WHITE PAPER

CDW PEOPLE WHO GET IT™

DELIVERING THE POWER OF THE NETWORK

Supervisory control and data acquisition (SCADA) networks help energy and utility companies connect their scattered sites and equipment, allowing them to remotely monitor and control operations.

Executive Summary

No matter the industry, the success of companies is becoming dependent on how effectively they are able to deploy and manage IT resources. This integrated approach to technology increasingly applies to the oil, gas and utility industries. In order to find new efficiencies, improve productivity and better compete in the marketplace, companies in these sectors are merging their operational and information technologies, collecting data from their industrial equipment and connecting machines through ruggedized networks.

Supervisory control and data acquisition or SCADA networks are designed to help organizations connect scattered sites and equipment, allowing them to remotely monitor and control operations. SCADA networks have traditionally been used by the energy industry. As locations become more remote, ruggedized hardware — capable of withstanding dust, liquids, large ranges in altitude and intense vibration — become critical to the network's efficiency and lifecycle.

To meet these needs, manufacturers design ruggedized networking tools to be dustproof and resistant to liquids. Each component of a ruggedized network is engineered to operate for long periods without maintenance. Rather than relying on vents and fans, rugged networking tools typically feature conductive cooling mechanisms.

Table of Contents

SHARE THIS WHITE PAPER

Remote monitoring with ruggedized networks is especially useful as gas and oil exploration increasingly migrates to far-flung locations that cannot easily be physically monitored. Utility companies are also using these networks to monitor equipment and improve customer service through smart meters that track and report usage without requiring a human meter reader.

Developing these complex networks requires robust planning to integrate disparate components, each of which must be carefully chosen based on network needs in order to optimize performance. As networks, including SCADA, become increasingly interconnected in order to benefit from cloud computing and the Internet of Things (IoT), security becomes a growing risk that must be addressed. Vulnerabilities in these networks could expose both IT systems and industrial systems.

Still, the benefits of implementing ruggedized SCADA networks make them worth the effort and investment. In addition to increased efficiency and productivity, networked equipment can help enterprises make more informed business decisions, reduce environmental impacts, provide better customer service and improve safety.

The Situation

As decreased regulation leads to more competition, energy and utility companies are continuously looking for an edge. Gas, oil and utility companies work in a constantly changing landscape characterized by fluctuating prices, uncertainty about future resources and increased risk of cyberattacks. In order to thrive, companies need to leverage every possible tool. Increasingly, this means uniting their field technology with their communications and information technology in the form of robust, ruggedized networks.

Historically, energy companies have not been early adopters of IT. They are in the business of bringing oil, gas or utilities to consumers as efficiently as possible. As a result, it has been easier to illustrate the benefits of operational functions, such as exploration and extraction, than IT upgrades. However, exploration and extraction are becoming more heavily dependent on IT as oil and gas resources dwindle in easy-to-reach areas. It once may have been economical to send crews to search for resource deposits and perform routine checks on equipment, but this is changing as companies move to more remote locations in search of gas and oil.

Increasingly, energy companies must rely on connected sensors to collect and transmit basic equipment safety and performance data and to alert managers if something potentially dangerous or out of the ordinary is happening. This reliance is especially true in areas where it is simply not practical to send workers to collect data — for example, 2,500 meters below the surface of the ocean. Amplifying the need for automation is the aging gas and oil workforce, a substantial portion of which is set to retire in the next few years.

8 TIPS FOR SCADA SUCCESS

Tim Haïdar, editor of the online information portal OilandGasIQ, identified eight key factors for implementing a successful SCADA system.

- **Choose a system wisely:** Companies should perform rigorous analysis of their business needs before making SCADA investments and identify the providers capable of meeting those needs. "Once you know what you want to achieve, find out which providers can actually provide all of that," says Haïdar.
- **Get network integration right:** Migrating from one system to another can cause significant downtime and carries the risk of data loss. "Make sure data is backed up, and that there is some kind of continuity planning in case things go awry," Haïdar says.
- **Prepare for environmental hazards:** New sources of gas and oil are almost uniformly found in inhospitable areas requiring ruggedized networking equipment. "The age of easy oil is over," Haïdar says. "It is inevitable that everything is going to have to go rugged, if it isn't already."
- **Plan ahead for updates:** Replacing obsolete components can lead to equipment downtime, similar to installing a new system, notes Haïdar: "You know what's coming down the pike. You just have to make sure you're prepared."
- **Watch for evolving security threats:** Like biological viruses, Haïdar notes that computer viruses evolve quickly, requiring enterprises to run regular security checks on their SCADA systems.
- **Realize that some threats are undetectable:** Enterprises cannot count on preventing every cyberattack. Therefore, they need to have a plan for handling worst-case breach scenarios.
- **Weigh interoperability considerations:** Many SCADA systems use their own dedicated and proprietary communication protocols rather than shared and open systems. This may present a hurdle for companies that want their SCADA networks to interact, for example, with mobile devices. However, achieving interoperability does have security drawbacks. "The more devices you bring into the mix, the more threats there are going to be," Haïdar says. "Now, there's a threat in everybody's pocket."
- **Be able to justify upgrades:** Upgrading a SCADA system can be extremely costly, and Haïdar says decision-makers within enterprises will be resistant to spending the money unless they can clearly see the business advantages. "Buy-in and awareness are crucial," he says.

Many oil companies that engage in hydraulic fracturing, or fracking, to extract oil from the earth have deployed mobile command centers to control operations. Sensors connected to these command centers via a SCADA network can monitor the pressure and flow of chemicals and oil in the fracking process to ensure safety and efficiency.

Companies also are connecting SCADA devices via the Internet protocol (IP), making them easier to deploy, and allowing data and device controls to be transmitted quickly and easily. This improves companies' ability to collect data and manage remote devices, alerting personnel of potential problems and helping them to address such issues.

Oil and gas companies also are making a greater investment in high-performance computing systems to help them identify, locate and exploit oil and gas deposits that are becoming increasingly hard to reach. These systems rely on massive volumes of data that are used in techniques such as 3D imaging to help exploration efforts determine where energy deposits may be located. Transmitting the mountains of data needed for these efforts from exploration sites to high-performance systems requires a powerful, ruggedized network.

60,000

Number of control systems that Russian researchers found exposed to the Internet and at risk of attack

SOURCE: IT News for Australian Business, "Hackers gain 'full control' of critical SCADA systems," January 2014

THE RISE OF THE SMART GRID

Networked (or "smart") energy meters do more than simply allow utilities to track usage remotely. They are helping to revolutionize how power companies supply electricity, and how people consume it.

Smart meters are one component of the "smart grid," which refers to a set of solutions that gathers and acts on data for more efficient production and distribution of electricity. Utility companies taking advantage of smart-grid systems are able to adjust the price of electricity based on demand.

For example, rates might go up during midday on a hot day. This increase theoretically encourages consumers to take conservation measures, such as turning down air conditioning or waiting until night to run dishwashers. Adjustments in use help to stabilize the amount of energy being used throughout the day, requiring utility companies to turn to backup or peak-demand generators less often and reducing the chance of brownouts.

Smart-grid systems also accommodate the production of renewable energy, as legacy systems were not built to handle rapid fluctuations in generation, which can occur during strong gusts at a wind power station, for instance.

A total of $9 billion in public and private funds was invested in smart-grid solutions as a result of the American Recovery and Reinvestment Act of 2009. Some cities, such as Austin, Texas, and Boulder, Colo., have been particularly active in this area.

According to a report released at the 2015 World Economic Forum, nearly $8 trillion will need to be spent worldwide in the next 25 years to meet various energy policy goals, including smart-grid enhancements.

Utilities are also becoming more reliant on automation to support their operations. As connected meters track and communicate customer energy use, utility companies are finding that they can both operate more efficiently and offer better customer service.

SCADA networks are increasingly integrated with business networks as dependence on collected data grows. High-performance computing has allowed managers to more quickly and accurately analyze data to make informed business decisions. The growth of the IoT and related hardware has also contributed to the greater interconnectivity of these once-closed networks.

For these reasons, energy companies that do not take full advantage of ruggedized networking could miss out on business opportunities, especially as connectivity and Big Data become more ingrained in the industry.

The Benefits of a Ruggedized Network

Networked equipment can mean the difference between a major problem that is caught in time and one that is not; between uptime and downtime; and between efficient and inefficient operations.

The world's leading energy companies have long known the benefits of connecting their equipment through ruggedized networks. As networks evolve to incorporate new interconnected technology, they are finding new and increasing benefits:

- **Automation:** As network-connected equipment in the field collects and transmits more data, energy companies can drastically reduce the amount of physical monitoring that must be conducted by workers. For example, many utility companies now rely on connected energy meters to report energy usage at homes and businesses, eliminating the need for regular meter-reading visits. Automation can be achieved in any situation where data could be collected by sensors, such as recording pressure and temperature readings by gas or oil companies.
- **Cost savings:** Along with automation comes the opportunity for immediate cost savings. Companies can save on both travel costs and staff time if connected sensors can collect the same

data that was previously collected by traveling employees. The additional data collected by networked equipment can also help managers to better monitor equipment performance, predict demand and prevent failures, which reduces maintenance and repair costs and minimizes downtime. Allowing automation to help with maintenance planning also allows IT staff to spend more time on long-term strategic planning, finding additional efficiencies and cost savings for the enterprise.

- **Better decision-making:** The implementation of a ruggedized network leads to the generation of more precise real-time data, which, in turn, leads to better data analytics. These analytics, often driven by high-performance computing, give managers the tools they need to make better decisions to optimize business operations. For instance, the data collected and transmitted by networked equipment can help energy companies better predict spikes in usage and demand, giving them the opportunity to prepare for these events, invest in additional equipment and increase their output.
- **Improved productivity:** When industrial equipment is not connected via a ruggedized network, enterprises can lack vital information when something goes wrong. Repair crews might spend hours onsite trying to diagnose a problem, then run the risk of further delays if they need to order a part or travel to retrieve a particular tool. A network can help to eliminate these inefficiencies. The data generated and transmitted by connected equipment may allow companies to identify problems before a repair team is dispatched. This efficiency ensures that crews have the information and tools they need to get to work as soon as they are onsite.
- **Reduced environmental impacts:** Energy companies are able to use data collected by ruggedized networking tools to reduce the environmental impact of their operations in a variety of ways. In addition to reducing the amount of travel required by staff to monitor equipment, the data helps companies to optimize the performance of equipment, potentially allowing it to perform the same tasks while consuming less energy. Networks also help companies to detect and prevent leaks or other potentially hazardous situations.
- **Better customer service:** Customers can also benefit from networked equipment. Data from ruggedized networks allows energy companies to prevent disruptions in service and respond more quickly when incidents do happen. In some cases, companies can even make adjustments remotely, quickly resolving a customer's issue. Networks also contribute to better day-to-day customer service, such as more accurate billing and remote control of equipment, for example, to limit the power supplied to a home while the owner is out of the country for an extended period.
- **Improved safety:** With the help of high-performance computing, the data collected by ruggedized networking tools can help companies to better predict and prevent equipment failure and other events that could potentially cause disasters that threaten worker safety. Another safety-related use of ruggedized networking involves warning employees of potential hazards: If data is made available to their mobile devices, they can receive automatic alerts when they enter a dangerous area.

The Elements of Ruggedized Networks

A robust and effective SCADA network consists of a number of components, including those that collect data; help the data travel throughout the network; and allow users to view and analyze data, as well as to send commands back out through the network to the equipment. A variety of storage and security tools are also important elements of an effective network.

A ruggedized SCADA network is not an off-the-shelf solution. In addition, different enterprises have vastly different needs, resulting in any number of potential network configurations. Because of the complexity of ruggedized networks, as well as the number of options available, effective planning is essential for ensuring optimal results.

Companies will often find that their internal IT staff lacks experience with developing ruggedized networks. Therefore, planning this will usually be undertaken with the help of solution architects at an external partner that specializes in networking. Time spent at the beginning of the process to analyze an enterprise's needs and map out the most appropriate solutions can help prevent problems later. By contrast, organizations that skip this step or skimp on important

THE SPECS BEHIND RUGGED TECH

Energy companies working in remote outdoor locations obviously cannot rely on standard networking devices to collect and transmit data from equipment. They need ruggedized tools that can withstand precipitation, dust, extreme temperatures and high levels of shock or vibration.

To meet these needs, manufacturers design ruggedized networking tools without vents or other openings, making them dustproof and resistant to liquids. Rugged tools also lack moving parts such as fans, allowing them to operate for long periods without maintenance. Rather than relying on vents and fans, rugged networking tools typically feature conductive cooling mechanisms.

Rugged enclosures are designed to meet a number of use specifications, including NEMA 4, established by the National Electrical Manufacturers Association for watertight operation. Other specifications include MIL-STD-810F and MIL-STD-461E, which are U.S. military standards for resistance to environmental stresses and electromagnetic interference, respectively. Other specifications include the Society of Automotive Engineers' J1211 and J1455 standards, which involve a variety of environmental factors, such as temperature, humidity, altitude and vibration.

planning may find that parts of their network are not compatible with one another, that they lack sufficient bandwidth, or that their chosen storage or security solutions do not fully meet their needs.

Common elements of a ruggedized SCADA network include:

- **Data acquisition and control systems:** These are the components that collect data from equipment and allow enterprises to control that equipment remotely. Connected sensors collect a wide range of data, including metrics such as pressure, temperature and input and output volumes. In addition to reporting data points, sensors can trip an alarm if, for instance, the pressure in a pipeline rises past a certain threshold or if the temperature in a data center nears the point where it could cause damage to the equipment.

  Employees can then use controls to manage equipment from afar, often using data from the connected sensors as a guide. For example, an employee at a company's headquarters might decide to remotely slow an input rate to lower the pressure in a pipeline or decide to remotely decrease the temperature of a data center to prevent damage to servers. (In fact, many of these control functions can be programmed to be automatically regulated by a SCADA system.)

- **Switches:** Switches are building blocks of business networks. They take packets of data from endpoint devices such as computers (or, in the case of ruggedized networks, from SCADA equipment) and analyze them to determine the destination device. The switches then "switch" the data out toward the appropriate device. Switches can either be built into other networking components or be stand-alone elements of a network.

- **Routers/gateways:** Gateways (typically routers or Layer 3 switches) examine addressing and determine where the data needs to be sent next. For example, certain data coming into a router from a rig on the Gulf of Mexico may be routed to a central data center in Ohio, while other data is sent to a server in California. Because gateways separate the SCADA network from external networks with a firewall, they provide a rudimentary layer of security.

- **Endpoints:** Connecting industrial equipment via a ruggedized network does not completely eliminate the need to send employees to the equipment location. Workers will still need to go onsite to perform maintenance. For the most part, employees use endpoints such as notebook computers, tablets and other mobile devices to record information onsite. Connecting these devices to the SCADA network gives workers real-time access to vital data, but it also creates a number of potential security vulnerabilities that must be addressed.

- **Wireless access points:** Most endpoint devices are used wirelessly on the job site, so Wi-Fi connectivity is an important element to many networks. In a warehouse environment, for example, workers may use their mobile devices to scan barcodes. This data will then be sent to wireless access points, which in turn send the information along to a router.

- **Backhaul:** Ruggedized networks require intermediate, or "backhaul," links to connect smaller subnetworks to the core network.

- **Storage:** A single sensor may generate a small amount of data. But if an enterprise adds 1,000 new sensors, all of which transmit data at regular intervals, the volume of data grows exponentially. As enterprises generate more information

47%

Percentage of process control systems that are vulnerable due to improper input validation

SOURCE: Cisco systems, "Cisco IPS Industrial Control Protection," July 2013

COMPLIANCE WITH SECURITY REQUIREMENTS

Since 2008, Critical Infrastructure Protection standards developed by the North American Electric Reliability Corp. have governed cybersecurity for the U.S. power grid. The standards require utilities to take a number of security measures, including the following:

- Develop a risk-based assessment methodology to identify critical cyber assets.
- Develop and implement security management controls to protect those critical cyber assets.
- Require personnel with access to critical cyber assets to undergo training, identity verification and criminal background checks.
- Identify and protect an electronic security perimeter encompassing critical cyber assets, as well as access points.
- Create and maintain a physical security plan ensuring that cyber assets within an electronic security perimeter are also kept inside an identified physical perimeter.
- Define methods, processes and procedures for securing critical cyber assets, as well as noncritical cyber assets within an electronic security perimeter.
- Identify, classify, respond to and report cybersecurity incidents related to critical cyber assets.
- Establish recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

from an ever-expanding network that includes many diverse sources of data, their storage demands will increase accordingly. Many companies opt for cloud-based or on-premises dynamic storage options that allow them to quickly scale up to meet new demands. Additionally, extra bandwidth will likely be necessary to accommodate the influx of new data.

As they amass vast stores of data, companies must also consider how they need to access this information. Vital data that is used often and must be accessed quickly should be stored in a system that can meet a company's requirements for speed, such as flash storage. However, such storage solutions can be costly, and lower-value data may be moved to slower media, such as spinning discs or tape drives.

- **Security hardware:** In addition to protecting the enormous amount of new data being generated by networked equipment, companies must also be concerned with the equipment itself. Vulnerability in the network could expose a company's industrial equipment as well as its IT infrastructure. In order to provide comprehensive protection, enterprises must invest in a range of security measures, including firewalls, intrusion detection and protection solutions, access controls and centralized security management.

The Importance of Security

Most equipment used by energy companies was originally created for a non-networked or closed-network environment. As a result, much of this equipment lacks adequate security to ward off cyberattacks. Greater interconnectivity increases this risk. A robust security plan is critical to protect both IT and industrial systems.

Attacks on energy and utility systems have been documented in recent decades, often with startling results. For example, shortly after Australia's Maroochy Shire wastewater treatment system installed a SCADA network in 2000, the system went haywire. Pumps did not run; alarms were not reported; sewage valves opened unexpectedly, flooding local parks and rivers with waste; waters turned black, marine life died and a permeating stench lingered in the area. This disaster was caused by a hacker. A disgruntled former employee of the company that installed the system had taken over the network using radio and computer equipment.

More recently, the computer worm Stuxnet was discovered in 2010. The worm, which attacks programmable logic controllers used to control machinery, was thought to be introduced via an infected flash drive before spreading throughout a network. Although it caused much of its damage to Iranian nuclear centrifuges, its success in taking down highly secure systems shows how networked mechanical systems can be just as vulnerable to cyberattacks as computer systems.

In addition to the Maroochy Shire incident and the Stuxnet worm, there have been worm infestations at Daimler-Chrysler's manufacturing plants (resulting in a temporary assembly line shutdown) and at a First Energy nuclear power plant. National Geographic even released a docudrama in 2013 called "American Blackout" that depicted what might happen if a large-scale SCADA attack took down the United States' electrical grid.

CRITICAL STEPS TO PROTECTION

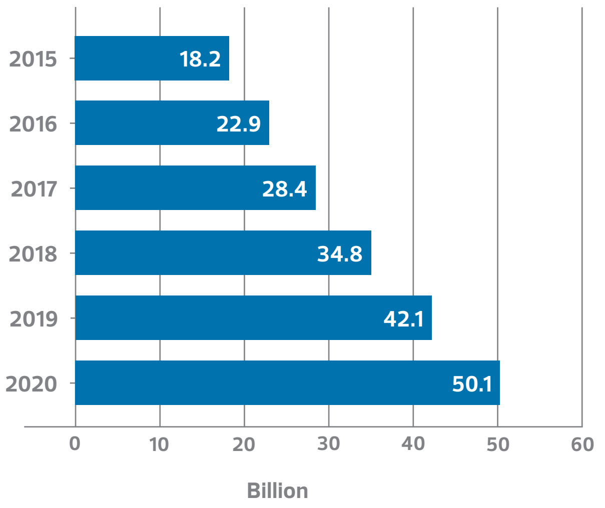
Companies looking to improve the security of their SCADA networks can turn to guidance from the federal Energy Department and the President's Critical Infrastructure Protection Board. A report from these agencies lays out numerous actions that companies take to protect their networks. Here are some key steps:

- **Identify all connections to SCADA networks:** IT staff should conduct a risk analysis of each asset that connects to a SCADA network. This should help security staff to understand how assets are connected to the SCADA network and how they are protected.
- **Disconnect unnecessary connections to the SCADA network:** The SCADA network should be isolated from other network devices as much as possible. Each connection introduces greater security risk, so minimizing these connections reduces risks. The use of demilitarized zones and data warehousing can help to secure data as it moves from SCADA networks to business networks.
- **Implement native device security features:** Many newer SCADA devices are equipped with security features, which are often disabled to simplify installation of the device on the network. IT staff should identity the security features available and adjust settings to provide the maximum level of security.

In order to protect their networks from cyberattacks, energy companies should plan for and employ a variety of measures:

- **Perimeter security:** Effective perimeter firewalls include a secure zone for control system network elements, a demilitarized zone (DMZ) and an insecure zone. Continuous monitoring and proper protection of authentication devices, workstations and servers in the DMZ reduce the chances of an attack through the corporate network.
- **Identity management:** The largest internal threat to SCADA security comes not from disgruntled employees, but from workers who unwittingly connect to the network with a compromised device. If a worker's device has picked up a worm, for example, that worm may start scanning the network and cause outages. The proliferation of wireless access points increases the probability of such a scenario. To protect their networks, enterprises must ensure that every user and device to access the network is authenticated.
- **Device/endpoint security:** To prevent employees from accidentally introducing security threats to the enterprise, companies must also ensure that all computers, notebooks,

PROJECTED NUMBER OF OBJECTS CONNECTED THROUGH THE INTERNET OF THINGS:



SOURCE: Cisco Systems, "Connections Counter: The Internet of Everything in Motion," 2013

smartphones, tablets and specialized equipment accessing the network comply with security standards.

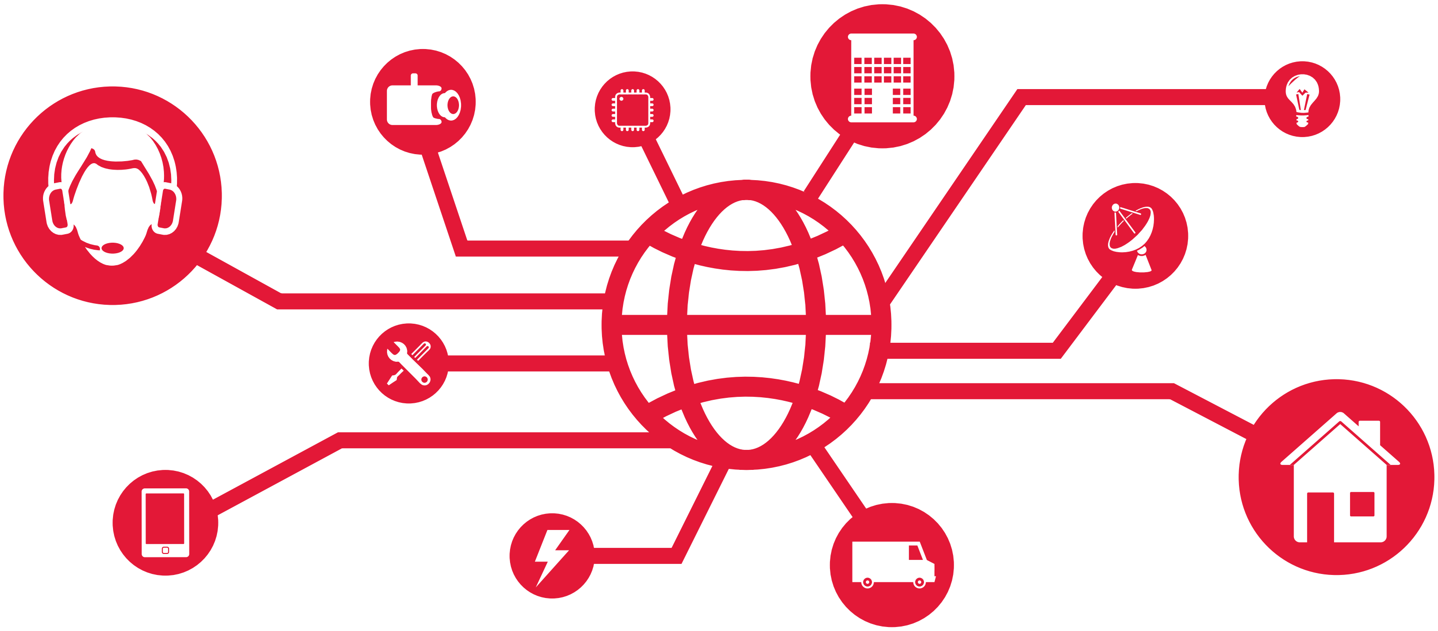
- **Remote access security:** Companies may need to grant employees or external vendors remote access to a SCADA network for any number of reasons, including data collection, equipment monitoring, and diagnosing and fixing problems. This remote access must be secure to prevent users from accidentally or maliciously launching an attack. Remote access security measures include limiting users to the functions for which they are authorized, as well as denying network access to any external device that lacks proper security or is infected with spyware.
- **Monitoring:** Security measures such as firewalls and intrusion prevention systems do not merely ward off attacks. They also act as monitoring stations that can inform IT security staff if there has been a violation of the network access policy. Enterprises can also use information about network use and applications to establish baselines for expected communications. Any substantial deviation from the norm can then trigger an automatic alarm. Automated IT tools can notify network administrators of any new services being deployed or changes in existing services, as well as any attempt to connect to hostile hosts or networks.

SCADA and the Internet of Things

SCADA networks have been around for decades, although newer terms such as "machine to machine" (M2M) and the Internet of Things seem to have taken over as alternative ways to describe network-connected physical objects. These terms all refer to collecting data from non-IT resources, but they are commonly used in different ways.

SCADA applies almost exclusively to networks used by operations and field service departments in the oil, gas and utility industries. SCADA equipment is often connected only inside the enterprise, separate from the Internet (SCADA networks initially relied on analog connections). While nearly identical, M2M more commonly refers to networked machines across a variety of industries and includes other systems, such as enterprise resource planning and customer relationship management. IoT refers to interconnected objects, devices, applications and services.

The development of IoT technology offers opportunities for greater connectivity and broader application of SCADA networks. Energy



companies and utilities expect to benefit from this connectivity. According to a Cisco Systems survey, 91 percent of businesses in the oil and gas industry expect their investment in IoT to increase somewhat or significantly over the next three years. Similarly, 89 percent of utility companies expect their IoT investments to grow.

The growth of IoT technology means that more devices are able to collect and share data. By integrating this technology into SCADA networks, companies can more easily monitor and adjust equipment remotely, predict and prevent failures, provide better customer service, and even refine designs and processes. A good example of IoT technology in the energy industry is the smart grid used by utilities to remotely track and adapt for electricity use. Within oil and gas, IoT technology is contributing to everything from well optimization to supply chain traceability.

As the IoT continues to evolve, it will likely support increasingly complex applications that enable collaboration between devices, people and systems. A trusted network solutions partner can help companies to securely build this technology into ruggedized networks and optimize its use.

CDW: A Networking Partner That Gets IT

For more than 25 years, CDW has partnered with companies in oil, gas, utilities and renewable energy to optimize their IT infrastructures. Through solutions such as ruggedized networking, high-performance computing, remote infrastructure and mobile workforce tools, CDW has helped these organizations to grow, become more efficient and meet regulatory compliance guidelines.

CDW understands the unique needs of energy companies and knows that continuous operations depend on optimal IT performance around the clock. The security experts and solution architects at CDW begin by reviewing organizations' current operations and assessing outstanding needs. Next, they develop comprehensive plans to help organizations meet those needs. Finally, they continue with implementing solutions. This ongoing teamwork ensures that customers will meet their desired business outcomes without unanswered questions.

At every stage, CDW solution architects can help with a ruggedized network implementation:

- **Planning and design:** CDW experts consult and collaborate with customers' IT staff to evaluate the legacy infrastructure and help ensure that it can scale with technology requirements.
- **Configuration:** CDW customizes customers' technology solutions to their precise specifications in its Configuration Centers.
- **Installation and deployment:** CDW installation services, including an onsite CDW engineer, ensure that customers' new technology is up and running as fast as possible and working properly.
- **Product lifecycle support:** CDW can offer extra support through onsite staffing and training. We can also help protect the lifespan of new technology through maintenance agreements.

To learn more about how CDW can deliver IT solutions optimized for the energy and utility industries, contact your CDW account manager, call 877.645.0685 or visit CDW.com/energy.

CISCO Gold Partner

The Cisco® Industrial Ethernet 3000 Series (IE 3000 Series) is a family of Layer 2 and Layer 3 switches that bring Cisco's advancements in switching to Industrial Ethernet applications with innovative features, robust security and ease of use. The Cisco IE 3000 Series features industrial design and compliance; tools for easy deployment, management and replacement; network security based on open standards; and integration of IT and industrial automation networks.

CDW.com/cisco

SHARE THIS WHITE PAPER

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark 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

CDW® PEOPLE WHO GET IT™