JUSTIN POLLOCK, Senior Antenna Engineer,
KP Performance Antennas, https://www.kpperformance.com

SCADA: Alive and Well in the Age of IoT

Despite the onslaught of the Internet of Things within the industrial world, SCADA will continue to evolve to meet today's demands.

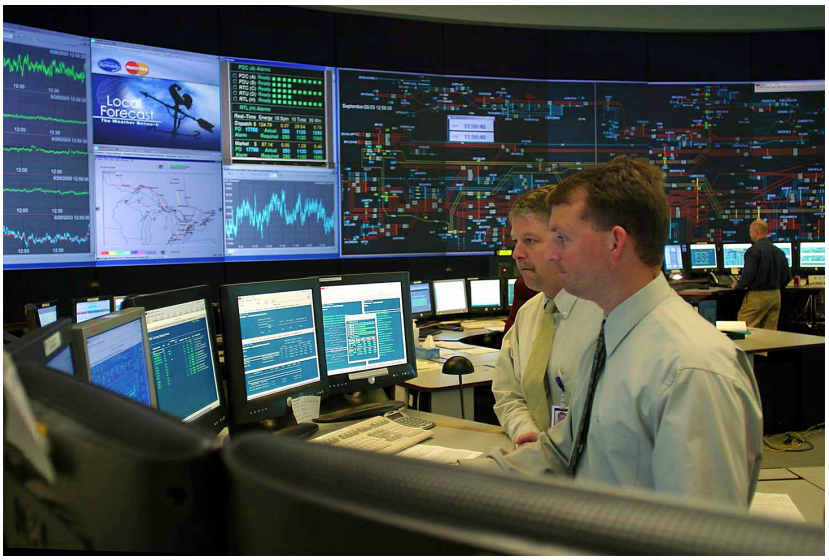
When most people think of the Internet of Things (IoT), home automation is what comes to mind. But in terms of complexity, home automation is a simple network compared with applications in "smart" cities, huge manufacturing facilities, and eventually connecting everything necessary to enable vehicle autonomy.

However, IoT may have some of its greatest impact on the utilities market and others considered mission-critical. They have been using supervisory control and data acquisition (SCADA) systems for decades to monitor and control far-flung assets of industrial, government, energy, and other industries. IoT and SCADA are different in many ways, but the former is so all-encompassing it's certain to influence SCADA. The question now is how.

For those not familiar with SCADA, it's a supervisory system designed to monitor and control critical equipment usually dispersed over a large area. It's a crucial technology for ensuring reliable operation of systems ranging from water and waste control to energy distribution, oil and gas refining, transportation, fossil-fuel and nuclear power plants, and many others. Without SCADA, these systems would function "in the dark" with no feedback concerning the status of their hundreds to tens of thousands of sensitive areas.

SCADA systems offer two basic functions: remote control of equipment such as power switches and breakers, including load control/load shedding, valves and actuators, and telemetry to report their current status to a central point. They also allow for remote measurement and reporting of more detailed data sensors connected to these and other devices.

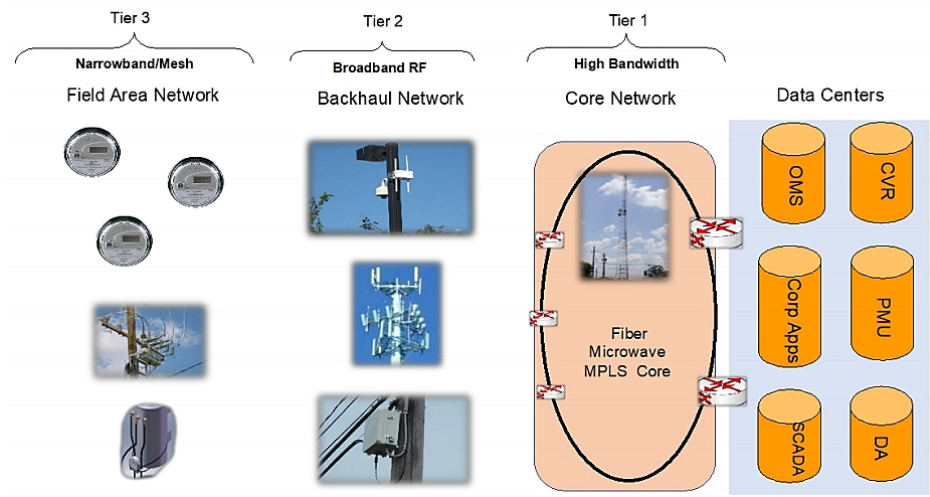
The concept was conceived at least as far back as the 1930s to provide supervisory control of electric utilities and has been updated periodically over the years to increase performance and reduce human intervention. A system consists of hardware, software, wired and wireless communications, and programmable logic controllers (PLCs) and remote terminal units (RTUs) to which are connected various types of sensors. Atop all of this hardware sits SCADA's supervisory capabilities.



1. The control center of a large organization gets its raw data from sensors in the SCADA system. (Source: All About Circuits)

The data from the sensors or RTUs can be transmitted via any means available, from telephone lines to Ethernet, satellite, or wireless sensor networks (WSNs), depending on what's available and cost-effective. A variety of wired protocols continue to be used, some dating back to the earliest SCADA deployments, although the trend is toward open-source protocols to eliminate dependence on proprietary solutions.

The information from the sensors is sent to a control center where all points



2. The three tiers of a utility telecommunications architecture consist of a field area network, backhaul, and the high-throughput network core. (Source: Utilities Technology Council; prepared by Red Rose Telecom)

in the system are displayed. In a large industrial facility or utility network control center (*Fig. 1*) is a wall of monitors with a striking resemblance to NASA Mission Control. A SCADA system also has a "historian" feature, a database of time-stamped data about alarms, measurements, and other types of information that can be used for statistical analysis.

SCADA and IIoT

With the emergence of the industrial IoT (IIoT), there are differing opinions about what will become of SCADA, ranging from SCADA complementing IoT, to SCADA gradually disappearing within IIoT. However, the smart money is on SCADA not just surviving, but expanding its supervisory role by adding some of the features employed by IoT. This includes edge- and cloud-based processing and analytics that enable automated preventative and ultimately prescriptive maintenance, thus lessening reliance on human intervention.

SCADA won't disappear any time soon for the simple reason that deployed SCADA systems dwarf IIoT deployments today. And this will be the case for years, because they are an essential ingredient in mission-critical systems that have been deployed and modified multiple times over decades. These systems include nuclear reactors, defense operations, the power grid, the entire fossil-fuel industry, and many more. Wholesale replacement of these systems with pure IIoT solutions would also be prohibitively expensive and immensely disruptive, potentially leaving some assets unprotected from cyberattack during the transition.

So, it shouldn't be surprising that SCADA represents a substantial portion of the global market for industrial control systems, which is projected to be nearly $200 billion by 2024. In short, while IIoT will continue to permeate more industry sectors, SCADA will continue to provide its traditional functions of alarming, data logging, real-time control, and database management—only better.

New Waves in Wireless SCADA

Traditionally, wireless SCADA used a self-provided network specifically designed to minimize single points of failure that alone could take an entire system down. To achieve this, many advances have been made to enhance this resilience by providing redundant signal paths, mesh-type network topologies, and various wireless systems and technologies.

Utilities and other mission-critical industries long ago decided that the only way to ensure "five nines" reliability was to build their own wired and private wireless networks. It was believed that commercial networks were not reliable enough and because much utility infrastructure is located in places not served by commercial carriers. As a result, utilities today own at least 80% of their own communications networks and use commercial systems sparingly. The networks originally served only voice communications, but when SCADA began its deployment, data was added to the mix and today consists of much of the traffic.

That said, other industries not designated as mission-critical use nearly all common standards and protocols, from unlicensed industrial, scientific and medical (ISM) bands at 902 to 928 MHz, 2.4 GHz and 5.7 GHz, WiMAX, TETRA, second- and third-generation cellular access methods, digital mobile radio (DMR), and private land-mobile radio systems. Satellite-based systems are also in widespread use, especially by industries whose assets are geographically diverse, a good example of which is the distribution of oil and gas and offshore drilling.

Point-to-point and point-to-multipoint RF and microwave links have been a mainstay of SCADA for many years, making it possible to connect widespread assets while also delivering high data rates and high reliability. The power grid illustrates where microwave links and other wireless technologies play a role in a complex, geographically massive network, which can be divided into three tiers *(Fig. 2)*. Tier 1, the network back-

bone, is served by fiber-optic and point-to-point microwave links in a ring topology so that any site can communicate to the central site via two completely different paths. Most utilities used licensed frequencies around 6 GHz for this purpose.

As always, fiber is the preferred transmission medium, but it's very expensive and often nearly impossible to deploy, especially in remote areas. As a result, microwave links account for at least half the backbone infrastructure. They can deliver very-high-speed connectivity over many hops throughout a wide geographical area. Up to four radios are typically installed on a tower. The protocol in both cases is typically Carrier Ethernet, although others are used as well.

3. The KP-5PDN-2 2-ft. parabolic antenna covering 4.9 to 6.4 GHz has gain ranging from 27.5 to 29.8 dBi, depending on frequency. This increases the input power from a maximum of 50 W to an EIRP nearly 10 times that, enabling long distances to be covered.

The benefit of microwave links is their ability to send information over long distances with a minimum amount of infrastructure, using cost-effective tower-mounted antennas. For example, the KP-5PDN-2 *(Fig. 3)* is a versatile 2-ft. parabolic antenna with N-type connectors covering 4.9 to 6.4 GHz with gain of 30 dBi. Its highly directional pattern reduces interference and provides a reliable link over paths of tens of miles. The YA17KPPD is a rugged, industrial yagi antenna operating between 880 and 948 MHz with 17 dBi of gain and can withstand heavy ice, high wind, and other harsh environmental conditions.

The second tier is connected using point-to-point microwave links for provision of telemetry and backhaul to substations that are connected to the Tier 1 backbone. One of the main problems currently faced by utilities is lack of available spectrum nearly anywhere at 6 GHz and below, so they must cope with sharing frequencies using the FCC's new Citizens Broadband Radio Service (CBRS) at 3.5 GHz.

Frequency sharing is becoming more common today, owing to the lack of available spectrum. However, for mission-critical applications, it leaves a lot to be desired. That is, the allocated spectrum is divided into three classes, the first being incumbents (primarily government radars). These incumbents must be protected from interference from licensed Priority Access Licensees (PAL). The lowest class, unlicensed General Authorized Access (GAA) users, who have no protection from the upper classes and must not interfere with them. As CBRS is just now being deployed, it remains to be seen how well this extremely complex system will work as another frequency-sharing scenario, because the so-called white-space frequencies between 470 and 790 MHz have suffered significant issues.

The third tier is the one that resembles what most people would consider IoT as it consists of many sensors and RTUs served by a low-power, low-speed network using narrow channels at 900 MHz. Tier 3 is typically a much more localized solution. Nevertheless, it increasingly requires higher data rates to carry high-resolution video that's in limited use today, but will likely be a required capability in the future.

As 6 GHz is one of the primary frequencies used by utilities for SCADA, emergency management, and land-mobile radio, there's increasing concern about an FCC Notice of Proposed Rulemaking that would allow use of the 5.925- to 7.125-GHz band for unlicensed operation by other services. Like every snippet of potentially available spectrum, this one is contentious because of the potential for interference to other services operating on or near each other.

However, for mission-critical infrastructure, sharing of spectrum presents potential national security issues, which is why it has always relied on its own networks operating licensed frequencies. Nuclear power plants, for example, rely almost entirely on 6-GHz systems for backhaul communications. Utilities were already spectrally "refarmed" once from frequencies around 2 GHz in the 1990s, at massive cost, to make way for commercial services.

If this happens again, the alternatives are at 8 and 11 GHz, whose propagation characteristics are less favorable than 6 GHz for spanning distances between microwave radios. Consequently, this would require more than simply changing frequencies in hardware. Coverage analysis would be needed on a huge scale, along with moving existing towers and adding new ones, including their installed equipment like parabolic antennas. As of this writing, no decision has been made about how this spectrum will be used.

IIoT and SCADA

The emergence of IoT has already created one possible opportunity for organizations that use SCADA: Competition between the cellular industry and LPWAN providers for providing connectivity between IoT deployments and the internet. Both offer solutions designed specifically for connecting vast numbers of devices that transmit minimal amounts of data.

Cellular carriers offer the LTE-M and narrowband IoT (NB-IoT) protocols for this purpose, while LPWANs are increasingly centered on two solutions, Sigfox, and variations of the LoRa protocol, such as LinkLabs Symphony Link. The difference between these solutions and 4G is their focus on the needs of small, typically battery-operated devices rather than delivering blazingly fast speeds required for consumer applications.

Operators of mission-critical infrastructure would argue that while cellular wireless networks are the undisputed leaders in providing ubiquitous coverage, they're still commercial systems, and do not meet their demanding requirements for reliability. In addition, carriers and LPWAN providers charge a fee for every node they connect, In the case of LPWAN specifically, coverage is a tiny fraction of what cellular offers, and as a competitor to the cellular behemoth, is not certain to survive.

That said, in order to adequately serve "Industry 4.0," both services must find a way to connect devices with either minimal or no modern connections—wired or wireless. These could be pumps that have been in service for years but still work fine, are expensive, and would be senseless to replace if only for becoming part of a modern network.

The solution to this issue is "bolting-on" connectivity. This can be done via an inexpensive device that senses changes in some critical operating characteristic (like noise or vibration), converts the analog sensor to digital form, and communicates it to a gateway via one of the various short-range wireless protocols used for IoT (Zigbee, Bluetooth, Z-Wave, etc.).

However, issues arise when employing this approach in the SCADA environment, whose sensors typically use wired connections to the RTU or, like some of their legacy industrial counterparts, have no connectivity at all. Many of the locations monitored by SCADA are far from civilization and experience environmental conditions far more hostile than comparatively benign industrial settings. This is not an insurmountable problem in most cases, as some form of protection can be added to encase the device, assuming the addition is actually worth the effort.

Another fundamental issue when considering IoT integration with SCADA is whether it's worth the risk, since access to the internet is IoT's mandatory requirement. In SCADA, nearly all decision-making, limited though it may be when compared with IoT, resides at the PLC or RTU, which eliminates the ever-more onerous issues with internet security. With IoT, decisions are made locally as well, increasingly in edge computers and gateways, but the data eventually finds its way to a cloud data center—via the Internet.

Summary

IoT may be taking the industrial world by storm, but it won't replace SCADA systems, at least not in the foreseeable future. Instead, SCADA will take those IoT elements that benefit it, such as advanced sensors, and eventually have the ability to perform preventative and prescriptive maintenance. Right now, SCADA's biggest challenge is arguably finding frequencies in which it can perform its mission-critical functions without interference from other services. Once this problem is solved, it has a clear path toward advancing from a supervisory to a fully automated solution, employing high-resolution artificial intelligence and many other technologies.

Justin Pollock is senior antenna engineer at KP Performance Antennas in Edmonton, Alberta, Canada. He is responsible for the design, prototyping, and characterization of antennas for point-to-point and point-to-multipoint applications used in backhaul, client premise, and access point radio equipment. Justin received his BSEE and Ph.D from the University of Alberta.