintenance and uptime, and enhanced safety. By monitoring for tampering and equipment malfunctions, industrial control networks can detect dangerous situations and prevent them from becoming full-blown emergencies. Data from SCADA systems can also lead to more informed decision-making about maintenance schedules, preventing companies from falling victim to security and operational issues caused by allowing deferred maintenance to build up over time. An effective monitoring and control system will enable organizations to identify the root causes of equipment failure and network downtime, solve issues before they affect operational effectiveness and extend the useful life of valuable equipment.

Increased digitization can amplify these benefits, but it can also put organizations at greater risk of cyberattack. According to a 2020 cybersecurity survey , 91 percent of CISOs reported seeing an increase in overall attack frequency between 2019 and 2020. Additionally, the survey found that 54 percent of incident response professionals had recently encountered destructive cyberattacks, and 82 percent had experienced counter-incident response. The report specifically cited a potential increase in attacks on industrial networks as one of nine cybersecurity predictions for 2021.

What's in a Name (or an Acronym)?

Supervisory control and data acquisition (SCADA) networks, industrial control systems (ICS) and the Industrial Internet of Things (IIoT) are all related but distinct technologies:

- **SCADA** is a system of software and hardware that allows organizations to control industrial processes locally or at remote locations. This involves the gathering, monitoring and processing of real-time operational data and allows direct interaction with smart devices and human-machine interface software.
- **ICS** is an umbrella term that refers to multiple types of OT monitoring. SCADA is a subset of ICS, which is one reason the terms are often used interchangeably. In addition to SCADA, ICS encompasses distributed control systems (DCS), which connect controllers, sensors, operator terminals and actuators. An ICS network may monitor systems such as mining conveyor belts, electric grids and valves at a natural gas facility.
- **IIoT** refers to the extension and use of the Internet of Things (IoT) for industrial applications, with a focus on machine-to-machine communication, data analytics and machine learning. Typically, IIoT systems are able to ingest and process much larger volumes of data than SCADA systems. While SCADA systems are typically used to manage day-to-day operations, IIoT data is more often used for predictive applications, including maintenance, the reduction of downtime and expanded equipment life.

"As geopolitical tensions rise, we can expect an explosion of destructive cyberattacks against industrial control system (ICS) environments, with energy, oil, gas and manufacturing companies becoming renewed top targets for cybercriminals and spies," VMware Carbon Black wrote in December 2020. "New, destructive malware specific to ICS infrastructure will be a hot commodity on the dark web, with new versions of the Triton malware already in development."

To strike a balance that allows for operational improvements without putting their assets at risk, companies in energy, oil and gas, manufacturing and other industries must build out and manage their industrial control networks with a great deal of forethought and a comprehensive strategy.

The Elements of SCADA Technology

To build out and maintain a SCADA system that meets business objectives without putting IT and OT security at risk, organizations must carefully consider networking, edge computing, control and management, and security. While SCADA networks comprise countless individual components, a focus on these four broad functions will ensure an effective, secure network of industrial assets.

Networking

Historically, SCADA systems have been supported by wired networks. However, in recent years, more organizations have begun to add wireless connectivity to their industrial control networks, either through Wi-Fi or cellular connections.

When building out SCADA networks, it is important for organizations to solve for reliability and availability — two factors listed among Cisco's six SCADA system design principles. "Pipeline operations applications and services run in real or near real time, 24 hours a day, and the network must be available to users on a continuous basis, with little or no downtime," Cisco notes in its solution overview guide for SCADA systems in the oil and gas industries. "Operational pipeline management systems offer efficiency and reliability when they are working properly, but to know whether or not they are, you need real-time access to network health information across the system."

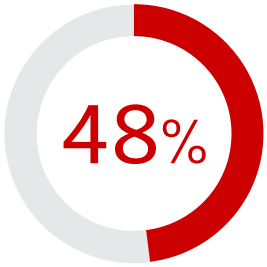
It is important for organizations to appropriately segment their SCADA networks. Rather than maintain a single network where every device can "talk" to everything else, network segmentation allows organizations to break their networks up into logical segments, based on function. This way, a single compromised element will be less likely to spark an attack capable of spreading throughout the network. Often, SCADA networks are divided into separate segments for host servers and switches, virtual servers, operator workstations and controllers.

Edge Sensing and Computing

In addition to sensors that gather data from equipment, many industrial control networks feature edge computing resources that bring processing capabilities out into the field. The "edge" in edge computing refers to physical proximity to the sites where data is being gathered. For instance, in oil and gas environments, the "edge" may mean a drilling rig that is grinding through rock, a

storage tank far from central facilities or a well that produces hydrocarbons. Or it could refer to the locations of midstream assets such as pumps, generators or even trucks. Edge computing devices must be powerful enough to process the data collected onsite and transmit it through the industrial control network, but they also must be rugged enough to operate in areas where there might not be power, lighting or onsite monitoring. Because of these hurdles, some energy companies have been slow to incorporate edge computing into their industrial control networks.

One advantage to edge computing devices is that they can store and process data locally, and transmit information to a central hub only in instances where an anomaly is noted or action is needed. This can drastically reduce the amount of data being sent back and forth over a wired or wireless network, which in turn simplifies networking needs.



The percentage of oil and gas companies that cite IT security as a driver of Internet of Things adoption[2]

Control and Management

As IT systems have become more sprawling and complex in recent years, there is increased value in simplified management and control. For instance, organizations that have invested in resources from multiple public cloud vendors often seek out management tools to help create a unified view of their environments. The gold standard is a "single pane of glass" dashboard that gives system administrators ready visibility into all components of a system within a single command center.

While some SCADA systems are too complex to be represented on a single dashboard, vendors now offer centralized management consoles that enable a comprehensive (or near-comprehensive) view of their industrial networks. These management tools can help lower overall costs and free up human operators for more mission-critical tasks.

How SCADA Systems Work

While industrial control networks are often sprawling and complex, their work can essentially be boiled down to a few broad steps:

1. Data acquisition: First, sensors in the field collect real-time data on factors such as heat, pressure, flow rates and motor speed. Field instrumentation may include proximity sensors, machine vision systems, energy monitors, and other monitors and transmitters.

2. Data communication: Using wired or wireless networks, the SCADA system transmits data gathered from sensors in the field to central hubs.

3. Data presentation: Raw data from the field must be converted into useful information. SCADA network components, such as remote terminal units or programmable logic controllers, prepare data supplied by field instrumentation for display and analysis.

4. Human-machine interface: SCADA networks use a human-machine interface to display information that needs to be monitored by workers. An HMI device serves as a SCADA system's central processor and allows operators to interact with data through a graphical interface.

5. Controlling and monitoring: Using the HMI, operators can make system adjustments as needed.

Security

In its solution overview guide for SCADA systems in the oil and gas industries, Cisco highlights both security and regulatory compliance among its six design principles. "Few industries require security more than those concerned with the protection of natural resources and the management of energy," Cisco notes. "Although the use of remote monitoring and control in critical processes continues to evolve, so does the need for enhanced security. Whether it is a measured value at a field instrument or the data path to the host, informational integrity can be realized only through focus on end-to-end data security."

Governance and asset management are critical components of SCADA security, as it is essential for system administrators to know exactly what devices are on the network. Also, it is fairly common for organizations to leave devices protected by default passwords; when operators do change them, they often choose an easily guessed word or phrase. Patching is also an important practice, but some older operating systems are no longer supported by the original equipment manufacturer.

Traditionally, energy and utility companies used air-gapped systems that weren't connected to other resources. However, these systems are increasingly being connected to networks that touch other resources, and therefore require process management, change management and asset management solutions.

Strategies for SCADA Success

Some headline-making attacks on industrial control networks show just how important it is for organizations to carefully design, deploy and manage their SCADA systems.

Alabama: In May 2021, a ransomware attack forced one of the nation's largest fuel pipeline operators to shut down its entire network for several days. The FBI stated that DarkSide, a criminal group that operates out of Russia, was responsible for the attack. Disruptions caused by the ransomware cascaded throughout the U.S. energy sector, affecting 45 percent of the East Coast's supply of diesel, gasoline and jet fuel and leading to increased gas prices at the pump for consumers.

Source: [2]Microsoft, "IoT Signals," October 2020

Florida: In early 2021, an attacker came perilously close to poisoning the water supply of the 15,000-person city of Oldsmar, Fla. The hacker likely accessed the system by exploiting cybersecurity weaknesses such as poor password hygiene and an outdated operating system. After gaining access to the system, the attacker used remote access software to raise the level of sodium hydroxide in the water from 100 parts per million to 11,100 parts per million for a few minutes. Luckily, a plant manager noticed the hack as it unfolded and was able to return the system to normal before the tainted water could hit the public supply.

Ukraine: In late 2015, hackers compromised the IT networks of three energy distribution companies, disrupting the supply of electricity to consumers in the first known successful cyberattack on a power grid. The hackers used spear phishing emails with malware to seize control of SCADA assets, remotely switching off substations and disabling or destroying infrastructure such as uninterruptible power supplies, modems, remote terminals and communicators.

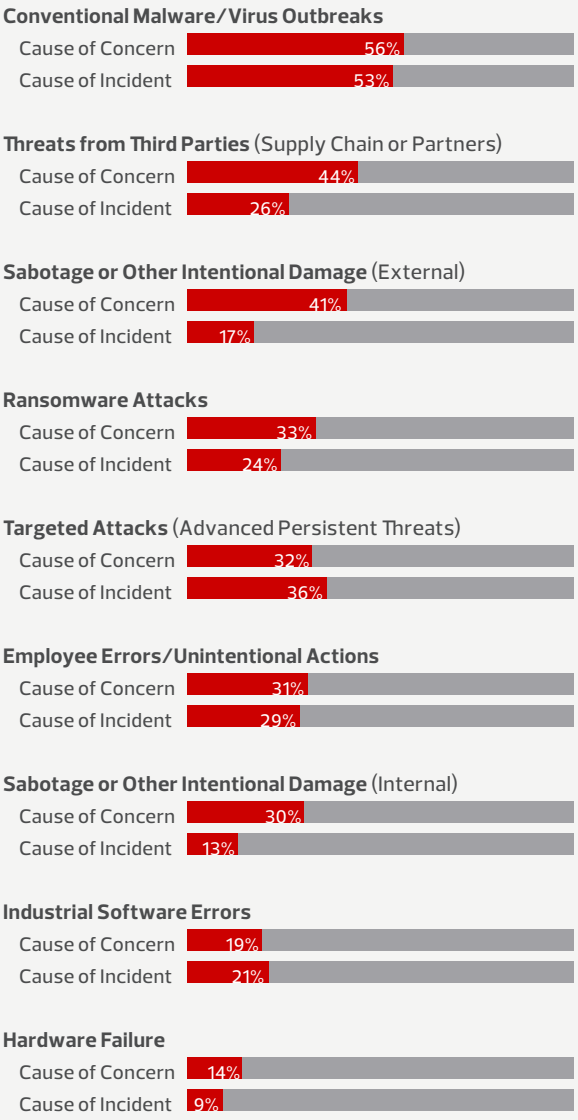
Security may be the most pressing SCADA-related challenge, but it is far from the only one. Organizations seeking to deploy and manage SCADA systems often struggle with systems integration, remote locations with poor connectivity, harsh or rugged conditions that are inhospitable to most technology devices, and regulatory compliance. Additionally, organizations must find efficient ways to securely provide data from SCADA networks to other stakeholders across the enterprise.

These challenges highlight the importance of crafting an overall strategy to guide SCADA implementation and management. Project leaders must understand their organization's environment and business objectives, and also understand exactly how different pieces of an industrial control network will interact. The use of third-party standards — such as the Risk Management Framework and SCADA guidance from the National Institute of Standards and Technology — can inform an organization's overall security strategy.

For many organizations, an effective SCADA strategy will incorporate services from a trusted third-party partner. Key services that can help a company optimize its SCADA systems include vulnerability management, application monitoring, incident response and human safety assessments.

Perceived and Actual Threats

Surveys show that organizations' top areas of cybersecurity concern tend to be fairly well aligned with the primary causes of actual incidents for industrial control systems.



Source: Cisco Systems, Oil and Gas Pipeline Security Reference Document, February 2019

Vulnerability Management Plan

Assessing network vulnerability starts with an inventory of network assets. After all, it is impossible to conduct a vulnerability assessment if stakeholders aren't aware of all of the devices, data sources and equipment attached to a network. Many traditional vulnerability management platforms conduct network scans, which are often a poor choice for SCADA networks. Connected equipment can react poorly to a ping or a scan, and in these instances, organizations need to be able to detect what is on their network (and associated vulnerabilities) without a traditional scan of the network. In such cases, passive vulnerability scanners can be a good fit. These passive scans can detect which systems are talking to each other and what firmware versions and code different systems are running — without interfering with SCADA operations.

Application Monitoring

By consistently monitoring applications, organizations can minimize the traffic running on their networks, limiting it to only the applications that are absolutely necessary to maintain operations. This prevents unwanted applications from being introduced to the network, whether by employees plugging

devices into the network or by hackers determined to load malicious software. To best protect their SCADA networks, organizations should take a whitelisting approach, being explicit in what they allow and denying everything else by default. Application monitoring efforts should also track these whitelisted applications to ensure they are behaving as expected.

Incident Response Playbooks

Too often, organizations lack a fully documented, formal response plan that can help guide their actions in the event of a major cybersecurity incident. Even when organizations have such plans in place, they may not have conducted robust testing to ensure their incident response playbooks are fully actionable. It is crucial to conduct activities such as red team and tabletop exercises to keep incident response plans up to date and give IT and business leaders the information they need to modify their plans in response to new threats. An aspect of incident response that is sometimes overlooked is public relations: When energy companies or utilities are breached, they often must explain themselves to a worried public and tense government officials. Organizations should take the time to develop policies that will allow them to publicly respond to incidents in ways that are both honest and helpful.

Human Safety Assessment

No asset is as important as the lives and safety of the people working at a facility (along with the lives and safety of the people served or affected by energy companies and utilities, such as the residents who were put at risk when hackers attacked the water supply in Florida). Organizations should conduct thoughtful, thorough assessments of how attacks on their SCADA networks could risk human safety, and then take appropriate steps to shore up those vulnerabilities.

CDW: We Get SCADA Networks

CDW's solution architects have decades of deep, industry-specific experience helping organizations design, deploy, manage and secure their IT and OT infrastructure. In particular, CDW can help energy and utility companies with the following:

Risk assessments: While networked operational technology yields a number of benefits, it can also put assets at risk. A comprehensive risk assessment from CDW can root out vulnerabilities and give organizations the information and tools they need to stop threats from getting through. Among other types of risk assessments, CDW offers penetration testing, vulnerability assessments and configuration reviews.

Gap analysis for NIST compliance: The fresh eyes of an impartial third party can be crucial in helping companies to comply with guidelines from the National Institute of Standards and Technology (NIST SP.800-82r2, at time of publication).

Policy and playbooks: Well-designed systems and strong security tools are not enough on their own to prevent security breaches. Governance is also critical in helping to minimize risks associated with human error, insider threats and social engineering attacks. CDW can help energy and utility companies to devise policies and playbooks that will keep OT and IT networks safe.

CDW AMPLIFIED™ Services

CDW Amplified™ Security services are composed of both information security and network security practices, offer an objective look at your current security posture and provide continuous defense against, detection of and response to growing threats.

DESIGN for the Future
All CDW Amplified Security services provide a comprehensive approach to prevent data breaches and proactively respond to cyberattacks.

ORCHESTRATE Progress
CDW Amplified Security engineers can assist with installation and deployment of advanced security techniques and ensure technologies are optimized for your needs.

MANAGE Operations
We can manage security solutions for you, helping you stay vigilant and maintain compliance while easing the burden on your IT staff.

Sponsors

Cisco Partner · Microsoft · SOPHOS · vmware Carbon Black

Learn more about how CDW can help your organization secure and optimize its SCADA and ICS networks.

CDW®, CDW·G® and PEOPLE WHO GET IT® are registered trademarks of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners. Together we strive for perfection. ISO 9001:2000 certified
MKT49861 — ©2021 CDW LLC

CDW PEOPLE WHO GET IT®

Daniel Balakov/Getty Images