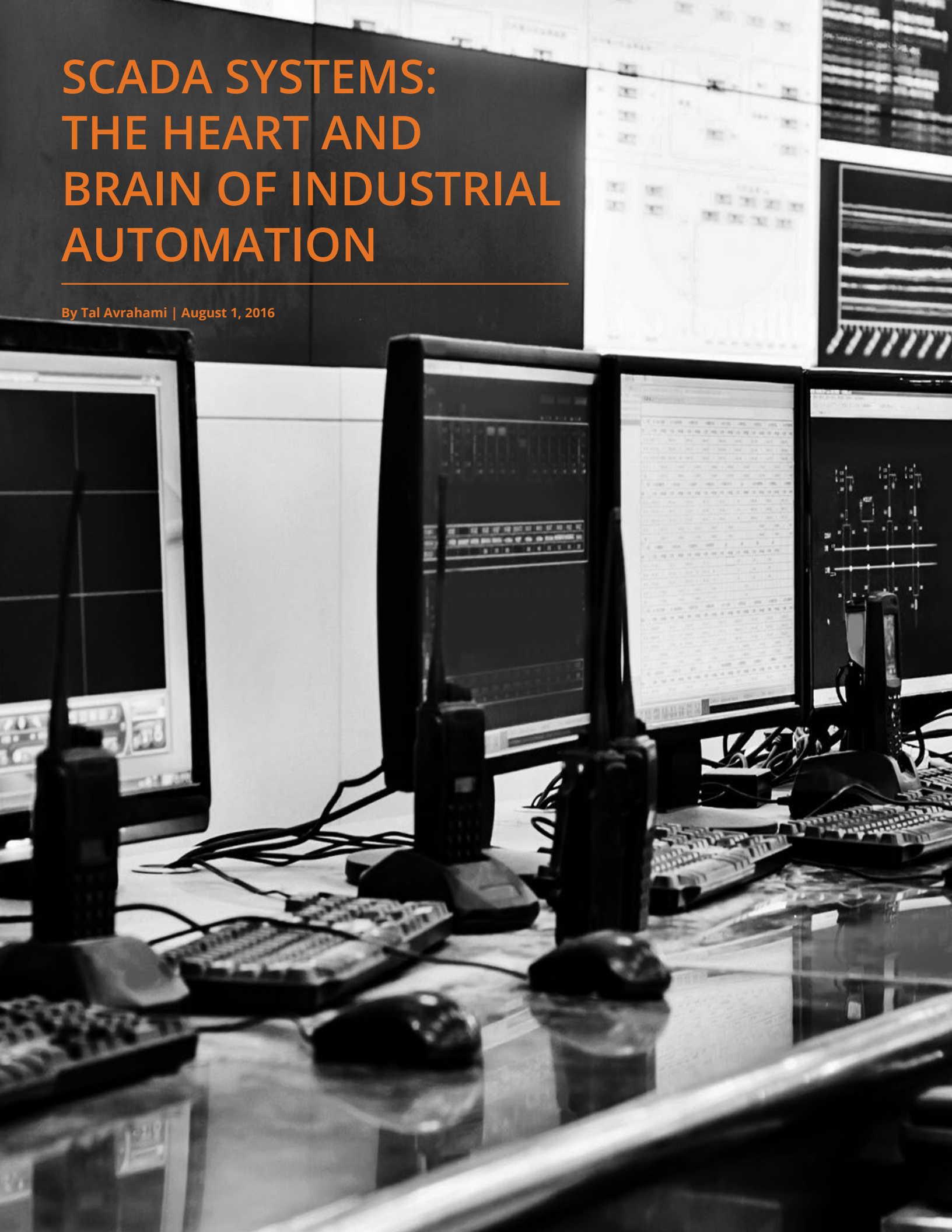
SCADA SYSTEMS: THE HEART AND BRAIN OF INDUSTRIAL AUTOMATION

By Tal Avrahami | August 1, 2016



INTRODUCTION

Digitalization of information and increasingly pervasive internet connectivity have changed many facets of everyday life. One of the most promising and discussed areas of current and future innovation is what technologists and analysts now often refer to as the Internet of Things (IoT), the Internet of Everything (IoE), and in the industrial sector as the Industrial Internet of Things (IIoT). Traditionally, this sphere of technology has been dubbed machine-to-machine (M2M) communications.

> ***Some of the chief objectives in connecting devices to the internet and making them communicate with one another include: increased process efficiency and resource productivity; improved management of infrastructure and the environment; and enhanced quality of life.***

In the industrial sector, especially where assets are dispersed and situated in remote locations, supervisory control and data acquisition (SCADA) systems are the heart and brain that manage data collection, perform data fusion and analytics, and automate industrial processes. These so-called outside-of-the-fence applications have leveraged SCADA technologies that were initially developed and thus optimized for inside-of-the-fence applications, where machinery and infrastructure are co-located or within short reach of a field office or central command center. By adopting SCADA technology for manufacturing plants without sufficiently adapting it to the characteristics of sprawling physical infrastructure, operators face a variety of challenges that we will elaborate further.

We will cover four main topics. First, we will review the technologies that comprise SCADA systems. Second, we will discuss the value of industrial automation. Third, we will address the key technological and economic challenges associated with SCADA systems in outside-of-the-fence applications. Finally, we will discuss the crucial significance of securing SCADA systems.

SCADA SYSTEM 101

SCADA systems are a type of industrial control system (ICS) used for data acquisition and automation in production and critical infrastructure applications. They are classified as operations technology (OT), which is distinguished from the catch-all term information technology (IT) used to describe all forms of hardware, software, and communication technology used for creating, storing, exchanging, and utilizing information. Typical applications for SCADA systems include: manufacturing plants, oil & gas refineries, power plants, and water and wastewater treatment plants.

SCADA systems consist of a complex architecture of hardware, software, and connectivity. This architecture is organized into four layers: 1) field instrumentation; 2) programmable logic controllers (PLCs) and remote telemetry units (RTUs); 3) communications; and 4) the SCADA host platform.

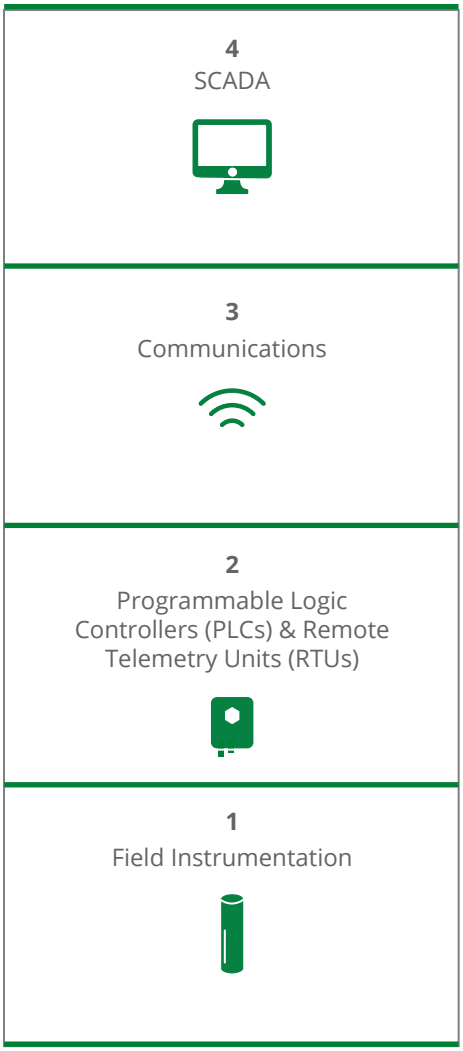


Image 1: Four layers of SCADA system architecture.

Field Instrumentation

The first layer consists of hardware collectively referred to as field instrumentation. Examples of this instrumentation include: sensors, samplers, relays, and actuators. For example, a temperature or pH sensor inserted into a drinking water pipe measures fluctuations over time, which can reflect changes in water quality. Piezo vibration sensors can measure physical stress of pumps and generators. An actuator powered by an electric source can convert that electric energy into mechanical energy to close a valve, for example. From the perspective of monitoring and automation, field instrumentation generates data, requires data, or both creates and consumes data.

PLCs and RTUs

The second layer consists of PLCs and RTUs (note: remote telemetry unit and remote terminal unit are used interchangeably to refer to the same class of devices). PLCs and RTUs are connected to field instrumentation and perform real-time or continuous data collection, relay data to the SCADA host platform, and perform varying levels of control.

As the name suggests, PLCs are designed and engineered for industrial control and automation based on programmable processing of measurements. These digital computers are hard-wired for real- or near-real-time processing and response at the installation point to ensure proper operations and avoid potentially disastrous mishaps. Typically, PLCs support numerous analog and digital inputs (e.g. sensors) and outputs (e.g. relays and actuators for pump, valve, and hydraulic cylinder operational control). PLCs and the microprocessors that power their computing capabilities are ruggedized to withstand harsh conditions, including dust, humidity, vibration, heat, and cold. Moreover, PLCs use more stable operating systems suitable for deterministic logic execution. The current generation of PLCs are programmed using a software on a desktop PC, and an ethernet, RS-232, RS-485, or RS-422 cable enables uploading of

the program to the PLC. The PLC program is editable using desktop PC software, but requires physical connection between the device and a desktop PC or a removable chip containing the PLC software.

RTUs were once relatively crude telemetry devices that logged data from field instrumentation and relayed it over fixed or wireless communication networks to the SCADA host platform. RTUs relative to PLCs are generally more environmentally compliant. The former were designed with the intention of operating in the field with exposure to variable elements, while the latter were designed for installation on factory floors, where conditions are largely stable.

Traditionally, RTUs lacked the processing and control capabilities of PLCs, but had more sophisticated communication capabilities than PLCs. Without doubt, legacy RTUs are still deployed in the field with an installed base measurable in the hundreds of thousands. Furthermore, a large share of this installed base utilizes legacy technology with limited communication capabilities by today's standards. More specifically, they provide unreliable and plain (i.e. non-encrypted) connectivity over a single communication network and protocol.

However, in the past few decades, the once highly differentiated technologies of PLCs and RTUs have blurred. Manufacturers of PLCs and RTUs alike have responded to evolving customer demands for improved communications capabilities from PLCs and more robust processing and control capabilities from RTUs. While PLCs and RTUs are increasingly analogous, there is still a meaningful divide on the control capabilities that is reflected in the higher cost of PLCs.

Communications

Through the third SCADA system layer – communications – PLCs and RTUs connect field instrumentation to the SCADA host platform. SCADA systems establish connectivity through wired or wireless (radio, satellite) networks using a variety of communication protocols.

Over the past few decades, the typical communication channel for SCADA systems has been wired over fiber optic cable. SCADA systems were first developed for inside-of-the-fence applications such as factory floors, where power supply is readily available on-site and field instrumentation and the SCADA host platform are co-located or within close proximity.

The most popular and widely-deployed computer networking technology is Ethernet, a link layer protocol. Historically, Ethernet has supported network footprints constrained to a radius of several hundred meters, as devices were connected exclusively by cable. Advances in technology have extended the feasible range of Ethernet-based LAN networks to several miles using wireless communications as a partial or total replacement for fibers and copper wire. But infrastructure and logistical feasibility as well as cyber-security issues remain a challenge for deploying Ethernet-based local area networks outside the confines of a building or industrial complex.

The most popular means for achieving SCADA system communications for inside-of-the-fence applications is Ethernet technology on a LAN. At a pharmaceutical manufacturing plant, for example, a PLC used to monitor and automate processes such as milling or coating can mean the difference between a safe, market-ready batch and one that is unsafe and must be disposed. In pharmaceutical manufacturing, as in other industrial segments, there is effectively zero margin for error. Real-time monitoring and control are tantamount to achieving quality control, avoiding accidents, reducing downtime, and maximizing throughput.

Dozens, if not hundreds, of PLCs on a pharmaceutical plant floor or drinking water treatment plant can be tied into the SCADA host platform with relative technological ease using Ethernet cables. LAN architecture over Ethernet allows for virtually instantaneous bi-directional communication between the PLC and SCADA host platform. While automation of manufacturing workflows and processes does not guarantee zero defect, it does represent a step change from manual processes.

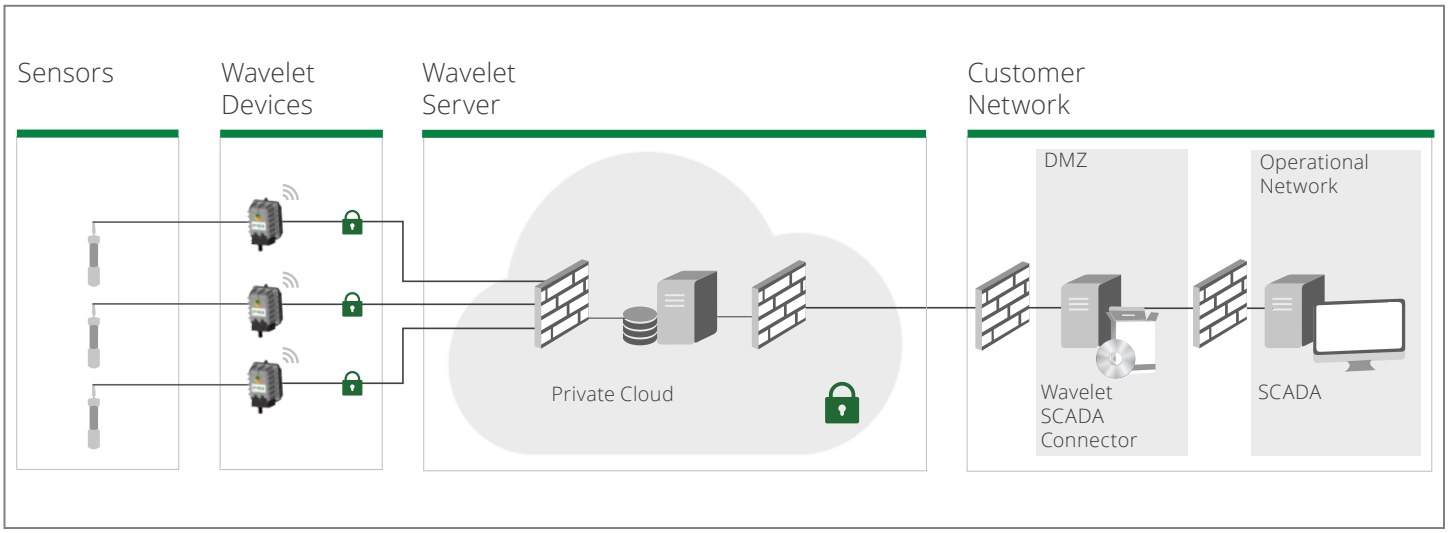


Image 2: One of various options of smart network architecture, connecting field-deployed devices through a private cloud and onto the customer SCADA.

Increasingly, SCADA systems have now been widely adopted as a solution for monitoring and industrial automation for outside-of-the-fence applications. The most common such operators include water, wastewater, electric power, and natural gas utilities.

As the number of SCADA system developers and integrators has grown, vendors competing over lucrative procurement contracts have sought sources of of differentiation. This has resulted in market fragmentation. One area of SCADA technology where this fragmentation reveals itself is the variety of communication protocols, which act as the glue connecting PLCs and RTUs on the one hand with the SCADA host platform on the other.

Proprietary communication protocols have proved an effective competitive advantage for certain vendors. This splintering tends to complicate matters for operators, who face longer and costlier integration efforts. System integrators tend to benefit from this dynamic, as specialized know-how and lengthier, more convoluted projects can be wildly profitable.

> ***Slowly but steadily, however, industry is moving away from old and proprietary protocols to ones which are open.***

OLE (object linking and embedding) for Process Control (OPC) and Distributed Network Protocol (DNP3) were developed by industry consortiums and first released in 1996[1] and 1993[2], respectively.

OPC establishes a standard set of objects, interfaces, and methods that govern communication of the SCADA host platforms with PLCs and RTUs. The legacy OPC protocol is based on OLE (object linking and embedding), COM (component object model), and DCOM (distributed component object model) technologies developed for Microsoft Windows.

OPC is segmented into separate specifications, including OPC Data Access (OPC DA) and OPC Historical Data Access (HDA). OPC DA is the generic form of OPC, and is referred to as Classic OPC Specifications. The OPC DA protocol is used for real-time data only. Put another way, it does not support historical data logged and time-stamped by RTUs from remote locations, where real-time communications is not feasible. By contrast, OPC HDA does support communication of archived data from devices such as RTUs.

There are a variety of limitations to to Classic OPC Specifications. Implementation is limited to platforms running Microsoft Windows only. Scalability is challenging as the number of smart sensors deployed in the field grows. Cyber-security capabilities are inadequate. Configuration issues with DCOM are frequent and burdensome.

The successor to Classic OPC Specifications is OPC Unified Architecture (OPC UA), which is functionally equivalent to the legacy technology, but includes meaningful improvements. In particular, OPC UA is platform-independent for both hardware (traditional PC hardware, cloud-based servers, etc) and operating systems (Microsoft Windows, Applex OSX, Android, etc). Buffering allows for data to be re-fetched in the event of temporary loss of connectivity. Cyber-security capabilities are more robust. The multi-layered architecture is extensible to support future development. Extremely complex data is turned into intelligible information due to complete object-oriented capabilities.

Distributed Network Protocol (DNP3), like OPC, was developed to achieve open, standards-based interoperability between various SCADA systems vendors' components. Originally designed with the needs of electric utilities in mind, DNP3 enables more reliable communications in challenging conditions, including where distortion can be created by electromagnetic interference. In addition to electric power utilities, the DNP3 communication protocol has been adopted by water and wastewater utilities, oil & gas operators, as well as by the transportation industry.

DNP3 uses the term "outstation" to refer to remote PLCs, RTUs, and equipment deployed in the field, while "master" refers to computers at the command center. DNP3 sets rules that govern the communication of data from outstation to master computers on the one hand, and control commands issued by master and executed by outstation computers on the other.

The DNP3 protocol was designed with reliability in mind, but did not have cyber-secure technology built into its foundations. Smart grid technology that has come to market since the inception of the DNP3 protocol in 1993 relies on third-party access to the physical networks and underlying internet protocol infrastructure of the grid. As a result, significant effort has been invested in adding secure authentication functionality to the DNP3 protocol.

Communication for SCADA systems used to monitor and control dispersed assets presents operators with challenges we will elaborate below in the section titled "Moving Inside-Out." Advances to the cyber-security standards of OPC UA and DNP3 do not guarantee fail-safe, hermetically sealed SCADA systems. We will review this in greater detail in the section below titled "Securing SCADA Systems."

Image 3: Data loggers are typically application-specific and lack any cyber-security.

SCADA Host Platform

On the software and information technology side, SCADA host platforms include: software drivers; a SCADA engine; one or multiple databases; and a human machine interface (HMI). The host platform represents the nerve center of the SCADA system architecture.

SCADA host platforms operate as follows: data streams generated by field instrumentation flow in via PLCs and RTUs over the communication layer; communication drivers that integrate data with the engine; the engine stores and runs queries from a database architecture, provides graphical displays of field instrumentation and physical processes, visualizes data and trends, and alarms. The final aspect of the SCADA host platform is the HMI, which is the means by which SCADA engineers, operators, technicians, and other decision makers manage the entire SCADA system architecture and control strategy.

The SCADA host platform drives the lion's share of value-add, which is derived from its feedback mechanisms. As a data fusion and analytics platform, the SCADA engine is responsible for integrating data from the field and subsequently delivering commands to PLCs, RTUs, and field instrumentation to automate and improve machinery and infrastructure management.

THE UPSIDE OF INDUSTRIAL AUTOMATION

SCADA systems have for several decades been the enabling tool set of industrial automation in manufacturing plants, oil refineries, and other environments where the SCADA host platform is co-located with the physical machinery and processes that it monitors and controls. Operators in these segments often do have assets outside of the confines of central facilities and complexes. But those remote assets generally are not integrated into a SCADA system, as the outsized share of value is enclosed within one location.

A different model and approach applies to electric power, natural gas, water, and wastewater utilities, oil & gas producers, and other industrial players that operate and deliver their products and services across large geographic areas and in remote locations. In virtually all cases, operators in these segments also manage centralized industrial facilities and assets. For example, a power plant "manufactures" energy by converting a feedstock (e.g. natural gas, coal, nuclear fuel) into a finished "product" (electricity).[†] Similarly, a centralized water and wastewater treatment plants are manufacturing facilities inasmuch as they are used to "manufacture" clean drinking water and dischargeable or reusable effluent. The SCADA host platform is frequently co-located with these central facilities. The same SCADA system often monitors and controls central locations and remote assets (e.g. pumps, valves, generators). But the outsized share of assets and value often lies outside a central complex.

> ***For both inside- and outside-of-the-fence applications, SCADA systems allow operators to: increase throughput; mitigate safety risks; reduce down time (RDT); and extract insights for long-term value creation and asset optimization, including predictive maintenance.***

Moreover, SCADA systems offer reliability and effectiveness currently unmatched by competing solutions for industrial control.

MOVING INSIDE-OUT

Operators utilizing SCADA systems to monitor and control sprawling network of assets, especially in truly remote and harsh locations, confront significant challenges that operators in inside-of-the-fence applications need not concern themselves. Nevertheless, there are significant benefits to bringing the capabilities of SCADA systems to remote locations. More specifically, operators with assets and resources in remote locations have zero visibility on a near-real-time or even consistent basis without continuous monitoring solutions. The

Image 4: "Outside-of-the-fence" remote monitoring supports improved management, but presents various challenges.

historic approach to remote monitoring is deploying personnel to the field to take measurements with handheld devices and take grab samples for laboratory testing. There is no way to scale these types of measurements cost-effectively across a large geographic area. More importantly, the outcome of deployment to each location is one or a handful of data points. Such data represents a single snapshot in time that has limited value for trend analysis and zero value for industrial automation.

SCADA systems offer robust and reliable capabilities for continuous and near-real-time monitoring and automation in remote locations. With SCADA systems, operators are able to work proactively to manage their networks rather than respond reactively after an issue has already presented itself.

The number of potential failure points across a sprawling network increases exponentially relative to the size and complexity of assets. Network operators must think strategically and perform cost-benefit analysis when deploying SCADA systems. Excluding operators with virtually unlimited budgets, the cost of hardware, integration expenses, telecommunications, maintenance, after-market parts, and other items limits the scope and scale of implementation of field instrumentation, PLCs, and RTUs.

Power and communications are both significant and interconnected limiting factors. When implemented in a manufacturing plant, all components of a SCADA system have access to a fixed, and thus reliable, power supply. By contrast, a PLC or RTU deployed in a remote location cannot easily be wired to a fixed source of power. In such cases, these systems depend on batteries, which must be replaced once depleted over time. Solar panels can offer redundant supply, but they require maintenance, as they become less efficient and effective when covered with debris or dust. Moreover, they are subject to vandalism and theft, especially when installed at street level in an urban environment.

Additionally, certain sensors are energy-intensive. More frequent wireless data transmission places significant demands on the battery powering a wireless modem of an RTU or PLC. Addressing these technological limitations requires higher energy-density or larger batteries, more frequent battery replacements, or communications networks with lower energy requirements. Better and bigger batteries and more frequent maintenance come at additional cost.

Low-power wide area networks (LPWAN) such as those developed by Sigfox and the LoRa Alliance show great promise.[3] But network coverage is still limited at this stage, and tight bandwidth limitations dictate the type, amount, and transmission frequency of data over these networks. 2G, 3G, CDMA, and LTE cellular as well as satellite networks, though not quite as parsimonious with bandwidth as LPWAN networks, are too power-intensive to enable fully-autonomous operations for longer durations with frequent data transmission. Future cellular networks (4G and 5G) will offer significantly more power-efficient communications when rolled out in the coming years, including LTE CAT-0, CAT-M, and NarrowBand IoT (NB-IoT), but it remains to be seen which communication technology will dominate the market.

Image 5: "Inside-of-the fence" remote monitoring enables real-time automation without power and communication constraints.

An inside-of-the-fence operator has visibility and autonomy when a LAN fails. As the administrator and owner of the IT/OT network, a plant operator can work swiftly to resolve issues. The same cannot be said for outside-of-the-fence operators relying on third-party wireless networks. When connectivity on cellular and satellite networks fails temporarily, a not so rare phenomenon, a SCADA system operator has no recourse over problem resolution on a third-party IT network. In a similar vein, the response time is longer and costs higher when troubleshooting issues with field instrumentation, RTUs, and PLCs.

SCADA system operators typically face additional complexity when selecting communication network providers. Network carriers may have strong coverage in most areas, but limited in others. Procuring SIM cards and data plans from multiple carriers to ensure reliable connectivity and verifying which carriers offer stronger network strength at each remote installation location is a messy and costly undertaking. In addition, network strength can vary considerably based on unpredictable conditions.

In short, the challenges of deploying, integrating, and maintaining SCADA systems for outside-of-the-fence applications drives faster growth in total cost of ownership relative to that of inside-of-the-fence applications.

Yet another area where managing SCADA systems for outside-of-the-fence applications is more challenging than for inside-of-the-fence applications is security.

SECURING SCADA SYSTEMS

Not until long ago, cyber-security was an afterthought in the industrial automation sector. SCADA systems were originally implemented on local networks. Securing communications over public networks did not enter the calculus of SCADA system technology developers. As a result, communications from remote assets via RTUs and PLCs was a problem from a cyber-security perspective from day one of its implementation. Legacy technologies that are still deployed in the field simply do not protect against the real and potentially very significant damage that can be carried by malevolent actors via cyber infiltration. Indeed, cyber attacks are becoming more prevalent and sophisticated, and many operators are woefully exposed and underprepared.

Today, SCADA system cyber-security has become a hot topic, and talented chief information security officers are in high demand. The large and growing number of technology companies in this niche raises questions about a possible market bubble.

> ***But when one considers the value at stake – trillions of dollars in infrastructure and assets as well as public and ecosystem health – it boggles the mind that strong IT/OT network security was not top priority from technology development for both inside- and outside-of-the-fence applications.***

There have been plenty of documented attacks on SCADA systems over the years, and many more that were not reported or have remained unnoticed. Perhaps no cyber attack is more infamous than Stuxnet, which was carried out on Iran's nuclear facilities. Revelations of Stuxnet in late-2010 finally gave industrial cyber-security the attention the topic deserves.[4]

Stuxnet, an advanced persistent threat that avoids detection, was introduced via Microsoft Windows on an infected USB flash drive. Subsequently, the worm propagated across the network, targeted the PLC software running on networked computers controlling PLCs. Stuxnet modified the PLC software to give unexpected commands to the PLCs and give false feedback of normal system operations to the user. The infected PLCs controlled centrifuges rotating at high speeds used for enriching uranium. Stuxnet caused fluctuations in the speed of rotation and the centrifuges, leading to useless product. This attack is credited with setting back Iran's nuclear development program.

Securing SCADA systems requires protection of both physical and cyber layers. Physical access can pose risk to the infrastructure and SCADA system. A trespasser at a remote location can steal or tamper with field instrumentation, PLCs, and RTUs, which can lead to disruption of normal operations and potential damage. This has led to the development and deployment of video surveillance and intrusion prevention and detection systems. But physical access at one point or even many points of the SCADA system poses less significant risk than access at the SCADA host platform. Poorly-engineered PLCs and RTUs can serve as a backdoor entry-point to the SCADA host platform. Indeed, these represent attack surfaces that have the potential to do harm across the entire network of infrastructure and assets. But the more typical means by which nefarious actors wreak havoc on SCADA systems, which can be achieved from thousands of miles away from any physical access points, is via the SCADA host platform and computers used to access the SCADA host platform.

It behooves operators to make securing their SCADA systems a top priority and an important part of their capital improvement budgets. Retiring legacy technologies that expose their SCADA systems to cyber attacks and implementing solutions that defend against them are expensive and time-intensive undertakings. But keeping outmoded, non-secured technologies in the field and continuing to deploy them all but ensures disruption to critical infrastructure. Forward-thinking operators have and will continue to mitigate and get ahead of these problems before they come to fruition.

CONCLUSION

Our aim was to provide a primer on SCADA systems that would be both accessible to all readers and contain enough detailed explanations to provide even the most technically-savvy readers with fresh insights. We gave an overview of the technologies and components that comprise a SCADA system. We then took a look at why SCADA systems are valuable for automation and monitoring of local and remote assets. Next, we examined the main challenges operators face when applying technology intended for monitoring and automation of local assets in remote locations, particularly power and communications. Finally, we emphasized the importance of securing SCADA systems.

Over the past few decades, SCADA system technology has been widely adopted by operators for applications spanning numerous market segments and cutting across entire value chains. SCADA systems play a critical role in monitoring trillions of dollars in resources and assets and automatic processes that deliver tremendous economic value to the global economy. It appears that SCADA system technology is here to stay for the foreseeable future. In a world where operational complexity is increasing, opportunities to extract value from remote monitoring and automation are growing, and cyber attacks are becoming more prevalent and sophisticated, step-change innovation in SCADA system technology is vital.

References

1. OPC Foundation. "What is OPC." OPC Foundation – The Interoperability Standard for Industrial Automation. Web. 06 Jul. 2016
2. DNP Users Group. "Overview of the DNP3 Protocol." Distributed Network Protocol. Web. 06 Jul. 2016.
3. Hunn, Nick. "LoRa vs LTE-M vs Sigfox." Creative Connectivity. Web. 06 Jul. 2016.
4. Fleming, Ryan. "BITS BEFORE BOMBS: HOW STUXNET CRIPPLED IRAN'S NUCLEAR DREAMS." Digital Trends. Web. 06 Jul. 2016.

