# TABLE OF CONTENTS

**Major Industry Partners Collaborate to Advance FDI Technology** | 5
We explore how Field Device Integration (FDI) technology, through its full featured capabilities, backward compatibility and wide industry support, provides automation stakeholders with an open, future-proof standard for integration and a superior user experience.

**Ethernet as an enabler** | 9
Success depends on the skill level of the system architect.

**Alternate paths from the field to cloud** | 12
Going off road to move data from the field and plant-floors to enterprises and the cloud includes bypassing the usual control routes.

**Wireless is a cornerstone of digitalization** | 30
From Ethernet to cloud-based services and the IIoT, how networks are being extended and assisted by wireless devices.

**What cost pervasive networking?** | 37
Comparing prices of HART, WirelessHART and fieldbus can lead to surprising results.

**Build those firewalls** | 40
Why and how secure industrial control and safety systems at every conduit.

**IT, OT unite during gas network upgrade** | 49
When the FBI identified unauthorized monitoring of one of its SQL systems several years ago, Washington Gas began working with the FBI and the U.S. Department of Homeland Security (DHS) to redesign its data infrastructure.
AD INDEX

Acromag • www.acromag.com/sp230 11
Kepware • www.kepware.com 29
Nexans • www.nexans.us/industrial 4
Turck • www.kepware.com 42, 43, 44
CONNECT & CONVERGE
Downtime is lost time. And lost time means lost profitability. With Nexans Industrial Ethernet Solutions, you’re getting a solution you can trust; one that supports your requirement for 100% uptime.

Nexans gives you the confidence to make the connection. Visit nexans.us/industrial to learn more.
Major industry partners collaborate to advance FDI technology

We explore how Field Device Integration (FDI) technology, through its full featured capabilities, backward compatibility and wide industry support, provides automation stakeholders with an open, future-proof standard for integration and a superior user experience.

By FieldComm Group

As digitalization increases throughout industrial operations, there is the creation of a significant amount of additional data. Thus, more sophisticated strategies are needed to manage data from intelligent devices and other sources, determine what is relevant, and assure that relevant data is made available to the appropriate systems.

Interoperability and data transparency on all levels are key factors in the acceptance of emerging technologies in the process industries. The following article describes how Field Device Integration (FDI) technology, through its full featured capabilities, backward compatibility and wide industry support, provides automation stakeholders with an open, future-proof standard for integration and a superior user experience.

**NEED FOR SEAMLESS INTEGRATION**

In today’s complex process automation systems, field instruments from many different manufacturers have to be integrated – resulting in significant effort for installation, version management and device operation.

The latest intelligent devices can also pose an information management problem, especially when there are devices on different networks with different underlying technologies for displaying and managing information.

Responding to the need for open and standardized device integration, leading process industry foundations, including FieldComm Group, Profieldus International, and the OPC Foundation, jointly developed the FDI
standard. Their goal was to solve the problem of integrating field devices with the multitude of networks, operating systems and control systems commonly used in process plants.

FDI helps bring previously inaccessible data into commonly reported and displayed information, so it can be used to add value for applications and businesses. The specification is based on the IEC 61804 - Electronic Device Description Language (EDDL) standard for the description of devices. It takes account of the various tasks over the entire lifecycle for both simple and the most complex devices.

The primary objective of FDI is to dramatically simplify software installation, configuration, maintenance, and management of field instruments and host systems. Modern field instruments often include a device information file that provides software access to the features and functions of the device, one or more user interface plug-ins that integrate with host system software to enhance the usability of the device with the host, numerous user manuals, installation instructions, and data sheets.

FDI brings standardization to the packaging and distribution of all the software and tools necessary to integrate a device with a host system. All registered FDI devices are required to have an associated FDI Device Package, which is a collection of files including an Electronic Device Description (EDD)-based on IEC 61804-3, an optional user interface plug-in (UIP) based on Windows® Presentation Foundation (WPF), and instrument documentation and technology-specific files.

FDI not only supports FieldComm Group protocols such as HART, WirelessHART and FOUNDATION Fieldbus, but also Profibus, Profinet and ISA 100.11a. Through stand-alone communication servers, additional protocols like Modbus and EtherNet/IP are also integrated with the technology.

**PREPARING FOR DIGITAL TRANSFORMATION**

In the industrial automation sector, there are ever-increasing demands to leverage process automation data from information systems, as well as utilize architectures for more open interfaces. Initiatives like the NAMUR Open Architecture, Industry 4.0 and the Industrial Internet of Things (IIoT) all seek to break down proprietary architecture barriers between field devices and, ultimately, cloud-based computing platforms. They are revolutionizing the way users and machines interact, as well as the way machines engage with each other.

Recognizing current trends in digital transformation, the architects of FDI partnered with the OPC Foundation to include several OPC specifications that define field device integration in the context of FDI technology. Their intention was to ensure that as
systems evolve an open pathway to field
device information is assured. This work
holds significant value for automation end
users, allowing them to take the data and
information models for the applications and
devices supported by FDI technology and
leverage OPC-UA information modeling and
corresponding services for complete appli-
cation-to-device integration.

FieldComm Group and OPC Foundation, as
of Q4 2017, have formed an official working
group around the OPC Unified Architecture
(UA) to develop an OPC-UA FDI Device Infor-
mation Model for process automation. The
goal of the working group is to leverage the
extensive experience of FieldComm Group
with the HART and FOUNDATION Fieldbus
communication protocols to standardize
data, information, and methods for all process
automation devices through FDI using OPC
UA. The OPC UA base information model and
companion Device Information (DI) specifica-
tion will be extended to include the generic
definition and information associated with
process automation devices. This information
model is at the core of the FDI standard. It
seamlessly integrates with OPC-UA to enable
further integration with platforms like the Mic-
rosoft Azure IoT hub.

The OPC-UA FDI Device Information Model
defines how the information of a field
device – described by an Electronic Device
Description (EDD) document – is mapped
to OPC-UA Objects, Methods and Variables.
The model is mainly based on OPC-UA for
Devices specification; in fact, most of the
OPC-UA for Devices model has been driven
by FDI requirements.

The FDI architecture brings field devices to
the IIoT, with each device type represented
by a Device Package. FDI specifies a Device
Information Model and uses OPC-UA com-
munication to enable other applications to
access it. This model is the single access
point for external applications.

FDI also addresses cyber security with
manufacturer-signed packages that hosts
validate to ensure they’re genuine and
haven’t been altered. This reduces the main-
tenance costs and security implications.

REALIZING THE PROMISE OF IIoT
Throughout the process industries, devel-
opments such as the IIoT will enable the
transition from reactive to predictive main-
tenance, as well as the optimization of
asset management strategies to improve
operations and reduce costs. Their prom-
ise is full utilization of digitally available
information from existing, installed field
instruments to improve safety, operations,
and reliability. Plant floor to executive office
real-time access is key to delivering value to
the enterprise.

By including all tools, documents, and
interfaces in a single device package, FDI
improves system integration efficiency
and allows easier access by Information Technology (IT) systems to Operational Technology (OT) information. Moreover, it unifies device drivers, configuration tools, diagnostics and documentation regardless of operating system with an independent and downloadable software package compatible with any FDI-registered host system.

With its device information model (set forth in IEC 62541-100), the client/server architecture of FDI technology provides all functions for modeling real devices as virtual objects for the IIoT.

Manufacturers and other industrial firms deploying IIoT applications can connect to valuable information in intelligent field devices – regardless of protocol – by using FDI to integrate the information in a process control system, asset management tool or Enterprise Resource Planning (ERP) system; visualize and evaluate the data; and then take action based on the information to prevent shutdowns, lower operating costs, reduce maintenance expenses, and become more predictive in how plants are run.

LOOKING TO THE FUTURE
For industrial organizations of all sizes, utilization of digital intelligence empowered by the IIoT will create more capital investment. Higher field reliability will help ensure increased uptime, safer operations, and greater efficiency. Advanced automation technology will also raise productivity, manage assets over their entire lifecycle, and optimize experts’ knowledge to drive profitable business results.

The future is sure to bring additional advancements in digital transformation. For example, the FieldComm Group-OPC Foundation Integration Working Group is currently enhancing the OPC-UA FDI Device Information Model specification to provide semantics for machine-readable information. When complete, this specification will allow cloud-based applications to process field device information without extra configuration.

Thanks to FDI, automation suppliers and end users can look forward to applying a single integration technology that can translate the binary data delivered by any communication protocol into tangible information that can be displayed and used by systems at varying levels throughout the enterprise.

CONCLUSION
The future is digital, and digital should be intuitive and easy to use. FDI is a versatile device integration technology that has been designed to meet current and future plant needs, which include investment protection, robustness, easy system administration, easy to use devices, interoperability, and simple migration.

For more information, please visit the FDI Technology page on the FieldComm Group website.
Internet of things (IoT) and Industrial IoT (IIoT) don’t specifically identify Ethernet in the names themselves, but there’s no disputing that it’s a key enabler to making the concepts possible. Unfortunately, like so many things, the majority of people using the technology don’t have any idea of how it works. We as automation professionals are not so lucky, since not only do we have to design, build and maintain these systems, we must also do so without disruption to service, making maintenance and upgrading a challenge.

To be able to connect anything, anywhere, it’s also a foregone conclusion that at least part of the network will be wireless. The form of wireless network will be largely driven by bandwidth requirements and distance between nodes. For higher bandwidth and intermediate distances, wireless Ethernet (Wi-Fi) will be part of the equation.

Most of us now take wireless Ethernet for granted, and expect to access it with sufficient bandwidth almost anywhere. Wireless is so reliable in non-industrial settings that many houses and offices are no longer running copper—unless it’s for power over Ethernet (PoE), simply connect everything to the Wi-Fi network. An example of this is the streaming media player I purchased over holidays that only supports Wi-Fi, with a USB connection for power only.

Regrettably, the plant environment, with its fixed and mobile “canyons of steel,” EMI/RFI emissions due to medium- and high-voltage equipment, high humidity, and

---

Ethernet as an enabler

Success depends on the skill level of the system architect.

Ian Verhappen, Senior Project Manager, Automation, CIMA+
high and (as we are finding out this year) low temperatures is not quite as friendly as the family room at home. Fortunately, the latest 802.11 standards now support multipath routing, which has reduced the effect of those steel canyons on overall reliability.

Of course, control systems must have end-to-end connection with the right data going to and from the right place at the right time, over what is inherently a non-deterministic network. Making all the packets and information move across the systems is the responsibility of higher layers of the networking framework. However, like any control signal, if Ethernet, the physical layer, isn’t reliable, the protocols and messages won’t be reliable.

The role of system architect is therefore becoming increasingly important to ensure that new system designs incorporate the necessary features to provide the required end-to-end connectivity between the various nodes and protocols. When integrating a new and a legacy system, understanding the potential interactions between different network elements makes this role even more critical. Most system architects understand business networks and the systems associated with them. However, because of the relatively small number of control networks, it’s unlikely that an individual other than one employed by the control system supplier will be able to consider all the system nuances to deploy a rugged reliable network.

The resulting system must be designed for heavy traffic loads between certain nodes (i.e. updating HMI) as well as slower analog or serial connections and gateways, along with, of course, reliability and cybersecurity.

A well-designed system architecture must perform for present as well as anticipated future loading. As we know, estimating future loading is a “best guess” situation because the amount of data flowing continues to grow exponentially—not only in the business world, but also in the “closed” control system environment.

The architect must also stay abreast of constantly evolving standards and capabilities of new software, hardware, equipment and vulnerabilities. Considering all this, is it any wonder that if it’s possible to use Ethernet and IP-based systems to move all the data packets about, they’ll remain as the common denominator?

Ethernet is not a protocol. It is, however, an enabler for not only today’s control systems, but also those of the foreseeable future, where, if the vision of the Open Process Automation Forum is correct, the control system (other than the edge device signal processing equipment) will all be based on software modules communicating to each other over Ethernet and IP-based networks.
New Signal Splitters / Duplicators
Precise Scaling of I/O Ranges

New Signal Splitters Offer Easy Set-up

Acromag’s new SP230 series of isolated 2-wire signal splitters are designed for easier installation and setup.

Four models, covering a broad range of sensor signals, provide dual 4-20mA outputs proportional to a single current, voltage or temperature input. They receive power from either output loop.

A USB connection to a Windows PC or Android device enables simple, precise configuration of I/O ranges and a variety of operational settings with free software.

The combination of software-guided setup, two-wire loop-powered installation, and removable wiring terminal blocks, make SP230s the most convenient solution for signal splitting/duplicating applications.

And with a variety of models to support a spectrum of input, output, and power requirements, you can confidently standardize on this series for future signal conditioning projects.

Visit www.Acromag.com/SP230 TO LEARN MORE

Signal Conditioning & Network I/O Solutions

- microBlox® I/O Modules
- Transmitters, Isolators, Splitters
- Ethernet, Modbus & Profibus I/O
- Limit Alarms / Computation
Everyone’s looking for shortcuts. It’s a primary preoccupation of modern life and a cornerstone of business and industry. Part of always doing more with less, of course, includes moving production data faster and more efficiently from process applications, field equipment and plant-floors up to decision-makers and enterprise levels.

In the past, this required running data from sensors, instruments, transmitters and I/O modules through dedicated components, controls and networks that—even though they’ve evolved from using point-to-point hardwiring to fieldbuses and Ethernet—are showing up as increasingly inflexible. Some process users and system integrators report that adding devices and functions to existing systems, and even making adjustments, typically requires lengthy and complex reprogramming and reconfiguration, if they can be done at all. Think of it as road construction added to traffic jams.

FINDING THE FAST LANE
“We’re in the process of monitoring several hundred variable frequency drives (VFD) that run the kiln fans and setting equipment at an architectural brick manufacturer because some of the drives previously had failures,” says Steve Beck, chemical engineer at Huffman Engineering, a CSIA-certified system integrator in Lincoln, Neb. “We thought about adding a PLC to get the data to the SCADA system, but we also wanted to limit costs, so we added an OPC-UA server, Ignition SCADA software from Inductive Automation and an embedded Ethernet switch/adapter, which
can communicate directly with the VFDs. We initially replaced 20 of the drives, and this new solution has already saved about $10,000, not including the labor saved by not having to install, configure, program and get power to another controller. We’re already looking to expand to monitoring more drives. If we build out the whole plant, the savings could be six figures.”

Though Huffman’s VFD project at the brick plant only involves monitoring at present, Beck adds it could eventually be used for control, too. “We’re not changing controls yet. It would depend on the success of the monitoring project, but we could bypass the existing controls, and do control with the Ignition SCADA software,” says Beck. “We could write setpoints to the parameters in the VFDs instead of writing to the usual PLC, and this would let us use Ignition to perform control functions. Other similar arrangements could do the same, such as using a simple protocol converter with software like Wonderware’s InTouch or System Platform, or Kepware’s Kepserver. There’s not much documentation about how to do this, so it’s also important to test hardware and software you’re considering. We set up a bench test for monitoring the VFDs, and checked that Ignition, OPC-UA and the Ethernet switch would work before installing them at the factory.”

Colin Geis, product management director at Red Lion Controls, adds that, “The IIoT is evolving quickly and can be classified in a few stages. At first, IIoT was seen as a data visualization tool in the cloud. Data would be transmitted to a cloud repository, and the IIoT platform would present a data dashboard allowing anybody, anywhere to see system data easily. These cloud dashboards could be considered “IIoT v1.” Next, IoT v2 took the data visualization and added intelligence, reporting and alarming, which allowed more autonomous operation, notifying if a system or process outside of programmed conditions and didn’t require an operator to monitor screens 24/7. Now, IIoT v3 is opening the way for distributed control, or bidirectional control with systems and processes. This phase of the IIoT is expanding on data dashboards, centralized alarming and also creating a feedback loop with the edge of the network. While some customers are allowing the feedback loop control equipment, more customers are simply allowing this feedback loop to modify a local database in the field (e.g. confirming that an alarm was received or an action was taken by the cloud platform).

“Another practice we’re seeing is having edge devices alert and alarm locally based on their programming, even as they’re communicating information upstream to a cloud platform where further action may be taken. Customers must place a large amount of trust in their equipment and network to allow for full autonomous control of their equipment by an IIoT platform, and this
“Many process applications don’t need millisecond or one-second updates, and instead have updates of a minute or more, so some users are looking outside the process control network to develop a process data network.”

hybrid model gives customers greater confidence. More customers asking questions about this functionality, and our equipment is capable of performing these tasks, but it’s still a little early to call it mainstream. Customers are deploying more edge control with IIoT connectivity because the visibility to the system and process has improved so much, but it isn’t standard practice to deploy platform-driven edge control yet.”

Stephen Neuberger, CEO of Krohne Group, adds that, “Users need standard, uniform, open communication channels to participate in the IIoT without compromising safety and availability. Likewise, modularized and decentralized instrumentation of sensors is allowing them to send data directly to plant enterprise resource planning (ERP) systems. We’re not saying the DCS is going to disappear, and it can’t because real-time control can’t be in the cloud. However, there have to be some added paths for clients’ information to take, which improves their ability to add value, and achieve individual production with all the advantages of mass production.”

DESPERATELY SEEKING DETOURS

Just as gridlocked drivers fantasize about cruising on the shoulder, users and integrators have long sought similar ways to get around the networking snarls and data delays up ahead. However, though they could dream, there was no fast lane due to scarce resources, network bandwidth limits and other constraints, which have only recently started to give way to new pathways.

“In our circle of control users, we’re all very conservative, but we accept that we must get data from plant floors to businesses. We’ve worked with custom applications and data collection for many years, but there’s a growing tendency to believe that we can’t continue with proprietary software, which was a typical solution practice in the
past,” says Michael McEnery, president of McEnery Automation, which is a CSIA-certified system integrator in St. Louis. It serves mostly large beverage manufacturers and their batching, recipe management, filling and canning applications. “We try to support older operating systems, but keeping up with traditional technology is just getting to be too costly, and users want standardized operating systems, hardware and security.

“Plant managers at one sewer district want to see operations like well levels on their tablet PCs and smart phones, so we’re putting together a quote to take their data that’s now in a GE iFix historian, and put it in a best-fit application that’s cost effective and reliable. Fifteen years ago, we did custom databases and web pages for monitoring and maintaining valves, motors and other equipment, but we don’t prefer that approach anymore. Now, data from historians such as Rockwell Automation’s FactoryTalk Historian, OSI PI or Wonderware Historian can be delivered by off-the-shelf reporting tool clients that easily integrate with browsers on PCs, tablets and smart phones. We’re also seeing more clients considering IIoT and big data, but there’s still more talk than action.”

McEnery adds that phenomena like IIoT and big data are forcing process engineers and system integrators to make some mental shifts. “As engineers, we’re supposed to be as efficient as possible, including how much memory we use and data we gather,” he explains. “If we didn’t need specific data, we didn’t capture it because of cost. However, these days, data and memory are a lot cheaper, so the new mindset is to collect as much as possible, and then use analytic software to see if it’s useful later.”

Mike Boudreaux, director of the Connected Services program at Emerson Automation Solutions, adds that, “A wide swath of users are recognizing that new analytics, applications, software and other capabilities can be enabled by connecting to existing systems. So, while getting DCS data still makes sense, they can also deploy wireless and other network points that aren’t needed for control and safety, and get valuable pressure, temperature and flow measurements. Many process applications don’t need millisecond or 1 second updates, and instead have updates of a minute or more, so some users are looking outside the process control network to develop a ‘process data network’ with many of the same devices. For example, Emerson’s wireless pressure gauge now has an electronic sensor and digital wireless instead of the traditional mechanical device with dials.”

Of course, once this data reaches an Ethernet network, it can be delivered immediately to the enterprise, the cloud and other server-based applications for analysis.
and performance/reliability monitoring on laptops, tablet PCs, smart phones and other interfaces. “Emerson and other providers can host applications, and even do monitoring for clients as a service,” adds Boudreaux. “It’s a lot like a cable TV subscription. However, this only monitoring; we’re not doing control and safety functions in the cloud, though wireless for monitoring is proven, and more efforts to leverage the cloud are happening.”

“Many users want to aggregate and visualize data, and not do control or deal with the extra costs of adding PLCs and HMIs. They’re asking why they need a PLC if they’re not doing control?”

HISTORY OF SHRINKAGE

While the idea of skipping the PLC or DCS might be unthinkable to many engineers, operators and managers, this concept is just one chapter in the epic story of faster, more powerful, less costly and smaller computing devices in industry and elsewhere. The journey from clunky hardware to virtual software seems inexorable in all cases.

“We should remember that PLCs have shrunk a ton since they were first introduced,” says Michael Robinson, national marketing manager for projects, solutions and services at Endress+Hauser. “The first 8-bit PLCs in the 1970s were big and very costly, but by 2012, they were 32- or 64-bit, fit in your hand, and cost only $500. Ten years ago, getting data from instruments was cumbersome and expensive with analog inputs and outputs, but for today’s users that just want to visualize or analyze their data, it may still be difficult to integrate and network several plant controllers. Everyone uses the same Ethernet cables now, but the fieldbus protocol wars of the mid-1990s still haunt us today, so we still have five communication cards talking different languages.

“Nevertheless, many users want to aggregate and visualize data, and not necessarily do control, or deal with the extra costs of adding PLCs and HMIs. They just want to monitor their flows and tanks, and communicate that data to the cloud. These efforts began with HART, Profibus and Ethernet gateways and WiFi or cellular modems. We also made chart
recorder replacements, Memograph and Ecograph, which brought instrument data in, and did local visualization. Now, it’s just shared with the enterprise via the cloud, and the gateways are called IoT or edge devices, some of which can run open-source code like Python to manipulate their data streams. As result, many users ask themselves why they need a PLC if they’re not doing control?”

Dave Emerson, director of the U.S. technology center at Yokogawa Corp. of America, adds that, “The influx of IT into the automation space is increasing. It’s obvious, just like when computing went from Unix to Windows, and the same is happening to distributed controls. If you want to add I/O points to a DCS then you typically need to call a specialist, but new, low-cost sensors, wireless and edge devices are getting data to the cloud faster and at less cost.”

Bruce Billedeaux, senior consultant at system integrator Maverick Technologies, a Rockwell Automation company, adds that bypassing PLCs can be accomplished. In fact, doing it was one of the initial visions of the HART protocol, which was developed in the mid-1980s, and originally sought to perform distributed control through a 4-20 mA loop. “However, HART was too far ahead of its time back then, and users couldn’t handle the communications needed,” says Billedeaux. “Now, HART is getting more of backbone it needs, and we’re going to become ubiquitous as more controls move to the cloud.”

**SIMPLIFYING WITH SCADA**

Once data from any sensor, instrument or other field or plant device touches Ethernet and the Internet, it’s basically off to the races, and users at every level from the enterprise to the cloud can access it if they’re speaking the right protocol and have the right permissions and programming. Whether it’s bypassed controls or not, this information also needs a place to land and a SCADA/HMI to display it, though these interfaces are also simplifying and standardizing around the Internet’s well-known, Ethernet-based Transmission Control Protocol/Internet Protocol (TCP/IP).

For instance, vegetable oil and grain processor Adams Group Inc. in Arbuckle, Calif.,
recently worked with system integrator Calcon Systems in San Ramon, Calif., to also implement web- and Java-based Ignition software for supervisory control, data acquisition, manufacturing execution systems (MES) and IoT solutions in its vegetable oil plant. Adams is the largest U.S. supplier of organic oils, expeller-pressed oils, including sunflower, safflower and canola.

“We just wanted to share data between two systems, and Ignition’s advantage is that it’s all in its open database,” says Shawn Ferron, project manager at Calcon. “The information isn’t in some proprietary database you can’t access.”

Adams reports Ignition enables more efficiency, better visual displays, more data, faster implementation and is easier to use than its previous SCADA systems, and adds it may apply it company-wide. About 20 operators and managers in the vegetable oil plant’s control room use Ignition on nine computer monitors, which show KPIs and details about batches, alarms, downtime, runtime, shift performance and historical data (Figure 1). “We’ve seen an increase in some efficiencies that were tangible,” says David Kay, operations manager at Adams Group.

Lee Smith, general manager at Adams Vegetable Oils, adds that Ignition’s unlimited licenses gives his operations more flexibility. “I didn’t want to be limited by how many licenses I could have, or how many screens I could put in my plant, or how many people I could have looking at a computer at night,” he explains. “I didn’t want to have to buy a new client every time we wanted to do something. The future is open-source technology and limitless licenses.” As a result, Adams has created several projects with Ignition, including dashboards with graphic displays of KPIs and other information and a work order creation system.

“Certainly, Ignition is SCADA software, but in fact, SCADA is only part of the overall platform. It’s vital to bring device data into the infrastructure, and make it available to the whole enterprise. To do that, you have to decouple devices from applications,” says Don Pearson, Inductive’s chief strategy officer. “The Ignition industrial application platform and its unlimited license model are perfectly suited for this task. Old licensing models break the bank because they couple applications and devices, and charge by connections, users and tags, effectively stifling innovation. They’re complex and costly when users want to get more data, add devices and scale to hundreds of thousands of connections across an enterprise.”

Likewise, eight oil and gas production facilities in Oman’s Mukhaizna field have used steam-assisted gravity drainage to increase recovery for more than 10 years, but their data collection systems based on Rockwell
Automation’s PLCs linked to Iconics Genesis32’s HMI/SCADA software began to need help as the facilities’ data points multiplied over the years. They’d been using Top Server OPC server from Software Toolbox to gather data from up to 20 PLCs and feed it to the HMI, but recent equipment additions had increased tags in the system close to 30,000. This wouldn’t usually be a problem for Top Server, but the HMI was also requiring it to make device reads that bypassed the server’s device-level optimization, and the HMI was requesting out-of-order updates on groups of OPC tags—which both slowed the data collection process.

“The OPC server seemed to be dying under the load,” says Juan Munoz, project manager at the Mukhaizna oil field project. “Even at rates as low as once per second, it was difficult to scan 30,000 tags, and get the critical data changes that we needed.”

Knowing the server wasn’t at fault, Munoz reports he searched Software Toolbox’s website, and found Cogent DataHub, a memory-resident, real-time database from Cogent Real-Time Systems, a subsidiary of Skkynet. Acting as an OPC client to Top Server, DataHub can request data based on tag value changes, which are called “asynchronous advise.” This means that, instead of 30,000 tags per second, the server only sends data for a tag when it changes value, and it’s free to poll the devices in the most efficient way, always keeping DataHub up to date with the latest data values. DataHub also keeps all the latest tag values in memory, and can efficiently send them to the HMI on each poll.

“DataHub effectively decouples the OPC server from the client,” adds Munoz. “All the load is on DataHub’s shoulders now, and the performance is much better.” Top Server is now free to optimize communications to the device, while DataHub protects it from device reads. This has relieved Mukhaizna’s users from having to redesign their HMI and PLC configurations, saving tens of thousands of dollars in engineering and development work.

Teresa Benson, product marketing manager at Red Lion, explains, “We continue to see two key considerations—simplicity and security—driving decisions in the field-to-enterprise area. While some sensor and instrument manufacturers offer “IoT-enabled” technology (for example, cables with built-in power sensors and network connectivity, or small Raspberry Pi-like cellular devices bolted on to sensors), most users still employ a simpler aggregate-and-act architecture. Even in applications where we see LPW/WPAN sensor networks, ultimately there are one or more gateway devices that act as converter, aggregator and occasionally actor, though they usually send data upstream (if even just upstream in a plant to an edge device) for decision
and action. This aggregation architecture also gives customers a lower cost of entry into IoT, as they’re usually able to start with existing sensors versus requiring new and potentially more costly sensing equipment or instrumentation.”

“While the choice of backhaul medium (such as cellular versus wired Ethernet) is usually driven by geography of deployment, we’re increasingly seeing it as a choice about network security. Sometimes, especially for OEMs who are deploying machines with a ‘remote service’ feature or built in recurring revenue stream, manufacturers are building cellular communications into equipment that may be installed on premise. The most common reason we’ve found is that they want to offer connected services such as remote diagnostics and maintenance. Offering cellular connectivity, and therefore a completely separate, owned and managed network connection, is a way to reduce concerns of their users’ IT teams about having to provide and maintain a secure, accessible node on the network for a third party.”

**IIOT AND MQTT**

No doubt the main draw of bypassing traditional controls is it simplifies the trip from the field up to the enterprise and its cloud-computing services and Industrial Internet of Things (IIoT) participants. There are several ways to do this job, but one that appears to be gaining the most ground lately is Message Queue Telemetry Transport, which is a publish-subscribe, machine-to-machine messaging protocol that sits on top of TCP/IP.

“Traditionally, a HART transmitter would bring one value from a process device such as a Magnetrol level instrument, and send it via 4-20 mA to a PLC using a poll-and-response protocol,” says Arlen Nipper, president of Cirrus Link Solutions and co-inventor of MQTT. “Usually, there are many applications and devices mish-mashed together, and they eat bandwidth, aren’t scalable for adding applications, and are difficult to maintain. We think a new architecture is needed that decouples applications from their devices, and uses MQTT as a broker that can publish data from the application side, and let users on the subscriber side use it as needed.

“MQTT lets us eliminate the PLC by using hybrid poll-response or publish-subscribe protocol to free us from traditional poll-and-response. When these devices plug in, their tags are explained, they don’t need configuration, they immediately begin storing history, and they let users easily make screens and alarms.”

Travis Cox, co-director of sales engineering at Inductive, adds that, “Sensors and field devices usually send one or two values to their PLC, but there can be hundreds of
“We’re not disrespecting PLCs. It’s just that traditional control setups you don’t touch for 20 years and the mentality that goes with them don’t work with the Internet.”

others that don’t go to the controllers. In the case of Magnetrol’s level probe, the question is what happens when you have a problem, and the level indication isn’t enough for troubleshooting? Usually, it means a technician has to go and physically read the 1x4 in. LED screen on the device, and a lot of other data getting stranded. As a result, we worked with Magnetrol, and added a little Blue Tech PC with an ARM processor, HART modem and cellular connection to read the instrument’s 480 local data points, and publish them to the cloud. Sometimes you need to skip the PLC because some data can’t get to it, but it’s still important for troubleshooting. Plus, many users can’t put a PLC in a certain location because it’s just too expensive.”

To bring MQTT down closer to operations, Inductive recently introduced its Ignition Edge Panel software to create local HMIs for field devices with local and remote web clients, Ignition Edge Enterprise that synchs data from edge devices to a centralized server, and Ignition Edge MQTT that turns field devices into MQTT-enabled, edge-of-network gateways.

“MQTT is the next big development for transferring process data from sensors and field instruments to PLCs, DCSs and higher-level MES computing, Internet and cloud-based solutions,” says Aldo Ferrante, president of ITG Technologies, a CSIA-member system integrator in Jacksonville, Fla., which recently developed its own cloud-based, IoT platform called Smart Operational Real-time, Big data Analytics (SORBA). “An MQTT broker manages data between devices and can handle small amounts to very large blocks of data making it very versatile and provide an industry standard between multiple systems.

“MQTT offer enterprise-level security and data encryption to protect the integrity of the system. And, as sensors become smarter and self-contained, decisions don’t need to rely on a master control platform. Instead, embedded logic allows devices to control
by exception, reducing the need for lightning-speed, isolated networks. Lightweight, embedded processors with MQTT can enable and extended the ability to distribute sensors over a vast geographical area.”

THE HARDWARE WAY

While it can seem like software is doing all the work and having all the fun of simplifying networks and circumventing controls, there are actually several different hardware-based approaches that can achieve the same goals—even if they rely on software, too.

For instance, Opto 22 recently released what it reports is an industry-first representational state transfer (RESTful) application program interface (API) and server to its programmable automation controllers (PAC), which will accelerate adoption, rollout, and ROI of IIoT applications by flattening IIoT architectures, reducing complexity and eliminating middleware.

Through this new RESTful API, developers gain secure programmatic access to new or legacy physical assets through control variables and I/O data using any programming language that supports JavaScript object notation (JSON). Available through a free updated firmware release for Opto 22’s Snap PACs, its RESTful API includes an HTTP/S server accessible from any HTTP/S-compatible client.

“Putting RESTful API right down in the PAC means data requests are open and
documented, and just reference the API’s documentation, so it’s clear what data to pull,” says Benson Hougland, Opto 22’s vice president marketing and product strategy. “This means data requests don’t need to set a database ahead of time or give a tag list. This is a much more fluid method for moving and sharing data among entities in an simple, open and understandable way. The industrial automation and control industry is in transition right now. Vendors that have relied on a product development strategy based on proprietary and closed technologies have become outdated. The future of the industrial automation and process control industries lies in the rising API and data economies made possible through open standards-based technologies.”

Philip Marshall, CEO of Hilscher North America, adds that, “Users want stable systems that are robust against attacks, but no one wants to patch their PLCs three to five times per week. This is where edge devices on the front line can really help. Because edge devices aren’t doing critical control functions, they’re easier to secure and patch if necessary. Hilscher’s netIOT Edge gateway with our netX communication chip inside can be air-gapped for read access only from IT/cloud applications. This prevents external intrusions, as data can’t be written from the cloud to the gateway. In passive mode, the Edge gateway ‘listens-to-all’ on the existing control network. Its main activity is aggregating mostly real-time Ethernet and IIoT data, such as OPC UA and MQTT, and configuring that data to formats that can be used by management systems, such as those from IBM, Microsoft and SAP. (Figure 2)

Marshall adds that two netX microprocessors have been added to Hilsher’s existing family of five. The two new netX chips enable OPC-UA and MQTT communications, and include security features such as secure boot and encryption.

“There’s a lot of benefits to bypassing PLCs and/or working with PLCs to bring only the data that’s needed to the cloud,” explained Marshall. “If you go right from the PLC to the cloud there can be added security risks for operations. We’re not disrespecting PLCs. It’s just that traditional control setups that you don’t touch for 20 years and the mentality that goes with them don’t work with the Internet. If you’re going to work with the cloud, you need to use dynamic systems that are hardened against attack and patched regularly like PCs, which don’t need to resolve requested updates with traditional controller software. We’re not out to replace PLCs. These edge devices are adjunct that just take IIoT-related data to the cloud, and don’t disturb or impact the process control that’s going on.”

Likewise, coming from the hardware side, Advantech B+B SmartWorx reports its Wzzard hardware and protocols, including
MQTT, work together to reduce the expertise and time needed to build scalable IoT connections. These devices include Wzzard intelligent edge nodes that connect to industry-standard sensors; SmartMesh IP wireless sensing technology that enables auto-形成了, self-healing, self-sustaining networks that are also highly scalable; and Swarm 341 Gateway that connects equipment and devices to the Internet or Intranets over wired Ethernet or wireless cellular connections.

“The sensor nodes pick up auxiliary signals from the process or automation system, and reports them to the gateway, which can have aggregation points such as smart metering,” explains Paul Kutch, IIoT solutions sales director at Advantech B+B SmartWorx. “The aggregation points let us add intelligence at the edge, enrich data, pick reports by exception, and reduce data consumption. For 40 years, we’ve been connecting devices to applications, but we need to think more about connecting devices infrastructure, and then plugging in applications. By using MQTT, Wzzard can publish temperature sensor data, for example, and 100 other devices can subscribe and use it as needed. We have to drop these monolithic, poll-and-response hosts that bottleneck our data.”

In addition, Turck Inc. recently introduced its field logic controllers (FLC) that bring simple logic programming down to the device level via IP-rated Ethernet I/O blocks with built-in FLC technology, which can run standalone without any PLC or cooperate with or backup PLCs. FLC technology uses a flowchart system to custom program the local Ethernet I/O blocks via an HTML5-compatible web browser. Through a series of drop-down menus, engineers can set up multiple conditions, operations and actions on one block. FLC also allows users to create high-density I/O without a PLC.

Similarly, Littelfuse Inc. recently launched its MP8000/MP8100 Series Bluetooth-enabled motor protection relay that allows maintenance personnel to communicate with it from up to 30 feet away using an app on a tablet PC or iPhone or Android smartphone. Once a smartphone is securely paired with MP8000/MP8100, users can easily monitor system status in real time, set up the relay, adjust its settings, and review its fault history. The app is intuitive and requires no training to use.

Varun Nagaraj, CEO of Sierra Monitor Corp., adds that, “Innovations in these technologies is all about novelty and value creation. For example, Digi International provides its model-oriented sensor cloud, while Monnit Corp. does all kinds of remote monitoring, and Samsara manufactures Internet-connected sensors systems. Even voice activated Amazon Echo is getting into building and facilities management, and could probably perform some monitoring or control tasks soon.”
**WIRELESS WEIGHS IN**
Because Ethernet provides the physical path for data to skip controls and/or simplify networks and communications, it’s no surprise that wireless can help, too.

Emerson’s Boudreaux adds that users in operations are examining other common, non-critical functions that might be candidates for network simplification, including bypassing controls. “Heat exchangers have instruments and controls that usually go to the DCS to control temperature, but they also have pressure signals that don’t go to the DCS, and these can be used to check for build-up and indicate the need for maintenance,’ explains Boudreaux. “Now we can replace a mechanical pressure gauge with a wireless one, and integrate measurements with heat exchanger monitoring software, so engineers can assess heat exchanger performance without opening it and with more certainty about what needs to be done. And, combining pressure sensing data with temperature and flow means we can also do thermodynamic evaluations on heat exchanger efficiency that are more holistic.

“Control is possible in some limited use cases using wireless measurements, but the biggest use case now is collecting data and monitoring applications outside of control, and finding areas that aren’t solved, such as heat exchangers, pump reliability, steam trap maintenance and others in the future. My thought is the opportunity isn’t so much bypassing controls, but rather putting measurements into monitoring networks where they make sense. We wouldn’t wire a control signal into a safety system unless it was required for safety, so why should we wire a monitoring signal into a control system if it isn’t required for control?”

McEnery adds that wireless can even deliver signals right to cloud-computing platforms and other server-based applications. For example, McEnery Automation recently took over integrating and maintaining remote terminal units (RTU) in some of the municipal water/wastewater systems operated by American Water Enterprises in St. Louis. McEnery has worked with American Water for many years, but this project involved RTUs implemented by Mission Communications Inc., which automates small pumping applications with just a few I/O points for level indication and pump control, and uses digital, cellular-connected radios to reach the Internet, and feed data to Mission’s server and cloud service. It also employs an OPC-UA server to gather data from all the locations in a customer’s facility, and send it to a Schneider Electric Wonderware SCADA system in their control room.

“RTUs have microcontrollers, so their pumps can run on their own and collect data, but in this case, their information skips the usual PLC or DCS, and goes right to the cellular connection, Internet and
server, which sends it back to the customer’s SCADA/HMI via the OPC connection and Wonderware Historian,” says McEnery. “This is a very cost effective approach when having to communicate with many small remote devices.”

**SUSTAINING SECURITY**

One of the richest ironies created by doing an end run on typical control infrastructures is that PLCs and DCSs can sometimes do the same—skip their own infrastructure, get on the Internet, and provide information without going through their usual channels. However, whether data goes around the PLC or DCS or through it, security remains a top concern for all users, integrators and suppliers.

“Probably the largest three arguments about using existing equipment versus bypassing it is security, access to relevant data, and impacts to current equipment/processes,” says Red Lion’s Geis. “Using existing equipment to access data can be an easy integration point, but how secure is the device (PLC, RTU, drive, etc.)? PLCs and most automation equipment were never designed to be deployed on a publicly accessible network and lack effective security from external threats. Integrating existing equipment to a secure IIoT gateway can provide security, but also may open up the control network if not properly configured.

“Does the device have access to all the data or sensors necessary to allow for a systematic approach to process improvement? Existing equipment was deployed for an application, e.g. control, monitoring, maintenance, etc. As such, the data collected from that equipment is likely to be application-specific. IIoT is about breaking that paradigm, and allowing data to be accessible to any application that requires it. What customers are finding is that while using existing equipment is an easy first step in the process, unfortunately this method doesn’t often provide enough data for a clear picture. Finally, customers need to evaluate the impact on the current process for installation of the new data collection system. Does the system/process need to be shut down for the installation of new sensors or to tap into existing sensors? Do new PLCs, RTUs, DCSs, I/O, Ethernet, and power need to be run to the new locations?”

ITG’s Ferrante adds, “The benefits of bypassing PLCs and DCSs are complete autonomy and flexibility. Building complex multi-dimensional structures and control algorithms will be simpler and it makes the software easier to develop and data easier to collect and analyze. There’s no longer a need to build data handling software in PLCs and DCS systems to reach its final endpoint. Mobility is another big benefit because you can analyze sensors and instrument from your mobile device.

“However, security is always a concern, even though the same secure layer is
implemented using MQTT, and extra caution and design consideration need to be reviewed. At first, troubleshooting can be slightly more challenging because there’s no direct path to a device. Also, trying to diagnose the origin of sensors belonging to devices requires better tools and methods to determine root causes. These tools include better analytics and learning algorithms to model multi-dimensional problems.”

CLOUD REACHES DOWN
Just as field devices and plant applications are seeking simpler paths up to the enterprise, some cloud services and IIoT platforms are exploring top-down ways to access data from those components that may not include the usual control infrastructure.

Likewise, Honeywell Process Solutions (HPS) recently launched its Connected Plant program, which combines the domain knowledge of its UOP division with its own partner network and other capabilities. Paul Bonner, vice president of consulting and data analytics at HPS, reports that Honeywell Connected Plant improves users’ production efficiency and process reliability and optimizes their supply chains by augmented their process knowledge with OEM equipment analytics. The program also relies on Honeywell’s Sentience
Cloud, which is based on Microsoft Azure cloud-computing service. Field and plant devices deliver data to IIoT components that relay it via wireless to Sentience Cloud, which distributes it to analytics, modeling, asset management and other software tools, and to partners in Honeywell’s INspire joint innovation program. All of this is done without disturbing existing DCS and MES infrastructures, which can also report to Sentience Cloud via a firewall (Figure 3).

“Analyzing plant performance with a cloud-based service enables round-the-clock monitoring of plant data and rigorous simulations; provides ongoing, operational recommendations to close performance gaps; and employs UOP’s process models and experience in operational support and troubleshooting,” says Bonner. “The customer value of this is 30-50 cents per barrel in refining and $10-20 per metric ton in petrochemicals.”

ITG’s Ferrante adds, “The development of alternate paths will evolve to other alternate networks, such as mesh-canopy networks, Wi-Fi and cellular networks. In addition to sensors and control data, video and textual data will be combined to build even more complex models to decrease downtime and improve operations. The concept of smart virtual operators will replace the traditional operator as we know it, reducing the need for manual labor and people required to operate manufacturing facilities.”
Kepware’s industry-leading industrial connectivity solution provides:

- **A Scalable and Flexible Architecture**
  with connectivity to hundreds of protocols covering a wide range of PLCs, RTUs, flow computers, sensors, databases, custom applications and other industrial data sources.

- **Streamlined and Reliable Data Access**
  for HMI/SCADA, MES, Historian, ERP, custom applications and industrial IoT platforms, including ThingWorx®.

- **Increased Visibility**
  into industrial data—so everyone from the shop floor to the top floor can make smarter decisions.

Learn more at [www.kepware.com/CG](http://www.kepware.com/CG)
Maybe it’s because it’s mostly invisible, but wireless networking in process control isn’t getting the attention and respect it deserves.

Wireless may be intangible, but it’s not insubstantial because it’s holding up the capabilities and operations of a large part of today’s industrial networks, extending the reach of Ethernet, and enabling cloud-based computing services, the Industrial Internet of Things (IIoT) and other forms of digitalization. Pretty heavy lifting for a technology that seems to have no substance.

However, just like “computing,” “software,” “networking” and other all-pervasive technical shifts that are so huge that they impact everything, wireless may also be reaching a level of success where it’s everywhere.

Ironically, like the other big topics, this is the point where it also becomes seamless, gradually taken for granted, and fades into the technological background. Before it does, however, it might be good to get a little refresher on what wireless can do and how to apply it properly.

“The base of the IIoT pyramid is all wireless,” says Bob Karshnia, vice president and general manager of the wireless division at Emerson Automation Solutions (www.emerson.com). “The IIoT couldn’t happen without wireless, but wireless is also adapting in many ways, too. The key to it all is data, and transforming it into actionable information that can improve operations and impact key performance indicators (KPIs). The next level for wireless is going beyond monitoring to improve reliability,
safety and plant performance, perhaps by using our Plantweb Insight software, which has app-like tools and is like a Fitbit for process controls.”

BRING IN THE FIELD
While the word “wireless” logically suggests an absence of copper or at least less cabling, the potential savings weren’t enough to get wireless to critical mass. What did push wireless over the top and enable it to “go viral” was that it allowed users to reach places and gather signals they could never get before.

For instance, Linn Energy (www.linnenergy.com) operates about 1,500 oil and gas wells in the San Joaquin Valley near Bakersfield, Calif., but it also runs a steam flood field, where steam is injected to provide pressure to force oil and gas out of the wells. Unlike fracking, this process doesn’t use high-pressure liquid to fracture rock formations. The resulting water in Linn’s process is treated to meet U.S. Environmental Protection Agency (EPA) standards, and injected back into an underground reservoir via more than 20 water-disposal wells. Water injection rates and totals are carefully monitored to meet EPA requirements and optimize disposal well performance. Surface or injection pressure is also monitored to meet EPA and safety requirements. Periodically, these wells need to be cleaned using a process called well-bore cleanout, but it’s difficult to determine precisely when to do these cleanouts.

Josh Hernandez, senior product engineer at Emerson, reports Linn recently installed wireless pressure and totalizing transmitters on 15 water disposal wells, which helped it monitor productivity, eliminate unnecessary cleanouts, and save $150,000 in one year with similar savings expected in the future (Figure 1). “Savings were also realized because Linn Energy determined that fewer new disposal wells were required,” says Hernandez.

To reach this happy ending, Linn needed a better way to find out what was happening in its disposal wells, which are located about 500 feet apart. “The wells vary in depth, length of perforations and other parameters, and well performance is indicated by the volume of water injected per foot of perforations,” explained Hernandez. “Linn
wants to maximize this value because it’s closely related to total injected volume of water, which indicates well productivity.”

Previously, Linn personnel made daily manual rounds to read local chart recorders showing water flow into the wells, and read local gauges measuring surface pressure. However, because well operations and measurements change hourly, these rounds weren’t sufficient to optimize cleaning or determine when to drill new water disposal wells. Clearly, Linn needed online monitoring and trending of key parameters, and due to the wells’ remote location, battery-powered wireless transmitters were the most sensible choice.

“Many devices already integrate wireless like WiFi, cellular and 900-Mhz radios, and more people are willing to try it. So the main driver today is ease of use, and making wireless even quicker and easier to order and install,” says Justin Shade, wireless product marketing lead specialist at Phoenix Contact (www.phoenixcontact.com). “This is also helping remote access become more cost-effective. For example, instead of traveling to do maintenance on a custom-built panel, we added our mGuard VPN appliance and our FL WLAN client device, and diagnosed the panel at the user’s site over a secure VPN connection over the Internet. In fact, we just combined these two devices into a kit, so now our customers can get the security of our mGuard product line with the added flexibility of a reliable WLAN connection under a single part number.”

COORDINATE AND BUILD TRUST

Even though wireless can seem to be ubiquitous, there are still plenty of manufacturing applications where it could be beneficial if users weren’t worried that it would be interrupted like a dropped cell phone call or their residential WiFi. Many system integrators and suppliers report it’s been hard to dispel this prejudice, and convince potential users that industrial wireless is far more reliable than mainstream wireless—as long as its antennas, transmitters and receivers aren’t installed under motors or metal roof soffits.

WIRELESS EXTENDS ADVANCES

Figure 2: MOL Danube Refinery near Budapest in Hungary operates 42 WirelessHART devices and six gateways, which receive signals from 32 devices usually measuring temperature and corrosion. Its wireless projects include implementing an “uptime umbrella” reliability project to equip all key operating units with the plant’s field instrumentation management system (FIMS). Source: MOL Group
“There’s a lot of people that don’t trust wireless,” says Scott McNeil, senior network and security engineer at Global Process Automation (GPA, www.global-business.net), a CSIA-member system integrator in Wilmington, N.C. “They may have devices with WirelessHART protocol, but they won’t add it on their own.”

On the other hand, McNeal adds that preinstallation site surveys also remain essential because some new wireless converts seek to saturate their facilities with wireless, which can eat up air time and capacity, force applications to step on each other, and cause data collisions and drops. “To get users the data they want, role-based access is needed for wireless access based on credentials, so they can only reach what they need. So, while plant managers get access to everything, operators and contractors only get to see the equipment they’re working on.”

McNeal recommends using spectrum analysis to resolve wireless frequency conflicts. “We recently found some microwave dryers for industrial ceramics were running at 2.4 GHz, which was interfering with the local WiFi,” he explained. “This is why a site survey is needed to find local strengths and weaknesses. Once you have them, you can develop a wireless plan that includes identifying control measurements you want, arranging role-based access, and designing signal coverage, antenna placement, access points (AP) or mesh and power delivery. After deploying your hardware and logic—and training users—you need to maintain, monitor and stay secure with wireless intrusion detection like what’s offered by Aruba Networks (www.arubanetworks.com) wireless controllers that can pinpoint unauthorized traffic.”

McNeal added one problem is how to integrate cloud-controlled wireless into manufacturing because if its Internet connection goes down, then its wireless will be lost as well. “In this case, a non-cloud-controlled option would be best,” he said. “Losing wireless in a corporate setting might be acceptable, but it could cause financial losses and life safety issues on the plant floor. In general, wireless has been through the wringer and proved itself. The cloud and its security still needs to be proven.”

Bert Williams, global marketing director for ABB Wireless (http://new.abb.com), adds, “It’s important to remember that one ‘I’ in IIoT stands for ‘Internet,’ and one way to communicate over the Internet is wireless. Many of the tools used for years on the IT and enterprise side can be applied to field networks including wireless. The question is how to scale up for IIoT applications. We can control wireless communication network management systems with our Supros solution, which offers fault, configuration, administration, performance, security (FCAPS) management.”
“It’s important to remember that one ‘I’ in IIoT stands for ‘Internet,’ and one way to communicate over the Internet is wireless.”

**MONITOR AND MANAGE**

Even if a process facility is way ahead on the learning curve, it can still benefit from wireless. For example, MOL Danube Refinery (https://molgroup.info/en) near Budapest is the only two-time winner of FieldComm Group’s (FCG, www.fieldcommgroup.org) Plant of the Year Award for all its optimization efforts and performance gains over the past 15 years, but it recently started using wireless to achieve even more gains (Figure 2).

Overall, MOL Danube has a total of 40,000 instruments, including 30,000 with HART 4-20 mA, 8,000 with pneumatic and standard 4-20 mA, and 2,000 with Foundation fieldbus. As the only Hungarian MOL refinery conducting crude distillation since 2001, MOL Danube capacity is 8.1 million tonnes per annum (mtpa) with a 10.6 Nelson complexity index (NCI) ratio.

More recently, it pushed its use of FieldComm technologies up to 3,680 HART devices, 413 Foundation fieldbus devices, and 42 WirelessHART devices and six gateways, which receive signals from 32 devices, usually measuring temperature and corrosion. Gábor Bereznai, head of maintenance engineering at MOL Danube, and his cohorts are also planning to adopt HART-Internet protocol (IP) with their OSIsoft PI historian and software. This adds about 4,700 intelligent instruments on the 15 critical units connected to the SAP-PM computerized maintenance management system (CMMS).

MOL Danube’s wireless projects include improving its WirelessHART and other wireless systems, and implementing an “uptime umbrella” reliability project to equip all key operating units with the plant’s field instrumentation management system (FIMS), which includes revamping I/O interfaces, installing WirelessHART adapters, and replacing obsolete control valve positioners. Bereznai adds that MOL is also committed to using WirelessHART for corrosion control, instrument asset diagnostics, furnace wall temperature measurement and heat exchanger performance monitoring.

“We found it was hard to justify the cost benefits of just one to three wireless PV
transmitters, but the real benefits come from mid-sized projects,” explains Bereznai. “Wireless also requires different design approaches.”

Similarly, ARC Resources Ltd. (www.arcresources.com) in Calgary, Alberta, Canada, recently sought to streamline operations and minimize cabinet space on a large, multi-well pad site in Dawson Creek, B.C. (Figure 3) The pad had a ControlLogix PLC from Rockwell Automation (www.rockwellautomation.com) and standalone flow computers metering natural gas, but each device could only handle an eight-meter run, and this wasn’t sufficient for real-time data flows and future expansion.

Consequently, ARC decided to adopt Enhanced Flow Computers from ProSoft Technology (www.prosoft-technology.com) that freed up enclosure space, reduced wiring, improved data integration, required fewer computers, and didn’t have license fees.

“With this solution, we’re able to do 16 meter runs per flow computer, limiting the units we need,” says Charlie Kettner, programming specialist at ARC Resources. “We also like that the system can be expanded later if we need more meter runs.”

DATA FROM THE DESERT

Back at its water-disposal wells near Bakersfield, Linn Energy implemented 15 Rosemount 3051S wireless pressure transmitters on existing manifolds to monitor the surface pressure, or the injection pressure, of each well.

To receive the signals, Linn installed one Emerson WirelessHART gateway, which was aided by three high-gain antennas due to the distances of some wells. The field gateway communicates to a base station gateway, which is also integrated with the facility’s Rockwell Automation control system via EtherNet/IP. Next, 15 Rosemount 705 wireless totalizing transmitters were installed on the wells’ existing turbine meters to measure injection rates and totalized values of injection water.

“Within minutes of installation, the 3051S transmitters began transmitting data to the control system, while the 705 wireless totalizers started talking to the control system in about five minutes,” adds Hernandez. “Emerson assisted with the next 14 wells, and the total installation and startup time was 10 minutes per well.”

The wireless transmitters provide continuous data to optimize Linn’s PC-based well performance model. The data is used to calculate an “injectivity index,” which is a function of surface or injection pressure, injection rate and perforations per foot.

Linn improved its well-bore cleanout process by trending the surface or injection pressure.
pressure at each water-disposal well to detect stoppages, which was better than relying on single daily measurements. Because well-bore cleanout is expensive and time-consuming, the company estimates it saves $10,000 each time it avoids an unnecessary cleanout. It adds that it saved at least one cleanout a year for each of the 15 wells, which adds up to $150,000 in total savings.

“This success has led to four more water disposal wells being monitored since the initial installation, and more are planned,” adds Hernandez.
The plant had determined that monitoring the bleed line of a double-block-and-bleed isolation assembly would easily reveal whether either of the block valves were leaking. Since this was a key to validating the effectiveness of the isolation system, Sandra, the new instrument specialist, was tasked with bringing these points into the DCS. Problem was, there were 50 new temperatures to monitor.

For this back-of-the-envelope comparison, Sandra made a few assumptions. The cost of sensors was assumed to be the same, whether they were connecting to HART, WirelessHART or fieldbus. Sandra included the labor and material to bring the necessary signals to the host system, but made no attempt to compare incremental host I/O infrastructure—the cost of serial I/O or a Modbus TCP card is not a deal breaker compared to Foundation Fieldbus (FF) H1 or Profibus cards.

To get a generic quote for hardware pricing—no special discounting—Sandra used the “Rosemount Online Store” for the transmitters and Allied Electronics for as much of the bulk hardware as she could find there (cable, conduit, terminals, junction boxes, and so on).

For the HART 4-20 mA transmitters, Sandra priced the single-input 248. The Rosemount Online Store prices 50 at about $33,000. The wireless version of the 248 came in at over $83,000 for 50, so instead she opted for quantity 13 of the four-sensor 848TX, saving about $15,000. This choice makes...
wiring of sensors a little more complex, since the 248’s could have been mounted integrally to each sensor.

But it was comparable to the fieldbus option, which uses the eight-input fieldbus 848T. The FF option reduces transmitter hardware cost to only $24,000 for quantity 7. After adding batteries and a gateway, Sandra wonders whether the wireless option will pay for the $37,000 premium relative to wired HART, and nearly $45,000 compared to wired fieldbus, for her 50-point project.

Copper prices are volatile and sometimes cable prices can fluctuate weekly, but when Sandra searches the web for 12-pair, individually shielded, Div. 2- and tray-rated cable, she finds it for about $2 per foot (ca. $1,000 (list) per 500 ft. on Allied). To span the 700 ft. to each field junction box, she’ll need (5) 12-pair cables for the HART solution, or about $7,000 in multi-pair home run cables – and maybe, say, $10,000 to cover waste and rework. From the junction box to devices, Sandra budgets for 16 AWG twisted, shielded pairs—at $0.33 per foot, she figures another $1,000 for 3,000 ft.

The question becomes, with prevailing labor rates, how much conduit, wire and terminations will the remaining $25,000 buy before the wireless option begins to pay out? Setting aside $15,000 for conduit, supports, tools and equipment, there’s only $10,000 left for labor. In Sandra’s area, that only gets her two electricians for about two weeks. You might see the scale tipping distinctly toward the wireless approach.

But fieldbus came in very competitive. Cable is $0.99 per foot (list), and Sandra only needs 2,000 ft. for the whole job. She finds modular Phoenix junction boxes, power supplies, and device couplers online for less than $1,500 total for seven spurs and a home run. The remaining difference in cost to the 13 wireless transmitters—about $40,000—is more than enough for the relatively light infrastructure for single-pair
cable. Labor costs would need to be astronomical and productivity dismal before wireless breaks even.

For this case, fieldbus wins. But wireless often wins not because it’s cheaper, but because it’s easier. Errors and shabby workmanship have had an unfortunate impact on some early fieldbus installations, where a loose termination or a compromised transmitter case can impact the reliability of an entire segment. There’s incremental engineering—some might over-analyze and obsess about segment loading, but the same folks might also invest in overzealous wireless site evaluations.

Sometimes wireless is a slam-dunk. Next month’s column will continue the discussion of paths to pervasive networking, and when the choices—despite costs—are more obvious.
Build those firewalls
Why and how to secure industrial control and safety systems at every conduit.
By William Mostia, Jr., P.E.

Cybersecurity is all the rage now with everyone wondering if someone is peeking under their petticoats or will hack their control system and take over their process, a la Stuxnet, leading to a disaster. This is an important issue that requires a careful approach of engineering analysis and design to keep the barbarians at the gate and out of our kingdom. IT networks are being subjected to an increased level of cyber threats, and all the pundits are predicting that industrial control systems (ICS) are next, with a good dose of doom and gloom. When the corporate or enterprise IT network is connected (directly or indirectly through the plant network) to ICS network and/or potential sneak-path connections to the Internet, cyber threats have doorways to attempt to open and possibly penetrate the ICS to do no good.

Firewalls play an important role in blocking and containing external and internal cyber threats that could impact process control system availability, reliability and productivity, and potentially impact safety. The selection of firewalls, their locations and the protection they provide should be part of a holistic cybersecurity assessment and protection plan based on a risk-based assessment and good engineering practice.

The topic of firewalls is surprisingly complex, and requires a good amount of study to be competent in their application and support. The intent of this article is to discuss some of the basics of applying firewalls in ICS systems by looking at them from the perspective of the functional data flow in the industrial control system, without too much technical IT geek-speak.
The world of the industrial control system is a substantially different world than your standard IT environment, and has given birth to a brand-new buzzword and acronym—operational technology (OT). ICS and firewalls fall into the OT realm. The types of digital transactions in an ICS are substantially limited when compared to general-purpose IT computer networks. The ICS is purpose-built to transfer a limited range of data types and functions, such as measurements, setpoints, status, alarms,

**ZONES AND CONDUITS**

Figure 1: The enterprise or corporate system zone (Level 4) is connected to the plant computer network system (called the Plant DMZ, Level 3), which is usually a general-purpose computer network and is typically connected through an IT firewall to the enterprise system. Level 3 is connected to the basic process control system (BPCS, Level 2), typically through a specialized firewall or security appliance, which is later connected to the safety instrumented system (SIS, Level 2), again through a specialized firewall or security appliance. If the ICS is large enough or has separate functional areas (e.g. PLCs or process areas), there may be more defined zones with specialized firewall or security appliances.
calculated values, control signals, etc. Some configuration and programming is also done across the ICS network via engineering workstations. While there is typically an Internet connection to the plant network, or possibly indirectly through the enterprise network, there should not be any direct, continuous connection of the ICS network to the Internet, even through a firewall. However, there may have to be temporary connections to the Internet to download software updates and patches, which should be always be done through a firewall, and special care must be taken when doing so to control the transfer to ensure that a cyber threat does not sneak in.

STANDARDS AND LAYERS
ISA (www.isa.org) is aware of the issues and hazards of cyber threats to ICSs, and commissioned the ISA 99 committee in 2002 to address the issue of cybersecurity in industrial automation and control systems (IACS/ICS). This committee’s goal was to develop a series of standards and technical reports to address the issue of cybersecurity in IACSs/ICSs. This standard committee’s work later became known as the ANSI/ISA-99 standards, and in 2010 was harmonized with the International Electrotechnical Commission (www.iec.ch) and became ISA/IEC-62443, “Network and system security for industrial-process measurement and control.”

One of the methods in the technical report ANSI/ISA/TR99-2007 to fight cybersecurity intrusions is through the use of zones and conduits. The basic idea is to divide the ICS and connected systems into smaller functional chunks, e.g. zones, to provide isolation from each other, and to provide defense-in-depth capability. A communication “conduit” would be provided between zones, which allows a zone to communicate to another connected zone. At each conduit, there is essentially a doorway that controls the digital transactions in and out of a zone. This transaction control is commonly performed by a firewall or a data diode (hardware-enforced
unidirectional gateway). The concept of protection by zones and conduits is illustrated in Figure 1 for a chemical plant-type environment. Also note that the ICS in Level 2 is divided into the basic process control system (BPCS), which includes the human-machine interface (HMI), and the safety instrumented system (SIS). Level 1 consists of the field instruments for the SIS and BPCS.

From Figure 1, we can see that the enterprise or corporate system zone (Level 4) is connected to the plant computer network system (called the plant DMZ, Level 3), which is usually a general-purpose computer network, and is typically connected through a stateful-type IT firewall (https://en.wikipedia.org/wiki/Stateful_firewall) to the enterprise system. The plant DMZ (Level 3) is connected to the ICS (BPCS, Level 2) typically through a specialized firewall or security appliance (a term used by some manufacturers to differentiate their product), which is later connected to the SIS (Level 2), again through a specialized firewall or security appliance. If the ICS is large enough or has separate functional areas (e.g. PLCs or process areas), there may be more defined zones with specialized firewall or security appliances.

SCADA systems can have different zones and conduits due to their geographical distribution of components and control functions. It’s typical to have a stateful firewall at the central control center connection to the enterprise network. A specialized firewall or security appliance should be in place between the central control center and distributed control locations (typically RTU sites), and a specialized firewall or security appliance firewall at each control location. Firewalls are required at both ends because of the geographical distribution; a cyber threat attack may backdoor into the control center from one of the control locations. Depending on the design, there may or may not be separate SIS zones.
IT VS. ICS NETWORKS

Computers in networks perform digital transactions to accomplish tasks. Plant networks are typically Ethernet-based over fiber, and commonly connected to the outside world via a connection to the Internet. They are the realm of the IT department, but there’s an overlap where they connect to the ICS. While it may go against the grain of many control engineers to associate with IT personnel, for the sake of cybersecurity, making a friend with your local (hopefully friendly) IT guy is a good idea. Maintaining these networks against cyber threats requires quite a bit of work and skill, so all the help you can get will be good in the long run.

The enterprise network (Level 4) and the plant DMZ network (Level 3) are typically IT networks, and they’ll have a firewall at the system connection to the Internet as well as to each other and any other connected network. General-purpose IT firewalls are unsuitable for ICSs because they’re essentially packet filters with some smarts. They generally can’t distinguish at the application level which ICS data transactions/traffic packets to explicitly allow, and can let packets through without knowing if what they contain may be hazardous to our ICS. Smart hackers are always looking for and finding vulnerabilities to access these networks, which can lead to a cyber threat penetration into the ICS.

IT isn’t typically the recommended department to control ICS firewalls because they typically don’t understand what goes on in the ICS. IT personnel should be knowledgeable about IT firewalls, and the control engineer can define the allowable control system transactions that should pass through the IT firewalls, but control of the ICS firewalls should be in the control engineering department with the assistance of the IT department. Physical access to the ICS firewalls should be controlled, all firewall passwords should
be changed from their default, and each firewall should have a different password.

**BETWEEN THE DMZ AND BPCS**

The first step to designing a firewall system for an ICS is to determine your zones and define the conduits where you’ll locate firewalls based on the defense-in-depth concept. You must also determine what type of data transaction that you’ll allow across the firewalls (read, writes, program/configure, etc.) and what risks are associated with allowing these transactions. This requires engineering analysis and a risk assessment for allowing these transactions.

A key rule for ICS firewalls is that they should be configured by default to deny all transaction traffic except that which is explicitly authorized.

There should be only one access point between the ICS network and plant DMZ network—the ICS should be analyzed for other potential access points, including thumb/memory stick drives, and these access ports should be closed. The corporate or enterprise system should not connect directly to the ICS because this would eliminate the layer of protection of the plant DMZ/enterprise firewalls.

At the interface between the plant DMZ and the BPCS, a decision must be made as to what control system transactions are going to be allowed across the firewall. The location of the data historian can affect this if the enterprise system collects data from it. Remember, we wish to only allow data transactions that are explicitly authorized (necessary), and we also need to control who is authorized to use these data transactions.

Whitelisting, which specifies who or what can talk across the firewall, should be used rather than blacklisting, which is who should not be allowed to talk. Blacklisting is limited to those who you know should not be allowed to talk across the firewall. However, blacklisting does not help you when someone who you don’t know wants to talk for nefarious purposes, which is the case for many cyber threats. Whitelisting should follow the rule that if a system or user doesn’t need to communicate with a system, it should not be allowed. Blanket access should not be allowed.

The data transaction choices are typically reads, writes, programming access, and remote control access. The recommended transaction is to allow only “read-only” transactions. This should limit your risk from a cyber threat to vulnerabilities of the firewall itself, such as denial of service, buffer overflow, etc. This can be done with a data diode (unidirectional data flow) or a firewall with deep packet inspection (DPI) that only allows reads.

Unfortunately, allowing access by engineers via desktop or laptop from their offices due
to safety concerns (limiting personnel inside the plant battery limits) and/or convenience sometimes overrides cybersecurity concerns. Programming or remote-control access should not be allowed from the plant DMZ network to the ICS network. The consequence of a reprogramming of the control system or SIS cyber event, if it occurs, could be a potential disaster. If you must allow other types of access besides reads, a risk assessment should be done, and adequate cyber protection be added to the firewall for the access allowed. Knowing what transactions flow and where within the BPCS and SIS is important for locating and configuring the firewall, and a transaction map can be a good conceptual tool to locate and determine what authorized transactions will be allowed to be passed by the firewall.


Many firewalls that also have network intrusion detection and prevention systems and antivirus scanning are very useful features for control system networks—so long as they don’t interfere with control system availability and performance. When purchasing firewalls, in addition to a detailed technical review, you should request to look at all the firewall’s engineering change orders (ECO) to determine what vulnerabilities have been detected and fixed. A lot of fixes or patches can indicate a weak design.

BETWEEN THE BPCS AND SIS
The other minimum required firewall is between the BPCS and the SIS. To assure independence of the SIS from the BPCS, permitted firewall transactions should be limited and strictly enforced. The SIS engineer should be involved in configuring and supporting this firewall.

The best system from a cybersecurity perspective would be to have non-programmable SISs with read access only by the BPCS. A second option is to air-gap the SIS and have a separate HMI for the safety instrumented functions (SIF) that’s not connected to main control system network, the plant DMZ or the Internet. This type of SIS typically would still require a firewall between the HMI and the SIS, but the SIS is isolated from the main control network. However, the separate HMI adds different HMI hardware and software that have to be supported, and it’s not typically in line with most people’s HMI philosophy today.
Most BPCSs today will have a digital connection that will be used to interface the BPCS with the SIS logic solver. It’s still good engineering practice to isolate the SIS from the BPCS as much as possible to prevent simultaneous control of these systems by a cyber threat. Had this isolation existed between the control system and the safety system during the Stuxnet event, it might have turned out quite differently.

The best digital option is to allow only reads and no programming or configuring through the firewall from the BPCS control network to the SIS. Allowing programming over the process control network to the SIS exposes the SIS to unauthorized program changes and potential defeat of the SIS safety function by a cyber threat. Changing the operating mode of the SIS logic solver or any PLC from the BPCS also should not be authorized. For example, a Modbus firewall between BPCS and SIS should be designed specifically for Modbus, and limit the acceptable commands to Modbus Function Codes 01–04 (read function codes) to gather necessary read data from the SIS logic solver (e.g. SIS transmitter measurements, valve positions, SIF status, etc.) Any required writes to the SIS should be hard-wired via a BPCS digital output or analog 4-20 mA to the SIS. If writes are allowed through the firewall, as a minimum, they should be from a recognized source, go to specific registers in the SIS logic solver, and be within an acceptable range of values.

Due to evolution and competition, we have four basic SIS system designs:
1. Relay logic or trip-amp-based non-programmable (SIS-TECH);
2. Diverse design technology by separate manufacturers (Triconex, A-B, Rockwell Automation);
3. Partially integrated, but different technology SIS (Emerson, Honeywell); and
4. Fully integrated SIS (ABB).

Design 1 typically is interfaced to the BPCS hardwired or via Modbus (inherently read only); Design 2 commonly uses Modbus or a recognized proprietary protocol (e.g. A-B DH+) and should have a purpose-built firewall for that protocol that allows only certain types of transactions, and should allow access only to specific registers;

Designs 3 and 4 should use a firewall from the SIS manufacturer or recommended by the manufacturer. A number of manufacturers have licensed Tofino DPI technology (https://www.tofinosecurity.com) for their firewalls (MTL, Honeywell, Triconex).

The more integrated the SIS, the more vulnerability it has to a common cyber threat penetration into the BPCS that could also get into the SIS. Connecting Ethernet directly to a SIS is not recommended, and if done, should only be done with a risk assessment, through a manufacturer-recommended firewall, and use DPI technology or equivalent. Get the manufacturers involved early, and get their insights.
into their systems and their cybersecurity recommendations.

Level 1 is where the field instruments interface with the process and do the actual work. Many of these are connected to the BPCS controllers and PLCs in Level 2 via analog or discrete digital signals, and don’t require firewall protection, but an increasing number use fieldbus or some other digital communication protocol (e.g. motor or electrical protection relay com links). The potential vulnerabilities here must be risk-assessed and protected against.

ICS AND SIS FIREWALLS
Because the ICS will typically run a proprietary operating system and network protocol, ICS firewalls must be purpose-built for that protocol and specifically designed for ICS and SIS service. These firewalls should not have any extra ports that might be open to a cyberattack, and should not allow general computer transactions (Internet, e-mail, access to server-based programs, etc.) ICS and SIS firewalls should use DPI, similar firewall technology or a data diode to control data flow. DPI is an advanced packet filter method that examines the data or payload of the transaction in the application context as it passes into an inspection point, searching using defined criteria to decide whether the packet may pass. DPI functions at the application layer of the Open Systems Interconnect (OSI) seven-layer model (https://en.wikipedia.org/wiki/OSI_model). Data diodes are less common than firewalls and are different from them because they only allow hardware-enforced data transfer one way, no exceptions, and can be used to create a read-only interface.

Ethernet is a common transport protocol in ICS. In addition to normal, safe transactions, it can transport a range of hazardous payloads using general-purpose communication protocols, making it inherently more risky than proprietary protocols due its generic nature. If the ICS or SIS firewall is on an Ethernet-based control network, HTTP and other general-purpose computer traffic not specifically related the control functionality should be explicitly forbidden. This is to prevent computer malware and viruses from tunneling into the ICS and SIS. Unfortunately, the proprietary protocols are disappearing, along with purpose-built human machine interfaces (HMI). Typically to financial considerations, they’re giving way to HMIs on Microsoft Windows-based PCs, which many times use some form of Ethernet, opening more potential doors for hackers to infest your control systems. These types of HMIs should be reviewed to see if it’s appropriate to have additional firewall protection on them.

William Mostia, Jr., P.E., is a frequent contributor to Control.
IT, OT unite during gas network upgrade

When the FBI identified unauthorized monitoring of one of its SQL systems several years ago, Washington Gas began working with the FBI and the U.S. Department of Homeland Security (DHS) to redesign its data infrastructure.

By Jim Montague

Washington Gas (www.washingtongas.com) is a local delivery company that provides natural gas via a 300-square-mile network of high-pressure lines to more than 1 million residential and commercial customers in Washington, D.C., and surrounding communities. This transmission network traditionally used microwave rings as its data backbone, along with stationary and mobile radios, to deliver pressure and other readings. The network, which includes a 300-psi line under the National Mall, also employs pneumatic backup controllers in case any electronics or PLCs fail, and they’re monitored by a parallel, Verizon-based alarm management system from tattletale (www.tattletale.com), which queries standalone devices and produces reports.

However, when the FBI identified unauthorized monitoring of one of its SQL systems several years ago, Washington Gas began working with the FBI and the U.S. Department of Homeland Security (DHS) to redesign its data infrastructure, according to Craig Lightner, automation and control manager at Washington Gas, who spoke at the ARC Industry Forum 2017 in Orlando. “We previously had a standard, corporate IT environment with servers, apps and authentication to an active directory, while the plant had a separate, standalone system,” says Lightner. “So, with DHS help, we built a new infrastructure with multiple demilitarized zones (DMZ) between each network layer, and put improved security polices and procedures in place. For us, this was also a good example of a successful IT/OT convergence.”
Though it provides natural gas and not electricity, Lightner adds that Washington Gas was also guided by the North American Electric Reliability Corp. (www.nerc.com) Critical Infrastructure Protection (NERC CIP) standards. “If taken to heart, NERC CIP is a method for process control system security, and we took it to heart,” explains Lightner. “I think the American Gas Association (www.aga.org) will be coming out with similar best practices soon.”

Beyond following standards, Washington Gas also adopted IT-based, managed security services from SecureWorks (www.secureworks.com). “It streams all our network traffic, loss-of-service and other data; analyzes it to find intrusions, bad actors and resources that are out; and lets us know in 15 minutes if anything is happening, such as suspicious traffic, unauthorized logins, attempted intrusions or malware. After examining our traffic for three weeks, it can identify what’s regular and what’s new.” In addition, the utility’s networked equipment also communicates outward through data diodes that don’t allow any data or other communications to come back in.

“Related to our IT/OT convergence, we learned it was part of our cybersecurity journey, which isn’t going to end,” adds Lightner. “We can secure our network as best we can and keep it up to date, but we’re going to have to keep doing analytics on our disparate data sources, including process inputs, phones, radios and video feeds. There are different types of communication, such as operations reporting that pressure is down or residents reporting that they smell gas, but where these sources have been separate, we’re saying they should all be unified so we can get alerts sooner and respond more quickly. In fact, we’re working on reducing our situation identification time from 15 or 20 minutes down to three minutes.”