

CONTROL

PROMOTING EXCELLENCE IN PROCESS AUTOMATION CONTROLGLOBAL.COM

Industrial IoT

Orientalmotor

α STEP AZ Series

Hybrid Control Systems

Open loop
performance.

Closed loop
control.



Now With

EtherNet/IP™

α STEP AZ Series Family of Products



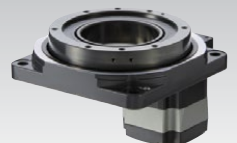
Rack & Pinion Systems



Compact Electric Cylinders



Electric Actuators



Rotary Actuators

Providing Innovative Motion Control Solutions Since 1885

570 Alaska Avenue • Torrance, CA 90503 • Tel: 800-468-3982 • sales@orientalmotor.com

www.orientalmotor.com

EtherNet/IP is a registered trademark of ODVA, Inc.



TABLE OF CONTENTS

Get into the IIoT mindset	5
IIoT requires users to shift their personal perspectives	
Evolving network architectures	7
IIoT and cloud computing are changing our view of the venerable Purdue model	
Smooth the road to IIoT	10
Common methods and best practices for the Industrial Internet of Things start to solidify	
Primary IIoT players	20
A guide to major components of the Industrial Internet of Things	

AD INDEX

Acromag • www.acromag.com/xt	4
Oriental Motor • www.orientalmotor.com	2

Going the Distance with Remote Ethernet I/O

Industrial-Strength Ethernet I/O with High-Density Efficiency



Acromag's Ethernet I/O Modules are ideal for SCADA, IIoT and remote monitoring or control applications. These rugged modules provide a very cost-effective and highly dependable solution to interface sensors, actuators, relays, instruments, and other devices to an ethernet-based control system.

Acromag Advantages

- High-channel density for very cost-effective solutions
- Ethernet/IP, Profinet, Modbus TCP/IP, or peer-to-peer communication
- Easy configuration via USB/Windows or built-in web server
- Dual Ethernet ports for daisy chain connections
- Counter, integrator and totalizer functions

Rock-Solid Reliability

- High-voltage isolation and surge protection dissipate harmful signals
- Redundant power and communication prevent costly downtime
- -40 to 85°C operation and Class 1 Div 2 hazloc approvals and ATEX certification

 Visit www.Acromag.com/XT
TO LEARN MORE

Get into the IIoT mindset

IIoT requires users to shift their personal perspectives

By Jim Montague



Gaining operational benefits from the Industrial Internet of Things (IIoT) requires more than adding components and common protocols—it also requires users to shift their personal perspectives.

“IIoT isn’t a switch that’s turned on and off or a magical gemstone that’s achieved because it evolves over time,” says Chris Hamilton, industrial information technology/operations technology (IT/OT) director at Grantek Systems Integration (<https://grantek.com>), a CSIA-certified system integrator (SI) in Burlington, Ontario, Canada. “IIoT still requires users to look at what they’re doing because they’re already using Internet technologies whether they know it or not. Now, they need to consciously pick the concepts they

need, get comfortable with them, evaluate areas where they can do better with IIoT, expand where possible, and add policy and governance where needed.”

Hamilton reports that when the Internet and web first gained momentum in the 1990s, it took too many clicks to get from place to place online, but this eventually gave way to more seamless websites and better user experiences (UX) in the 2000s. “My big push is for a better UX, which includes asking why users have to go through six button clicks to get somewhere, especially when Google emphasizes requiring only two clicks,” he says.

To improve Internet UX for clients, their systems and their customers, Grantek strives to implement each user’s particular

“I like it when two standards disagree because it’s an opportunity to learn, take the best parts of both, and get to more overall improvement,” says Hamilton.

version of IIoT, so it will be the most suitable for them and their processes and goals. “System integration is still about getting a project done, so we have to shift from tinkering with the Internet to becoming specialists who can design IIoT systems that will be touched by hundreds of users,” adds Hamilton.

This journey to fewer clicks and more effective IIoT means examining all the standard practices that clients and their customers are already using online. “I like it when two standards disagree because it’s an opportunity to learn, take the best parts of both, and get to more overall improvement,” says Hamilton. “Grantek uses industry best practices from companies like Rockwell Automation, Cisco and Siemens for network design. However, clients often have other kinds of systems in place, so they need to be evaluated using a network maturity model, such as Panduit’s. Once they have a plan for their future structure, they don’t need to guess about their network or IIoT anymore. They can tell their OEMs and SIs what they need and how to do it, such as establishing logical segregation and firewalls for a VLAN or setting up remote access.”

Hamilton reports SIs and clients can find the right network and IIoT balance by “embracing their connected future,” planning for it based on their overall business goals, using these goals to help IT and OT reconcile their different priorities, and absorb each other’s skills. “OT knows how to keep operations running, but IT often has to be available 24/7/365, too,” he says. “OT can leverage the IT world, but it can’t burden IT financially without getting IT approvals that are planned and budgeted. This means OT must shift from doing tasks at the last minute that are often costly, and showing the ROI and risk avoidance that help get capital funding.”

To develop standard IIoT policies and procedures, Hamilton adds that companies need to work with individuals and organizations that know both sides of the OT and IT fence, and can talk about controls, finances and IT. “This requires really listening to groups on the other side, learning what they’re trying to accomplish and what they need, finding commonalities, and working through differences. It sounds touchy feely, but it works. At the root, we have to listen and learn about others’ requirements, so we can provide the best solutions to help our clients grow.”

Evolving network architectures

IIoT and cloud computing are changing our view of the venerable Purdue model

By Ian Verhappen

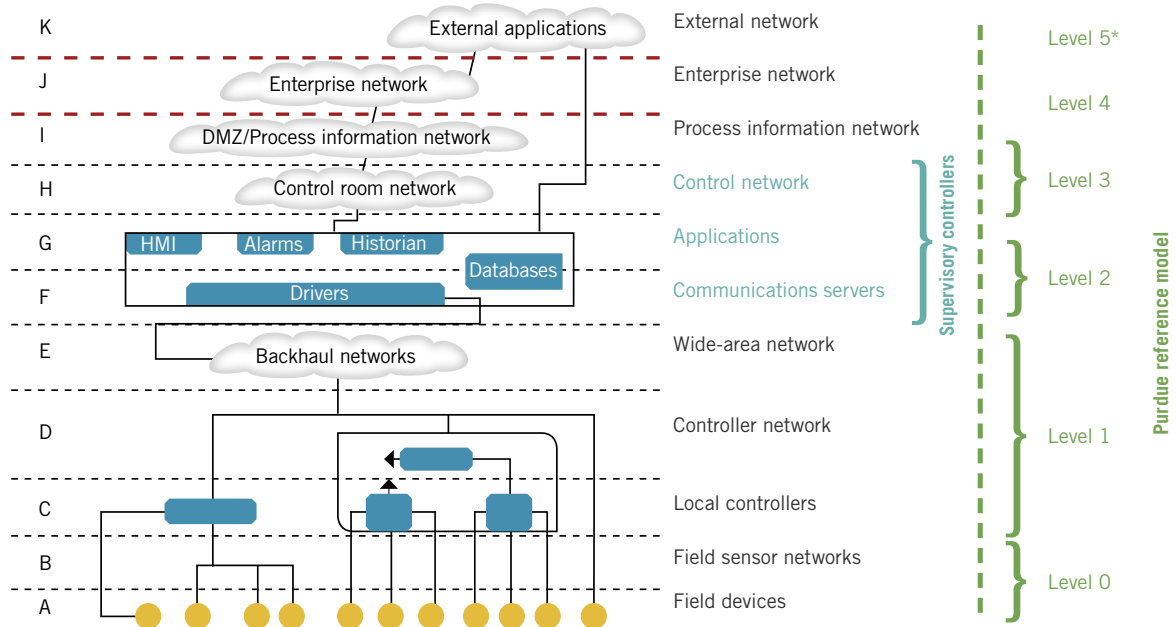


The Purdue Enterprise Reference Architecture incorporated in the ISA-95/IEC 62264 standard, on which the majority of control system architectures and subsequent standards including wireless, cybersecurity, safety, etc. are based, originated in 1989. Despite being in use for almost 30 years, many people still believe it's based on physical layers, when it actually defines the functions to be performed at each level of the architecture. At the time the model was developed, and in most cases today, it's still true that form follows function, and the various pieces of hardware tend to correlate closely to their assigned function. The IEC 62443/ISA-99 cybersecurity zone and conduit concept also tends to encourage the maintenance and separation of each of the function-based layers.

With the changes in processing and computing capability we've seen at the different levels of the enterprise, particularly Level 1, and the introduction of cloud-based systems, it's my understanding that ISA-95, as part of their regular review of the document, is revisiting the architecture model, with particular emphasis on Level 1 and Level 0.

Another ISA standards body, ISA-112 SCADA Systems (www.isa.org/isa112), also needed an architecture model on which to base their work. The present version of this model, which adds more granularity to the ISA-95 model, is shown here.

When creating this model, ISA-112 deliberately chose to use letters to show the different layers, in part to avoid confusion



SCADA ARCHITECTURE MODEL

In this model by the ISA-112 SCADA Systems standards committee, letters are used to label layers to avoid potential conflict with ISA-95 and other similar models. Routers and firewalls between layers are not shown, nor are other system-specific servers, applications and workstations. Remote-hosted external applications (cloud) could be configured to attach to devices at any level with appropriate firewalls, tunneling and routing.

* Note that although this shows a Purdue level 5, the true Purdue model only has levels 0 to 4 because it did not anticipate external applications.

with the Purdue model (shown for reference on the side) but also to help the committee relate the physical equipment against the function(s) that equipment needs to perform.

In general, layers A through D will tend to be at the remote site, which could be anything from a single point and RTU to a remote compressor or pump station complete with its own “mini” control system with wireless SCADA connections to associated well pads, isolation valves or remote storage facilities, thus making “site n” a

small SCADA system, or at least a data concentration site on its own.

Similarly, levels F and G identify the typical SCADA components that reside on the central SCADA server(s), typically in the main control center. Alarms and Historian have been identified as two typical databases residing at this level, though as indicated by the “database” box on the right, they’re by no means the only ones; they are just the ones that the committee believes require particular attention since, from a SCADA perspective, they will have

The virtualization of systems is changing control system architectures once more, with the biggest impact at the top and again at Level 1.

some unique constraints and items to be considered when developing a system.

The other addition to the proposed SCADA model is the concept of cloud computing, presently shown as the “external applications” cloud at the top. Though a link is only shown to the databases at the SCADA server, there is the potential to link to elements at any level, with, of course, the appropriate cybersecurity protocols.

Lastly, the red lines on either side of level J are intended to show the clear demarcation between the OT (SCADA related systems), IT and public or external networks as a reminder to pay particular attention to the cyber requirements when crossing between different layers and systems.

The virtualization of systems per Open Process Automation Forum (OPAF), and

arguably IIoT, is changing control system architectures once more, with the biggest impact at the top (nonexistent Level 5 at the top of the model) and again at Level 1, with basic regulatory control moving closer to the process itself. Because more functionality in these models will reside in software versus the hardware-based representation, the case can be made that the function-based reference model will become even more important since the physical hardware could potentially be flattened into fewer layers residing in the cloud and a couple virtual machines for the hardware above the sensor layer(s).

Early in 2019, we will continue the discussion on how SCADA and control systems are evolving by having a look at how LTE and 5G are adding another dimension to the ways future systems could potentially develop and be even more tightly integrated with their associated supply chains. ∞

Smooth the road to IIoT

Common methods and best practices for the Industrial Internet of Things start to solidify

By Jim Montague



It always helps when someone else scouts ahead, cuts through the jungle first, and sends back guidance about sought-after destinations and avoiding hazards. And just as geographical explorers assist travelers who come later, computing/networking pioneers can research, develop and experiment with new and emerging digitalized technologies to help those not as far up the learning curve. This is especially true for information technology (IT) experts, whose know-how is becoming more crucial to users in process control/automation and other operations technology (OT) disciplines as their industries are increasingly overrun by the Internet and its eponymous and unnecessarily named Internet of Things (IoT) and Industrial IoT (IIoT).

Buzzwords aside, as soon as software, microprocessors and wired/wireless Ethernet touched the plant floor, it was inevitable the Internet would support and take over from fieldbuses and their protocols—just as they previously supported and took over from hardwiring. The only question now is how make it simple, effective and secure in process applications, as well as the HMI/SCADA, MES, ERP, cloud-computing and other functions that serve them.

LOWER HURDLES, LESS BUMPS

“We began by implementing our building automation system (BAS) about 10-15 years ago for a multi-site pharmaceutical application with a standard automation approach using PLCs, thick clients and servers. Eventually, we moved to progressively smaller

PLCs and ARM-based embedded industrial PCs with a private cloud, and more recently expanded to public cloud-hosted servers using IIoT sensors and devices,” says Chris Hamilton, industrial information technology/operations technology (IT/OT) director at Grantek Systems Integration (<https://grantek.com>), a CSIA-certified system integrator (SI) in Burlington, Ontario, Canada. “In the past, this required a massive, costly BAS, along with a large investment in infrastructure, which wasn’t viable for medium sized or remote facilities that were equally as critical to our customers.”

Hamilton adds Grantek helped its longtime pharmaceutical customers extend the range of their temperature monitoring, ruggedize their equipment, and implement other BAS services with sensors and transmitters over the past four or five years. Previously, its customers were sending data to PLCs, but now, by leveraging its ARM-based embedded industrial PCs, Grantek can also aggregate data from other sources, such as Modbus and DNP3 devices, and leverage Amazon Web Services (AWS) cloud-computing services, including EC2 and RDS, for analytics and historization. “The customer needed low-cost monitoring of all their sites at a central location and on top of their engineering architecture,” explains Hamilton. “By leveraging industrial protocols like EtherNet/IP, and building on our experience in the industrial space, we could implement a more viable system built on low-cost

embedded devices.” Grantek continued to evolve its offering by adding plant-floor dashboards, powered again by ARM-based embedded PCs, delivering real-time, actionable data that customers rely on.

Following its BAS system’s success at Internet-based sensor monitoring, Hamilton reports Grantek expanded its use in power generation, solar and data center monitoring. “Due to their low price point, these simple devices together cost hundreds of dollars,” adds Hamilton. “Previously, controllers used for these tasks would cost thousands of dollars or more.”

SIMPLER, SHARPER HMI VIEWS

Probably the main way that common IIoT and web-enabled methods benefit users is by simplifying network pathways and access, which allows more consistent and detailed HMI display of their data that enable faster, better decisions.

For instance, in late 2017, Chobani (www.chobani.com) started the third expansion of its world’s largest yogurt plant in Twin Falls, Idaho, which is adding a \$20 million R&D center to its 1.4-million-square-foot facility. Much of Chobani’s meteoric rise is due to the public’s rediscovery of Greek yogurt, but it’s also because the company is a long-time user of web-based Ignition SCADA software from Inductive Automation (www.inductiveautomation.com), which it uses at all three of its plants on filling and packaging lines, and for



LIVE AND ACTIVE INTERNET

Figure 1: Chobani uses web-based, unlimited-licensing Ignition SCADA software on filling and packaging lines at its three Greek yogurt plants; for asset management, ERP and capex planning; to give all staff access to plant floor-to-enterprise data to improve efficiency; and to enable IT and OT convergence. Source: Chobani and Inductive Automation

quality control, asset management, enterprise resource planning (ERP) and capital expenditure (capex) project management. Hugh Roddy, global engineering and project management VP at Chobani, reports Ignition lets staff access data they never had before, view it from the plant floor to the executive level, and share it to improve efficiency and reduce downtime (Figure 1).

“Once we took Ignition onboard as one of our enterprise platforms, everything improved exponentially across the board from an operational standpoint,” says Roddy. “Having data from Ignition at their fingertips helps our employees be more efficient, and it makes

them feel part of the team. Ignition also lets us integrate the convergence of our operational technology (OT) and information technology (IT) environments into one platform to create more efficiencies.”

J.C. Givens, global network services manager at Chobani, adds, “Ignition is a good bridge for OT/IT collaboration. We can make gateways available to both networks, so whether people are in the office making decisions or on the plant floor making decisions, IT and OT information are both available.”

In addition, Chobani reports Ignition’s unlimited licensing arrangement gives it the

“Process applications are being impacted by IIoT and mobile computing in rapidly expanding ways.

The primary gains being experienced involve data democratization, which leads to data sharing, storage, analysis and better decision-making in near-real-time.”

flexibility to quickly keep up with production increases by rolling out as many devices and clients as it wants in as many places as it needs, or set up a single HMI for a special requirement, which happened in its new facility. “Previously, operators used a radio to call in, and had someone start each process step for them,” says Trevor Bell, automation engineer at Chobani. “With Ignition, we can put a special HMI out there, just for them. Ignition makes it cost-effective to do a one-off scenario like that.”

STANDARDS START TO GEL

One way to get new technologies and their users on the same page is to try to agree on standards for applying them, or if they have enough momentum, formalize the de facto standards that grow up with them. Though there aren’t really any completely settled or formal IIoT standards yet because it expanded so fast, there are a bunch of long-time Internet standards from the IT side that can be useful.

“Process applications are being impacted by IIoT and mobile computing in rapidly expanding ways. The primary gains being experienced involve data democratization,

which leads to data sharing, storage, analysis and better decision-making in near-real-time,” says Benson Houglund, vice president of marketing and product strategy at Opto 22 (www.opto22.com). “De facto standards are fine, but international standards defined and accepted across many industries are better.”

Houglund reports one IIoT-enabling standard is message queuing telemetry transport (MQTT), established as ISO/IEC PRF 20922. “MQTT emerged as an alternative to traditional poll-response mechanisms for getting data out of operational systems by using a publish-subscribe (pub-sub) model,” he explains. “The advantages of the MQTT pub-sub model are many, but the key issues addressed are security and performance. Pub-sub models like MQTT don’t require inbound network interface ports on OT devices (like PLCs) to be opened, which mitigates a major security risk. Further, MQTT methods publish data only on change, while maintaining a connection for state management and bidirectional data transfer and control.”

Another cornerstone standard that’s simplified the IIoT landscape is the

long-established and well-known transmission control protocol/Internet protocol (TCP/IP), or Internet protocol suite. In fact, MQTT and a host of other mostly four-letter protocols are organized as part the suite's application, transport, Internet and link layers. "TCP/IP isn't usually considered an emerging standard as it's used by nearly every networked computer, mobile device and most PLCs and PACs in existence today," adds Hougland. "However, the TCP/IP protocol suite is the grandfather of all networking standards in use today."

CAUTION, CARE STILL REQUIRED

Despite its advantages and increasing reliability, IIoT is still used mostly for monitoring and non-critical control because its communications and networking can still suffer interruptions and outages, especially when it uses mainstream Internet. "Potential users need to define their value proposition to decide if they can use non-standard or non-industry-norm technologies," says Grantek's Hamilton. "For instance, we wouldn't put a consumer grade device like a Raspberry Pi on a critical batch control system. However, if we're doing visualization or other non-critical functions, then we can be creative. It's also important to work with a vendor with a mature team that can use the right software development process, including version control and unit testing. This is important because these systems need to continue to evolve and grow to support

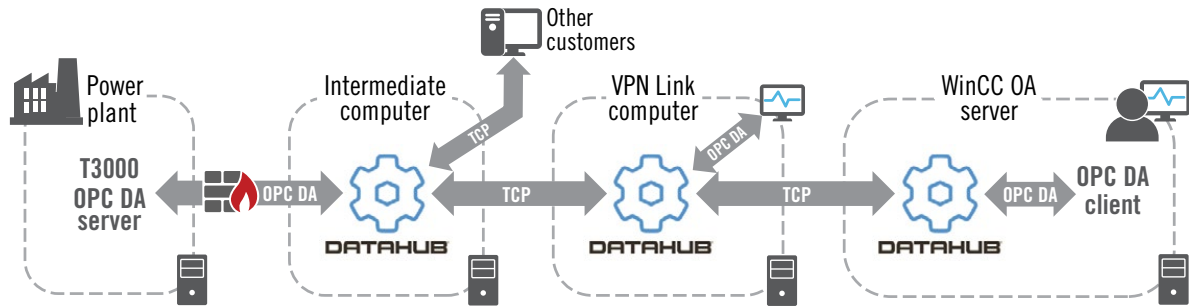
our customers' ever-changing needs. A traditional control system is a beast that doesn't change easily."

Because Modbus, DNP3 and other field-buses perform well on the plant-floor but need an IP protocol for IIoT, and because MQTT is a transport protocol that efficiently moves data but doesn't natively store-and-forward it like plant-floor networks do, Hamilton adds that some kind of protocol conversion is usually needed to get data from one realm to the other. "For example, it's a bad idea to try to do OPC UA directly over the Internet because it isn't a hardened WAN protocol, and it isn't designed to handle Internet latency and security requirements. So, when we're going from OPC UA to a Raspberry Pi, we need to use protocol conversion such as Ignition Edge or Kepware, or run some custom software on an embedded device. For users to be happy with IIoT, they must understand the landscape of how their devices are pulled together on these networks."

IP STREAMLINES OPERATIONS

Another advantage of IIoT and its common, IP-based networking methods is they can be simpler and faster to deploy than traditional fieldbuses and the data translation, configuration and other tasks they require.

For example, Alexis Tricco at Siemens Buenos Aires (<https://new.siemens.com/ar/es.html>) in Argentina recently undertook



OPC TUNNELS TO POWER PLANTS

Figure 2: To gather data from controls at remote power plants, Siemens Buenos Aires replicates data from a T3000 DCS to an interface PC and Siemens WinCC OA SCADA system and server; uses OPC to relay data because T3000 has an OPC server and WinCC has an OPC client; and tunnels OPC data over TCP with a company VPN and selected Cogent DataHub tunneling software from Skkynet. Source: Siemens and Skkynet

its first digitalization project as part of his firm’s overall digitalization program. To provide technical support backup for power plants’ generating operations, Tricco and his colleagues typically supervise and upgrade client operations, but the digitalization project assigned them to develop a reliable, secure way to collect data from controls at power plants located hundreds of kilometers away from their office. The first phase was a pilot connecting Tricco’s WinCC OA SCADA system to a Siemens T3000 DCS running at a power plant about 100 km from Buenos Aires, as well as include the plant’s control network and a multi-customer network (Figure 2).

“My idea was to bring all the process data onto my WinCC OA server running on the customer network,” says Tricco. “To get this, I needed to replicate the data from the T3000 to the interface PC and from there to the WinCC OA Server.” Tricco chose

OPC to relay plant data because its T3000 had an OPC server and WinCC has an OPC client. However, since OPC DA doesn’t network well, he decided to tunnel OPC data over TCP with a company VPN, and selected Cogent DataHub tunneling software from Skkynet (www.skkynet.com).

“I needed to communicate over different networks, with end points that could convert between TCP and OPC, acting as server and client simultaneously,” explains Tricco. “DataHub has an OPC server on one side and an OPC client on the other, which is what I needed. Other software would’ve required two licenses for each PC, and I had to think of the costs. DataHub was user-friendly and wasn’t complicated, and I got it working in less than a day.”

Following the pilot’s success and the client’s acceptance, Tricco can go online

from his WinCC OA server in Buenos Aires, collect OPC data from the plant's T3000, and perform real-time analysis. The plant's engineers can also monitor the performance of their gas turbines, and optimize combustion and control emissions to meet regulations without going onsite. Thanks to digitalization, the plant is running at higher capacity and reduced emissions, while the client plans to implement it at two more plants.

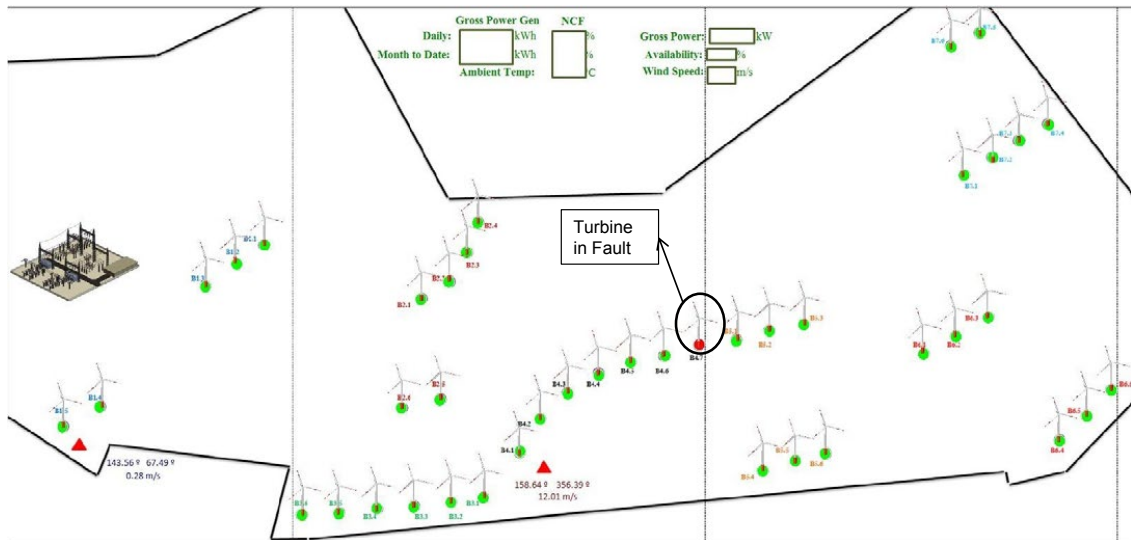
Similarly, Cemex (www.cemex.com) established its Cemex Energía subsidiary five years ago to reduce its electricity costs and CO2 emissions by using renewable energy sources such as wind to generate power for cement production. The division builds power plants and provides asset management services to other companies, and is working on more than 20 projects worldwide. Cemex Energía also owns and operates three power plants in Mexico, two wind and one geothermal, which have one gigawatt of combined capacity. The two wind farms each supply more than 250 megawatts of electricity and are critical to Cemex's cement production, but they also need data for efficient operations.

"The performance of the wind turbine generators directly impacts our main KPIs—technical, contractual and economic—so our challenge is maximizing the resources available from the wind farm,"

says Roberto Carlos Medrano, operations and maintenance manager at Cemex Energía. "We also needed data management to support our energy operational platform in all CemexEnergía operations to enable a reliable asset management strategy to comply with all our contractual obligations."

Consequently, Cemex Energía adopted OSIsoft's (www.osisoft.com) PI System, Web API, Connected Services and OPC data communications. "PI and Connected Services create a specialized and reliable analysis tool that measures deviations in real performance compared to warranty performance behavior in real time," says Medrano, who adds the wind farms use PI Server's four main features—Asset Framework (AF), Event Frames, notifications and high availability—to improve turbine operations by implementing simpler operations presentation on a few simple screens.

For instance, Cemex Energía employs PI System combined with a Google Maps image to produce a live-action overview of the wind farms, which shows the running status of the turbines in real time, any faults, and operations including daily and monthly production, ambient temperature, capacity and wind speed. Operators can double click on the graphic for individual turbines to view details; use AF navigation to move between turbines; view an



WIND BLOWS, CEMENT FLOWS

Figure 3: Cemex Energia is using wind power to generate electricity for making cement with help from OSIsoft's PI System, Web API, Connected Services and OPC data communications. PI even combines with a Google Maps image to produce a live-action overview of Cemex's wind farm, showing the status and operations of turbines in real time. Source: Cemex and OSIsoft

alarm panel page; and drill down to circuit breaker details (Figure 3).

“Without AF, I think this could not be possible,” adds Medrano. “We have a lot of turbines, which means we need the capabilities of AF and its templates, so we can create one template, and spread it among all the turbines.”

WIRELESS RIDES SHOTGUN

Of course, once Ethernet began popping up in process applications, it was closely followed by related wireless formats such as WiFi and Bluetooth, which joined the radio, cellular and satellite technologies that were often already there. And, because Ethernet paves the way for the Internet, IIoT can also expand via wireless.

For example, Kraft Heinz Co.'s (www.kraft-heinzcompany.com) plant in Champaign, Ill., has long used PLCs to manage operations and raw material/product refrigeration, but it didn't have enough sensors with real-time monitoring, notifications and alerts of out-of-range temperatures, and often resorted to paper chart recorders that had to be checked manually. As a result, Kraft Heinz engineers recently installed matchbox-sized, battery-powered wireless temperature sensors from Swift Sensors (www.swiftsensors.com), which send data to a wireless bridge that relays it via secure Wi-Fi to a cloud service for uniform display on a common dashboard available on PCs and mobile devices.

Better temperature monitoring and improved productivity encouraged Kraft



PLC, RTDS LOOP TO WIRELESS, CLOUD

Figure 4: Wireless, 4-20 mA sensors deployed at Kraft Heinz's plant in Champaign, Ill., are connected in a 4-20 mA current loop from RTD sensors and PLCs controlling operations, refrigeration and motors. They deliver data to a bridge and cloud service that displays it on a common dashboard, which users can view on PCs, tablets and smartphones. Source: Kraft Heinz and Swift Sensors

Heinz to add wireless vibration sensors to motors on its pumps and compressors, and provide real-time alerts to quality assurance and maintenance staff about changes in their performance without altering existing equipment. The latest wireless device deployed at the Champaign plant is Swift Sensors' 4-20 mA sensors, which are linked in a 4-20 mA current loop from RTD sensors used with the PLCs. The 4-20 mA sensors let users pull data from existing transducers and sensors connected to existing PLCs using the standard 4-20 mA current loop, and this delivers real-time updates from all sensors in the plant to one cloud-based dashboard viewable on PCs, tablets or smartphones (Figure 4).

Kraft Heinz reports automatic data logging and reporting by its new wireless network reduced its return on investment (ROI) to just five months, while immediate notifications have aided its food safety and saved hundred of thousands of dollars of raw materials and finished products.

SEEKING SECURITY

Despite its considerable and ongoing impact, one major snag holding the Internet back from being applied more widely in process applications and other industries is its perceived and often real lack of cybersecurity. And, even though perception and reality aren't the same, they still put the

same restrictions on using IIoT to aid and optimize process applications.

“The primary, potential risk in using IIoT and mobile technologies in process applications is addressing and implementing security. It’s very easy to quickly build systems without regard for security measures, and for this reason, many devices, controllers and other systems aren’t adequately protected from intruders or otherwise bad actors in a networked system,” explains Opto 22’s Hougland. “That said, there are plenty of security tools and architectures freely available to implement and protect process systems. However, because it is a choice and not a requirement on the part of the architect of these systems (whether end user, integrator, OEM or others), these security tools are often not implemented correctly, or in many cases, not implemented at all. This is due in part to the fact that security tools and architectures have principally been part of the IT domain, and not the OT domain. In many cases, this all simply boils down to knowledge and training.”

Because the classic process automation model is a PLC with I/O points reporting to it, Grantek’s Hamilton adds that IIoT really starts where ISA-95 Level 0 devices become network connected and add intelligence otherwise not available, though they bring vulnerabilities that must be addressed. “The benefit of IIoT is that it can

achieve much deeper visualization into process applications,” says Hamilton. “When a basic temperature sensor adds a chip, intelligence and the Internet, users can get many more and different indications. The sensor can tell when it was last calibrated or if there are any anomalies, and it can trend data. Previously, only one piece of data was available because of its analog output. Now, devices with chips are much more flexible, but they’re also vulnerable. Smart sensors can have their code modified to give bogus data or become part of denial-of-service (DoS) attacks, so users and their security teams need to work with security-aware system integrators and vendors to follow defense-in-depth, least-privilege and other security policies.”

Hamilton adds that every vendor wants to get onto the IIoT, but end users usually only ask if they can get the functions they want, and how cheaply they can get them. “Users and vendors need to give themselves a little more space to follow security best practices,” he says. “They must implement encryption and mutual authentication to make sure their devices are only used in the fashion intended and can access only what’s needed to do it. This means employing PKI or PGP cryptography, so during sign in, you send me a message that I can use to validate you and vice-versa. IIoT devices are proliferating rapidly, but they must follow procedures that make them not just functional, but secure as well.” ∞

Primary IIoT players

A guide to major components of the Industrial Internet of Things

By Jim Montague



- **Advanced message queuing protocol** (AMQP) is an application-layer protocol that's binary, open and standardized, and typically used by message-based software serving other applications. It's characterized by message orientation, queuing, point-to-point and publish-and-subscribe routing, security and reliability.
- **File transfer protocol** (FTP) is a standard network protocol for moving computer files between a client and server on a computer network, and is founded on a client-server model architecture using separate data and control connections. FTP can run in active or passive modes, which determines how the data connection is established.
- **Hypertext transfer protocol** (HTTP) is the application protocol for distributed, collaborative hypermedia information systems. HTTP is the foundation of data communication on the web, where hypertext documents include hyperlinks to other resources that users can access.
- **JavaScript object notation** (JSON) is an open-standard, language-independent data file format that uses readable text to send data objects made of attribute-value pairs and array data types or other values that can be serialized. It's a common format used for asynchronous browser/server communications, and many programming languages include code to generate and parse JSON-format data.

- **Message queuing telemetry transport** (MQTT) is a publish-subscribe protocol that uses message-brokering to let clients communicate with a server. It runs atop TCP/IP, is standardized as ISO/IEC PRF 20922, and links distributed devices with small amounts of programming and/or runs on lower-capacity networks. Every MQTT client can reach the broker, and each can publish data or subscribe to it. The protocol doesn't offer security functions, but these can be done at the TCP/IP level.
- **Node-RED** is a flow-based development tool for visual programming originally created by IBM for wiring together hardware devices, APIs and online services as part of the IoT. Node-RED provides a browser-based flow editor that's used to create JavaScript functions. Application elements can be saved or shared for reuse. Flows created in Node-RED are stored using JSON, and MQTT nodes can make properly configured TLS connections.
- **Representational state transfer** (REST) is a software architecture for distributed hypermedia systems that defines constraints for creating web services. When these services conform to REST's

six guiding constraints, they're called RESTful web services (RWS), and enable interoperability between Internet computing systems. RWSs allow inquiring systems to access and manipulate textual representations of web resources by using uniform, predefined stateless operations.

- **Simple network management protocol** (SNMP) is a widely used Internet standard protocol for network monitoring, gathering and organizing data about managed components on IP networks, and modifying that data to alter device performance.
- **Transmission control protocol/Internet protocol** (TCP/IP), also known as the Internet protocol suite, includes the model and end-to-end communication protocols used by the Internet and similar networks, and defines how digital information should be packaged, addressed, sent, routed and delivered. The suite's many protocols are divided into four abstraction layers—link for communicating within one network; Internet for communicating between networks; transport for communicating between host devices; and application for communicating between processes. ∞