IloT & Industry 4.0

- Industrial-strength MQTT/Sparkplug B
- Ultra-long-life batteries for IIoT devices
- Conquering the cloud with OPC UA
- Moderna’s process automation on AWS
- IT/OT convergence benefits
IIoT & Industry 4.0

Industry 4.0 is getting real, and technology is moving fast to support new applications that include the Industrial Internet of Things (IIoT). You'll find the latest tools and techniques in this edition of AUTOMATION 2021. Discover how new value is being created by fusing OT field data with new digital technologies including the cloud, artificial intelligence, and digital twins. Learn how you can use MQTT/Sparkplug B to build industrial networks at scale with edge computing, as well as how OPC UA can take your designs from the device to the cloud and back, protecting your automation investment. Understand how ultra-long-life lithium batteries are powering remote wireless devices at the edge and in the field. And don’t miss the article on Moderna's award-winning cGMP clinical development manufacturing facility, which has created a native digital process automation design in the cloud with the help of Amazon Web Services, one of the newest OPC Foundation partners.

Renee Bassett
Chief Editor
Industrial-strength MQTT/Sparkplug B
By Josh Eastburn, Opto 22
Building industrial MQTT networks at scale with edge computing.

Batteries Designed to Run an IIoT Marathon
By Sol Jacobs, Tadiran Batteries
Ultra-long-life lithium batteries can overcome the problem of high self-discharge to run for long distances while delivering the high pulses required for two-way wireless communications.

Conquering the Cloud with OPC UA
By Jim Redman, ErgoTech Systems, Inc.
This vendor-independent standard can take your designs from the device to the cloud and back, protecting your automation investment.

Native Digital Process Automation Built on Amazon Web Services
By Bill Lydon, Automation.com
Moderna's award-winning cGMP clinical development manufacturing facility uses the latest technological building blocks and IIoT ecosystem.

IT/OT Convergence Delivers a Growing Range of Benefits
By Masaru Yamazaki and Chigusa Akana, Yokogawa
New digital technologies can provide significant operational improvements, but connectivity and cybersecurity concerns must be addressed.
One I/O Module, 200,000 Possibilities.

Thousands of Unique Field I/O Combinations. Learn more at info.opto22.com/thousands

- Thermocouple inputs and discrete sinking outputs cannot be mixed on channels 0-3.

groov RIO® revolutionizes modular I/O by offering over 200,000 unique, software-configurable I/O combinations in a single, compact, PoE-powered industrial package.

Combined with web-based configuration, commissioning, and flow logic software built in, plus support for multiple OT and IT protocols, this could be the I/O you've always dreamed of.

Only from Opto 22.

Learn more about groov RIO today. Visit: info.opto22.com/introducingRIO
Building industrial MQTT networks at scale with edge computing.

By Josh Eastburn, Opto 22

MQTT (formerly MQ Telemetry Transport) consistently ranks as the most popular IoT-specific messaging protocol. However, there are several obstacles to bringing the power of MQTT to an industrial environment.

MQTT’s innate flexibility requires stronger guarantees of interoperability and state management to meet the needs of a diverse industrial network. Likewise, while MQTT provides a framework for large-scale integration and addresses fundamental cybersecurity issues, MQTT by itself cannot create a secure Industrial Internet of Things (IIoT) infrastructure.

For system integrators, developers, engineers, and managers wondering what MQTT can do for them, this article explains the protocol’s fundamentals, demonstrates how the Sparkplug B specification adapts MQTT to industrial applications, and shows how to establish and scale MQTT networks using industrial edge computing.
Fundamentals of MQTT v3.1.1

Traditional communication models use a poll-response mechanism to interrogate field devices and maintain state awareness. Data is refreshed when a master device or application requests new data, causing field devices to respond with the requested data. When IBM and Arcom Control Systems developed MQTT, they abandoned this model in favor of a brokered publish-subscribe model—MQTT’s central strength.

In that scheme, a central server acts as a broker, managing data delivery for the entire network. Rather than being prompted by command, MQTT-enabled devices publish data to the broker only when a monitored value changes, a behavior called report by exception.

Because some devices may not publish very often, state awareness is maintained by periodically sending a small keep-alive packet to the broker, plus other mechanisms that we’ll discuss later. Other clients, including software and other field devices, can register with the broker as subscribers to any data published on the network.

Figure 1. Poll-response protocols generate a lot more network traffic than report-by-exception models.
Flexible topic paths

Although each client identifies itself to the broker with a unique client ID, there is no device addressing scheme. Instead, clients identify published data using individual, hierarchical topic paths represented as plain text strings. For example, “CellA/Oven/Temperature” could represent the internal temperature of an oven in a particular work cell. Single- and multilevel wildcard characters (+, #) provide more flexibility.

The broker stores these topic filters with each client’s network session and routes matching updates from publishers to all matching subscribers: one-to-one or one-to-many. This system is something like Twitter for machines: a free flow of anonymous, interest-based, event-driven, bidirectional communication.

Efficient message payload

Both MQTT and HTTP are commonly used as IoT messaging transports, but while HTTP is famously heavyweight, MQTT is data-agnostic, with a streamlined on-the-wire footprint that devices with limited power and processing capabilities can process efficiently.

MQTT uses a simple byte array payload with a fixed 2-byte header and variable-length header fields (a few additional bytes) to indicate packet length or control codes. A packet is up to 256 MB in size and can transport anything from process variables to your pet’s photo.

Figure 2. The size of an MQTT packet can vary from 256 MB to as little as 2 bytes.
Fault tolerance mechanisms

MQTT’s designers also included features to gracefully handle unintended client disconnections and ensure data delivery to subscribers:

▶ Messages can be optionally transmitted at higher quality-of-service (QoS) levels that carry more overhead but have a stronger guarantee of delivery.

▶ Published topics can be flagged as retained messages. The MQTT broker keeps the most recent update available for new subscribers.

▶ If a client connects using a persistent session, the MQTT broker stores its configuration and high QoS messages should it disconnect unexpectedly.

▶ Each client can also register a special last will and testament (LWT) message with the broker, which is distributed to subscribers should the client connection be interrupted unexpectedly. The client’s keep-alive timer determines when the broker considers the connection lost.

Advantages of MQTT

Efficient communication

Combined with its streamlined payload, the MQTT communications model delivers an 80–90 percent reduction in bandwidth consumption compared to poll-response models, according to co-inventor Arlen Nipper. This efficiency creates room for existing networks to grow—up to millions of connections.
Decoupled data

But it is the decoupled nature of MQTT data exchange that unlocks industrial network scalability. Without point-to-point connections or direct addressing, MQTT networks can grow and share data flexibly. Any client wanting access to published data—a maintenance database, enterprise resource planning, or a supervisory control and data acquisition (SCADA) system, for instance—can simply point to the MQTT broker and subscribe to any desired topics, without needing details of the publishing source.

Figure 3. In the MQTT architecture, publishers and subscribers from across the organization connect through a common data broker.
Security

MQTT’s basic architecture also improves IoT security. The broker alone manages client authentication, data access rights, and message delivery, simplifying network management and allowing clients to remain anonymous. And because MQTT connections are device-originating (outgoing), only the broker requires open firewall ports. Field devices can be completely locked down while still permitting bidirectional communication.

MQTT also supports username and password requirements but usually relies on transport layer security (TLS) encryption (port 8883 is registered for MQTT TLS). With certificates of trust authenticating connected endpoints, secure site-to-site MQTT communication is feasible even over public networks.

Faster, better with Sparkplug B

Although this simple framework allows MQTT to support many kinds of IoT applications, configuring the large, diverse networks characteristic of industrial installations can require significant effort akin to mapping conventional tag data between applications. Further, there is no guarantee that a device vendor will use the features available to mitigate connection risks and maintain data quality.

These weaknesses inspired Arlen Nipper and Cirrus Link Solutions to develop the open-source “Sparkplug MQTT Topic Namespace and Payload Definition.” The current version, Sparkplug B (SpB), expands on the basic MQTT architecture to address common industrial use cases and adds important implementation details for MQTT clients.

Components of an MQTT/Sparkplug B network

Sparkplug adds to and clarifies the roles of basic MQTT clients, enabling new features and more explicit messaging that are the basis for other enhancements in the specification. The specification distinguishes between two essential types of MQTT clients:
MQTT/Sparkplug B Edge of Network (EoN) Nodes: These clients provide physical and/or logical gateway functions to enable MQTT/Sparkplug B communications for legacy devices and sensors. EoN nodes also include smart devices and sensors capable of publishing their own Sparkplug B data, process variables, or metrics directly to an MQTT broker.

MQTT/Sparkplug B Application Nodes: These are software clients, optionally including one primary application responsible for sending commands and receiving historical data. An MQTT/SpB application node may also be a gateway to legacy software systems.

Any MQTT 3.1.1–compliant broker supports Sparkplug B payloads, and one or more can be used for redundancy, high availability, or scalability.

Topic namespace
Sparkplug defines a standard format for MQTT topic paths:

```
spBv1.0/<Group ID>/<MESSAGE TYPE>/<Edge Node ID>/<Device ID>
```

<table>
<thead>
<tr>
<th>Element</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Group ID&gt;</td>
<td>Logical identifier for a group of MQTT nodes</td>
<td>User defined</td>
</tr>
<tr>
<td>&lt;MESSAGE TYPE&gt;</td>
<td>Indicates whether the message contains state information, data, or a command and whether it pertains to a node, device, or the primary application</td>
<td>Predefined by SpB spec; user cannot change</td>
</tr>
<tr>
<td>&lt;Edge Node ID&gt;</td>
<td>Identifies a specific MQTT node</td>
<td>User defined. The Group ID/Edge Node ID combination must be unique</td>
</tr>
<tr>
<td>&lt;Device ID&gt;</td>
<td>Identifies a device attached physically or logically to a node</td>
<td>(Optional) User defined</td>
</tr>
</tbody>
</table>
Payload definition

Sparkplug B also defines a standard, structured, data-rich yet efficient payload format. The core payload contains an array of metrics and associated metadata as well as optional fields and custom properties for each metric: name, description, data type, engineering units, scaling limits, and more. Data type indicators accommodate complex types common in industrial applications, like matrices and user-defined types (UDTs). The full payload is then time stamped, sequenced, and encoded using an efficient binary representation of the structured data. The decoded payload is typically represented in JavaScript Object Notation (JSON).

State management

Sparkplug defines *birth and death certificate* messages to enforce state monitoring. Death certificates use MQTT’s LWT message option and the special message types NDEATH or DDEATH, indicating whether the certificate pertains to a node or to an attached device, respectively. When first online, each client must also publish birth certificates (message types NBIRTH or DBIRTH) for itself and its attached devices. Birth messages define all available topics for that client/device and inform all subscribers that it is online.

Primary application

While an MQTT network may contain any number of application clients, the Sparkplug specification allows one application node to be designated as the primary application, typically a SCADA or IIoT host that sends commands and logs historical data. It publishes birth and death certificates using the unique topic STATE/<client ID> with elevated quality-of-service and retained message status, so any MQTT client can identify its state at any time.
Advantages of Sparkplug B

Low administration

Because a birth certificate is required from each client whenever it connects to the network or updates its topic structure, subscribers can automatically map out available MQTT topics in a few moments. And thanks to Sparkplug B’s payload structure, certificates include all metadata and UDT definitions. No more tag mapping.

Interoperability

The Sparkplug B specification addresses the potential for inconsistency in MQTT implementations by defining standard client roles and data interfaces designed around industrial applications. By standardizing on Sparkplug, MQTT clients from different vendors can identify, interpret, and use published data without needing to know details of the source. Even legacy automation networks and devices can leverage Sparkplug because of its explicit support for gateway-attached devices.

Unified namespace

This level of interoperability satisfies a critical requirement for digital transformation by making it possible to have an enterprise-spanning namespace defining all business data. Enterprise clients can consume data from the field via the broker, using Sparkplug to provide a common exchange format and uniform context, then publish results back into the network to be detected, interpreted, and acted on by other clients.

Figure 4. With Sparkplug, data from many domains can be shared interoperably across an organization.
Enhanced data integrity

By requiring LWT messages, Sparkplug ensures all subscribers are notified when data becomes stale. Likewise, birth certificates let subscribers know when data is fresh again. And the primary application mechanism creates new failover options to avoid critical data loss.

All clients can detect when the primary application’s connection is interrupted and search any alternate connections for a broker showing an “ONLINE” status for the application. Clients with storage capabilities can also use store-and-forward historization to queue up messages, flag them as historical data, and publish them into the network once the primary application is available again.

Figure 5. Sparkplug B’s primary application mechanism enables smart failover and store-and-forward historization.
Building mission-critical MQTT networks

Despite MQTT and Sparkplug B’s inherent advantages, they cannot function without robust support from all network clients. Sparkplug’s features, like legacy device integration and store-and-forward historization, cannot be realized without field device clients that implement the necessary gateway and storage functions.

And fundamental network reliability is undermined unless every network participant implements complementary cybersecurity and connectivity features. Even the sheer volume of data a large IIoT network generates can be overwhelming unless clients can filter and sanitize data locally before publishing.

Unfortunately, traditional industrial devices were designed for a narrow scope of operation and often lack general-purpose processing, communication, and storage.

Industrial edge computing

Many industrial automation vendors are drawing inspiration from information technology to address these gaps, turning to an approach known as edge computing—a form of distributed computing that moves computing resources closer to high-demand areas on the network’s edge. With more resources at the edge, data can be prepared locally before broad distribution; modern security measures can be layered onto legacy systems; and advanced functionality can be embedded in the process to support a resilient network.

Opto 22’s groov devices support edge data processing with embedded tools like Node-RED, IBM’s free, open-source IoT platform, and Ignition Edge from Inductive Automation. They provide modern IT security.
options like user authentication, TLS encryption, and device firewalling. And they support store-and-forward historization with local fault-tolerant storage. All groov devices provide robust MQTT/Sparkplug B client options, designed in collaboration with industry leaders like Cirrus Link.

**From concept to cash**

Using edge devices like these, users can build a secure MQTT/Sparkplug B network following a basic pattern:

1. First, instrument assets and connect I/O to an edge device like groov EPIC.

![Diagram of a basic pattern for building an MQTT network with industrial edge devices.](image-url)
2. If controls already exist, connect them to a segmented network interface on the EPIC, and use OPC UA drivers to retrieve data.

3. Then, the EPIC can open a secured connection to an MQTT broker, ideally in the corporate network's demilitarized zone (an isolated network that bridges internal and external networks).

4. Now, plug applications into the infrastructure. A gateway application like Cirrus Link’s MQTT Engine can integrate legacy applications, if needed.

5. With this foundation, the system can scale up using additional edge devices or brokers to build out a highly resilient, high-performance data exchange and command-and-control system.

By relying on a flexible, efficient, open-source standard like MQTT/Sparkplug B, this design reduces licensing and configuration costs, allows users to pick from a variety of components, provides multiple options for scaling up, and delivers subsecond response times even across global networks.

**Complete solution**

MQTT is popular, proven, and well supported in enterprise and consumer applications. It makes organization-spanning data exchange possible by decoupling data producers and consumers and by defining a lightweight, data-agnostic communication format supporting millions of connections. But its usefulness for industrial applications is challenged by various interoperability and reliability risks.
Sparkplug B defines an MQTT implementation standard that ensures client interoperability, delivers usable data for operations, gracefully handles instability, and helps organizations scale by reducing administrative overhead. Industrial edge devices complete the architecture by providing physical layer reliability, integration options, and sufficient computing power to process and transmit field data efficiently and securely.

The combination of MQTT, Sparkplug B, and industrial edge devices forms a complete solution for building and scaling connected IT/OT data networks. It is open, flexible, and powerful enough to support the requirements of any connected application.

All figures courtesy of Opto 22

ABOUT THE AUTHOR

Josh Eastburn is director of technical marketing at Opto 22. After 12 years as an automation engineer working in the semiconductor, petrochemical, food and beverage, and life sciences industries, Eastburn now works with the engineers at Opto 22 to understand the needs of tomorrow’s customers. He is a contributing writer at blog.opto22.com.
Remote wireless devices connected to the Industrial Internet of Things (IIoT) run on Tadiran bobbin-type LiSOCl₂ batteries.

Our batteries offer a winning combination: a patented hybrid layer capacitor (HLC) that delivers the high pulses required for two-way wireless communications; the widest temperature range of all; and the lowest self-discharge rate (0.7% per year), enabling our cells to last up to 4 times longer than the competition.

Looking to have your remote wireless device complete a 40-year marathon? Then team up with Tadiran batteries that last a lifetime.

* Tadiran LiSOCl₂ batteries feature the lowest annual self-discharge rate of any competitive battery, less than 1% per year, enabling these batteries to operate over 40 years depending on device operating usage. However, this is not an expressed or implied warranty, as each application differs in terms of annual energy consumption and/or operating environment.
Batteries Designed to Run an IIoT Marathon

Remote wireless devices are becoming increasingly essential to virtually all IIoT-connected applications, including asset tracking, supervisory control and data acquisition, environmental monitoring, AI, M2M, and machine learning, to name a few. Battery-powered devices eliminate the need for expensive hardwiring in challenging environments and inaccessible locations. Industrial-grade lithium batteries are preferable to short-lived consumer-grade batteries, as extended battery life can bring higher reliability, greater longevity, improved customer satisfaction, and a lower cost of ownership.

By Sol Jacobs, Tadiran Batteries

Ultra-long-life lithium batteries can overcome the problem of high self-discharge to run for long distances while delivering the high pulses required for two-way wireless communications.
Low-power wireless devices designed for marathons

Low-power devices can run long distances by carefully conserving energy. Two types of low-power wireless devices are available: those that draw an average current in microamps, typically powered by an industrial-grade primary (nonrechargeable) lithium battery; and those that draw average current in milliamps, enough to prematurely exhaust a primary battery. Because these applications involve greater energy consumption, they can require the use of an energy harvesting device in tandem with an industrial-grade rechargeable lithium-ion (Li-ion) battery.

Specifying an ultra-long-life battery involves numerous parameters, including: the amount of current consumed while in active mode (including the size, duration, and frequency of pulses); the amount of energy consumed while in standby mode (the base current); storage time (as normal self-discharge during storage diminishes capacity); thermal environments (including storage and in-field operation); and equipment cut-off voltage, which drops as cell capacity is exhausted or during prolonged exposure to extreme temperatures. Most important is the annual self-discharge of the cell, which often exceeds the amount of current required to operate the device.

Remote wireless devices are predominantly powered by primary (nonrechargeable) chemistries, including iron disulfate (LiFeS$_2$), lithium manganese dioxide (LiMnO$_2$), lithium thionyl chloride (LiSOCl$_2$), alkaline, and lithium metal oxide chemistry (table 1).

Figure 1. Bobbin-type LiSOCl$_2$ batteries are preferred for use in remote wireless applications. These cells deliver higher capacity and energy density, up to 40-year operating life, and the widest possible temperature range, which is ideal for hard-to-access locations and extreme environments.
Lithium stands apart as the lightest nongaseous metal, with a high intrinsic negative potential that exceeds all others, resulting in the highest specific energy (energy per unit weight) and energy density (energy per unit volume) of all commercially available chemistries. Lithium cells operate within a normal operating current voltage range of 2.7 to 3.6 V. These chemistries are also nonaqueous, whereas water-based chemistries can freeze in extremely frigid temperatures.

Lithium thionyl chloride (LiSOCl₂) chemistry, which offers the longest operating life, is constructed in two ways: bobbin-type or spiral wound. Spiral wound cells are specified for applications that require higher energy flow. Bobbin-type cells are better suited for low-power applications due to their higher capacity and higher energy density, as well as a wider temperature range (–80°C to 125°C). A key feature of bobbin-type LiSOCl₂ chemistry is its exceptionally low annual self-discharge rate (less than 1 percent per year for certain cells), permitting up to 40-year battery life.
Self-discharge shortens battery life

Battery self-discharge is common to all chemistries, as chemical reactions naturally consume energy even while a cell is inactive. Fortunately, you can modify the self-discharge rate of a bobbin-type LiSOCl$_2$ battery by controlling the passivation effect.

Passivation occurs only with LiSOCl$_2$ batteries, caused by a thin film of lithium chloride (LiCl) that forms on the surface of the lithium anode, separating the anode from the electrode to limit the chemical reactions that cause self-discharge. When a load is placed on the cell, the passivation layer causes initial high resistance along with a temporary drop in voltage until the discharge reaction slowly dissipates the LiCl layer: a process that repeats itself each time the load is removed.

Several other factors can influence cell passivation, including current discharge capacity, the length of storage and storage temperature, discharge temperature, and prior discharge, as partially discharging a cell and then removing the load can increase the amount of passivation relative to when the cell was new.

The good side of passivation is its ability to minimize battery self-discharge. The bad side is that too much of it can restrict energy flow.

Self-discharge is also affected by the cell’s current discharge potential, the method of manufacturing, and the quality of the raw materials. The highest-quality bobbin-type LiSOCl$_2$ cell can feature a self-discharge rate as low as 0.7 percent per year, retaining 70 percent of its original capacity after 40 years. Conversely, a lower-quality bobbin-type LiSOCl$_2$ cell can experience a self-discharge rate of up to 3 percent per year, losing 30 percent of its initial capacity every 10 years, making 40-year battery life impossible.

Be aware that it can take years for battery self-discharge to become fully apparent and that theoretical test data tends to be unreliable. For these reasons, thorough due diligence is required, especially if the battery needs to run for the life of the device.

Figure 2. Bobbin-type LiSOCl$_2$ batteries can be combined with a patented hybrid layer capacitor (HLC) to offer up to 40-year operating life while also providing high pulses to power two-way wireless communications.
Two-way wireless connectivity demands high pulses

A growing number of remote wireless devices require periodic high pulses to power two-way wireless communications. To conserve energy, these devices typically incorporate a low-power communications protocol (e.g., WirelessHART, ZigBee, or LoRa), along with a low-power chipset and proprietary energy-conserving techniques.

Standard bobbin-type LiSOCl$_2$ cells cannot deliver the high pulses required for two-way communications: a challenge that can be easily overcome with the addition of a patented hybrid layer capacitor (HLC). The bobbin-type LiSOCl$_2$ cell delivers nominal background current during “standby” mode, while the HLC works like a rechargeable battery to generate high pulses up to 15A. As an added bonus, the HLC also features

The Runner Analogy: Winning a Marathon

The distance is equivalent to the battery/device operating life. The farther a runner can travel, the more years a device will be able to operate.

The incline is equivalent to the battery’s self-discharge rate. The higher the self-discharge rate, the larger the incline, which draws more power and shortens the duration of the run. Similarly, higher battery self-discharge consumes more energy to shorten the cell’s operating life.

Hurdles are equivalent to pulses. The higher the hurdle, or obstacle, the higher the pulse required to support two-way wireless communications and other advanced functionality.
an end-of-life voltage plateau that can be interpreted to communicate “low battery” status alerts (figure 2).

Supercapacitors provide the same function in consumer electronics but are generally not suited for industrial applications due to inherent limitations, including short-duration power, linear discharge qualities that do not permit full discharge of available energy, low capacity, low energy density, and a very high self-discharge rate of up to 60 percent per year. Supercapacitors linked in series require cell-balancing circuits that are bulky, expensive, and draw additional energy to further shorten their operating life.

Here are some typical real-life examples that rely upon bobbin-type LiSOCl₂ batteries:

**Cryoegg**: Researchers studying the relationship between climate change, rising sea levels, and deep-water channels beneath glaciers in Greenland and Antarctica use Cryoegg, a remote wireless sensor that continuously monitors temperature, pressure, and electrical connectivity (figure 4). Cryoegg eliminates the need for bulky and expensive cables that can be easily damaged by glacial movement. Bobbin-type LiSOCl₂ cells were specified due to their high capacity, high energy density, wide temperature range, and high pulse capabilities.

Cryoegg utilizes the same 169 MHz wireless M-Bus radio waves found in automated meter reading and advanced metering infrastructure water and gas utility meter transmitter units (MTUs). Bobbin-type LiSOCl₂ batteries lower the cost of ownership of a water or gas MTU by preventing widespread battery failures that can disrupt billing systems and disable remote startup/shutoff capabilities.

**Oceantronics**: To simplify the transport of scientific equipment across the Artic, Oceantronics redesigned the battery pack for its GPS/
ice buoy by replacing a huge battery pack consisting of 380 alkaline D cells with a more compact, lighter, and cost-efficient solution using 32 bobbin-type LiSOCl₂ cells and four HLCs. The company achieved a 90 percent reduction in size and weight (54 kg down to 3.2 kg), enabling the GPS/ice buoy to be more easily transported by helicopter. Converting from alkaline to LiSOCl₂ chemistry also multiplied the device’s operating life manifolds.

Southwire: Reducing size and weight is highly beneficial to utility line crews installing line/connector sensors that monitor temperature, catenary, and line current on utility power lines to warn if a transmission line goes down. Use of bobbin-type LiSOCl₂ cells enables a more compact and lightweight (3.5 lb) solution that can handle extreme temperatures (–40°C to 50°C), providing months of backup power if no line current is detected.

Long-life energy harvesting applications growing

While primary batteries continue to dominate, we are also seeing a dramatic rise in applications that draw milliamps of current, enough to quickly exhaust a primary lithium battery. Returning to our runner analogy, these applications burn up more calories, thus requiring the use of an energy-harvesting device in tandem with an industrial-grade rechargeable lithium-ion battery.

For example, Cattlewatch combines small solar (PV) panels and Li-ion batteries to create a mesh network that tracks the location, health, and safety of animal herds. Similarly, solar/Li-ion hybrids power smart meters that collect parking fees and are equipped with AI-enabled sensors to communicate when open parking spots become available (figure 5).

Low-cost, consumer-grade rechargeable Li-ion cells cannot run such applications because of their relatively short operating life (five years and 500 recharge cycles), a limited temperature range (0–40°C), and their inability to deliver high pulses. By contrast, industrial-grade Li-ion batteries can operate...
up to 20 years and 5,000 full recharge cycles, featuring an expanded temperature range (−40° to 85°C) and the ability to deliver periodic high pulses to power two-way wireless communications (table 2).

<table>
<thead>
<tr>
<th></th>
<th>TLI-1550 (AA) Industrial grade</th>
<th>Li-ion 18650</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diameter (max) [cm]</td>
<td>1.51</td>
<td>1.86</td>
</tr>
<tr>
<td>Length (max) [cm]</td>
<td>5.30</td>
<td>6.52</td>
</tr>
<tr>
<td>Volume [cc]</td>
<td>9.49</td>
<td>17.71</td>
</tr>
<tr>
<td>Nominal voltage [V]</td>
<td>3.7</td>
<td>3.7</td>
</tr>
<tr>
<td>Max discharge rate [C]</td>
<td>15 C</td>
<td>1.6 C</td>
</tr>
<tr>
<td>Max continuous discharge current [A]</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Capacity [mAh]</td>
<td>Up to 1000</td>
<td>3000</td>
</tr>
<tr>
<td>Energy density [Wh/l]</td>
<td>129</td>
<td>627</td>
</tr>
<tr>
<td>Power [RT] [W/liter]</td>
<td>1950</td>
<td>1045</td>
</tr>
<tr>
<td>Power [-20C] [W/liter]</td>
<td>&gt; 630</td>
<td>&lt; 170</td>
</tr>
<tr>
<td>Operating temperature deg. C</td>
<td>−40 to +90</td>
<td>−20 to +60</td>
</tr>
<tr>
<td>Charging temperature deg. C</td>
<td>−40 to +85</td>
<td>0 to +45</td>
</tr>
<tr>
<td>Self-discharge rate [%/year]</td>
<td>&lt;5</td>
<td>&lt;20</td>
</tr>
<tr>
<td>Cycle life [100% DOD] [Years]</td>
<td>&gt;5000</td>
<td>&gt;300</td>
</tr>
<tr>
<td>Cycle life [75% DOD] [Years]</td>
<td>&gt;6250</td>
<td>&gt;400</td>
</tr>
<tr>
<td>Cycle life [50% DOD] [Years]</td>
<td>&gt;10000</td>
<td>&gt;650</td>
</tr>
</tbody>
</table>

Table 2.

In the long run, it often pays to specify an extended life battery to increase product reliability while also reducing the total cost of ownership.

ABOUT THE AUTHOR

Sol Jacobs is VP and general manager of Tadiran Batteries. He has more than 30 years of experience in powering remote devices. His educational background includes a BS in engineering and an MBA.
Industrial Cybersecurity is a Global Imperative

It’s time to join forces. We are stronger together.

The ISA Global Cybersecurity Alliance is an open, collaborative body. We welcome members of all kinds:

- end-user companies
- asset owners
- automation and control systems vendors
- cybersecurity technology vendors
- IT infrastructure vendors
- services providers
- system integrators
- industry organizations
- government agencies
- insurance companies
- other stakeholders

Founding Members:

[Logos of various companies]
Conquering the Cloud with OPC UA

This vendor-independent standard can take your designs from the device to the cloud and back, protecting your automation investment.

Exchanging data between Industrial Internet of Things (IIoT) devices and the cloud presents a bewildering array of options. Cloud providers, Amazon Web Services, Microsoft Azure, Google IO, and many others each advocate for their own technique for IIoT data interchange.

There is a confusing hodgepodge of different approaches. IIoT "standards" such as MQTT, AMQP, REST, and Kafka compete to serve as pipelines to move data across the network. The machine-readable format of the data, usually defined in XML or JSON and different for each solution, creates a custom protocol that may not be ideally suited for

By Jim Redman,
ErgoTech Systems, Inc.
automation data. These cloud vendor–specific solutions have, in turn, caused a proliferation of “gateways” with multiple vendors promoting different methods as a way to transfer data to the cloud.

Custom implementations from IIoT/edge/cloud software and hardware vendors cause a “vendor lock,” limiting your choices and flexibility. Operational technology (OT) applications have a very long life, and in the fast-moving world of cloud IT some solutions are likely to be orphaned.

We have been here before. Historically vendors would sell programmable logic controllers (PLCs) and automation products with proprietary interfaces that worked only with their software. What changed the landscape then is a clear solution to our current dilemma—OPC.

There is no reason for the cloud to be intimidating or complex. There is one technology you already know that will take your designs from device to cloud and back, and that’s OPC UA.

**OPC Unified Architecture – A complete redesign**

OPC has come a long way from the original Windows-centric, network unfriendly, insecure, legacy standard of the late 1990s. The most recent OPC specification—OPC UA—continues to be very widely supported and provides access to almost any field device. It is the preferred way to share data with factory automation software and is implemented by many vendors.

The redesign of the OPC standard was much more than a modernization of the legacy standard. With many years of experience in the OT field, the OPC UA standard kept the utility and capabilities of the legacy standard while addressing the limitations. The importance of IIoT and the continuing growth of the cloud may not have been obvious when the *OPC Unified Architecture* standard was first published in 2006, but some prescient decisions help make OPC UA a natural choice for the entire cloud environment. The most obvious is that OPC UA is cross-platform and provides secure-by-design network communications.
OPC has always been targeted at automation data—a continuous stream of values that we need to share between applications to populate user interfaces and trends and from which we need to extract alarms and anomalies. OPC reflects the reality of the OT environment. Each tag or data point has descriptive metadata including valuable text descriptions of the point, units, ranges, locations, etc. Critical for good OT data management are a quality indicator and the time stamp of the actual reading—not the time it was uploaded. As obvious and vital as all these requirements are for OT data, many widely adopted protocols and custom cloud/IIoT solutions do not include these essential aspects.

Security is always a priority whenever data is passed across a network. OPC UA security is based on state-of-the-art IT best practices, but you do not have to understand the intricacies to deliver a secure solution. Security is an integral part of the standard and is part of all OPC UA clients and servers. OT professionals, with reasonable care and understanding, can ensure a secure OPC system end-to-end—indeed, if you have already installed and configured any OPC UA solution you know the procedure.

OPC UA, like legacy OPC, supports subscriptions and on-data-change notifications. Clients can subscribe to the server and receive notification of tags that have changed in real time. This service has been enhanced so that on-data-change notifications are queued at the server. If there is a short network outage, the server will maintain the notifications for the client and deliver them in order when the client can receive them. Another addition to the standard is the “HistoryRead” service. Clients can request data starting from a particular date and time, allowing data notifications that were missed during a more major network issue to be retrieved once the network connection is reestablished.
Communication is always initiated by the client. Data requests from the client use a technique similar to the well-understood web concept of a “long poll.” Normally, when we consider polling, we think of constant periodic requests to a PLC for the current value. With large datasets this is inefficient and can use a lot of bandwidth. In a long poll from the client, the server will not immediately return the current values, but wait, either until values are available or a timeout has expired. This approach maintains efficiency but still leaves the client in control. The client sets the timeout, which is essentially a heartbeat ensuring that the communication between client and server is healthy. This behavior, always initiating the connection from the client, is transparent to the user, but is consistent with a modern web/HTTPS architecture. More importantly, it allows redundancy and replication of the server.

Cloud deployment

You are likely familiar with using OPC UA locally—running OPC clients and servers, and frequently databases, within a facility for monitoring and data sharing. Conceptually, very little changes as these servers are moved to the cloud. It is a simple and obvious extension to leverage OPC UA technology on remote platforms.

Moving the servers off the local computer has huge potential for cost savings and security improvements. A 24/7/365 team of IT and security experts manage systems in the cloud at a scale that few organizations could justify internally. Computers and operating systems are updated and patched as needed. Applications are protected behind cloud components that are constantly monitored for security issues. Cloud data centers are physically secure systems—protected from break in and theft of...
hardware. Intruders must break these defenses before they can attack your data. These benefits are all part of the cost of the services, which are generally less than the costs of providing an in-house system.

The OPC UA server in the cloud is accessible from any authorized OPC UA client, worldwide. All communications with the server are secured and encrypted. We need to understand only one protocol from device to cloud and back with the obvious cost savings and benefits that come with familiarity. The expertise to make connections and transfer data is likely already available in-house—you do not need to outsource to IT developers.

In applications that have exposure to the Internet—almost all SCADA and remote monitoring systems—the security benefits and cost savings of the cloud are compelling. Maintaining OPC servers 24/7 on remote customer sites can be costly. The never-ending need to patch these systems and the potential for hardware failure of a system that is long obsolete are distractions, not central OT tasks. Providing secure access to these systems adds to these challenges. Many failures in this area are often very public and costly for all concerned. Everyone must be responsible for the security of a system, but leveraging the expertise, vigilance, and capabilities of cloud deployment removes some of the burden from OT.

In applications that have exposure to the Internet—almost all SCADA and remote monitoring systems—the security benefits and cost savings of the cloud are compelling.

Moving IT infrastructure off site and making it available worldwide in the cloud provides advantages to organizations like sharing data between multiple facilities or tracking remote assets anywhere in the world. Although the physical location of the computer hosting the OPC UA server is relatively unimportant, it is nonetheless possible to host the server geographically close to the assets or facilities being monitored. This can help with compliance to local data requirements by hosting the data in the country of origin.
Moving the server off premises also encourages a natural network segmentation. Systems that only need to communicate with the cloud can be "logically" removed from the facilities network. These systems remain physically connected—they are using the same cables—but viruses, Trojans, and other malware cannot easily travel between the "virtual LANs" (VLANs). Cyberattacks are becoming more common and more sophisticated, but a great many start with social engineering attacks through email—phishing and spear phishing emails that seem legitimate enough that the end user opens them and inadvertently releases a malware attack. There is no single solution, but a remote OPC UA server is more isolated from these attacks and helps guide good security practices throughout the installation.

**Scaling up**

Using OPC UA servers deployed in the cloud increases security and lowers cost. A cloud-based OPC UA server eliminates proprietary solutions and removes the need for custom gateways and vendor-specific implementations. This leaves you free to choose your cloud provider or to use multiple providers for different projects based on customer preference—and you can change provider. Overwhelmingly, the features of the OPC UA standard match the requirements for a cloud-based deployment—they provide the features we need and already have near-universal support among OT providers.

Cloud resources are generally far more reliable than in-house computers. Failures are rare, and intense system monitoring often provides notice of potential hardware failures so that applications can be moved before the hardware fails completely. You can choose a convenient time to migrate to a healthy system. Cloud data centers have multiple network connections and backup power from both grid-connected and on-site generation.

For very high availability, multiple servers can be deployed. The standard has guidance on redundancy for both clients and servers. In the case of OPC servers, redundancy options include transparent failover—the clients are unaware that a single server has failed and can continue
to be served by an alternate server. This architecture permits multiple live servers in the cloud—replication rather than simple redundancy. Multiple servers can provide load balancing and, as a result, additional performance. To protect against the failure of a single data center, servers can be deployed within an “availability zone”—independent but closely located data centers connected together on a very high speed network, or across “regions”—distinct geographical locations.

Deploying at scale will also generally require limiting tag access—not all clients should have access to the entire collection of tags. This is the cloud concept of “tenancy”—deploying a resource that will be used by multiple groups. OPC defines role-based access limits that can allow all, read, write or no access to tags based on the role defined by the OPC client.
OPC UA is a collection of specifications. The primary specification, and by far the most widely implemented and recognized, is the “Data Access” standard. Other standards are gaining industry support. Of particular interest in the cloud is the “Historical Data Access” (OPC HDA) specification. This extends the OPC server to include reading and writing historical data as well as real-time transfers. Databases are a huge component of almost any cloud architecture. Modern simple-to-use cloud database dashboards let you set up and configure everything from a small historian to enterprise storage with replication, redundancy, and data encryption. HDA allows any OPC client to use these cloud databases in a transparent, database-independent fashion. This allows you to select different databases based on customer preference or project requirements.

A recent addition to the OPC standard is the “publish-subscribe” model. This provides features similar to the Data Access model with some additional performance and lower overhead. This standard further enhances the benefits of OPC UA in the cloud.

Robust cloud applications

OPC UA makes using the cloud easy and safe. You already know OPC and can create secure, robust cloud and IIoT applications. Moving application data to the cloud lets you do your job better while saving cost and lowering security risks. A vendor-independent, widely implemented standard ensures long-term support and protects your investment in a rapidly changing cloud environment.

ABOUT THE AUTHOR

Jim Redman, as president of ErgoTech Systems, Inc., was delivering what has become “IIoT” systems way back in 1998. ErgoTech’s MISTudio suite reflects his holistic vision to provide a single tool for integration and visualization from sensor to AI, and from tiny IIoT to worldwide cloud. Jim can be reached at jredman@ergotech.com.
Upstream Data Analytics Virtual Conference
22 February
Learn the principles behind creating a robust, strategic data analytics program to modernize unconventional drilling applications. Sessions and workshops led by industry experts will teach you how to move beyond the collection and formatting of raw data and start driving real-time performance improvements.

Analysis Division Virtual Conference
23 March
Gain a fresh view of important regulatory topics, best practices, and emerging trends in process analysis. Peer-reviewed presentations will cover spectroscopy, chromatography, electrochemistry, and sample handling, while featuring advice and lessons learned in today’s challenging environment.

IIoT & Smart Manufacturing Conference
11 May
Achieve a better understanding of the latest advances in connectivity, automation, and cybersecurity – and how you can leverage these technologies to optimize processes. Through end user case studies and dynamic panel discussions, you will explore challenges faced in adoption, integration, and implementation of new technical solutions.

Digital Transformation Virtual Conference
31 August
Learn from the world’s top manufacturing companies as they share best practices for leveraging new technologies to make capital-intensive projects viable. Sessions will explore the benefits of digital transformation, including accelerating design processes, improving safety and efficiency, speeding up commissioning and startup, improving uptime, and minimizing operational risks.

Cybersecurity Standards Implementation Virtual Conference
19 October
Explore the best practices and lessons learned from hundreds of end user application as they showcase the tried-and-true approaches for securing automation and control systems across dozens of industry segments. Sessions and panel discussions in this interactive event will explore the lifecycle of OT cybersecurity projects, along with the roles and responsibilities of end users, product suppliers, system integrators, and maintenance providers.

Process Industry Virtual Conference
2 November
Find clarity around ever-evolving technologies and explore what’s next in process manufacturing. Peer-reviewed sessions, panel discussions, and one-on-one networking opportunities will ensure that you walk away with practical advice to improve performance, increase productivity, and ensure the safety and security of facilities and processes.

Learn more at: isa.org/virtualevents
Modernas award-winning cGMP clinical development manufacturing facility—based in Norwood, Mass.—has a native digital process automation design built on Amazon Web Services (AWS). It is a great example of the integration of an entire manufacturing business using the latest technological building blocks, architecture, and Internet of Things (IoT) ecosystem and is reflective of the company’s culture to be “bold, relentless, collaborative, and curious.”

“In 2019, the facility was named Facility of the Year by the International Society for Pharmaceutical Engineering (ISPE),” said Roland Smith, senior director, Digital GxP Systems, Moderna. “What differentiated the site, according to ISPE, was fully integrated native digital manufacturing capabilities built on AWS.”
The Moderna native digital process automation design eliminates the large divide between business systems and production that in the past meant disjointed and unsynchronized operations, resulting in inefficiencies from supply chain to the customers. Major goals achieved include:

- better data – better decisions
- innovation within the existing workflow
- prediction – identifying the process variables that are related to an outcome
- better real-time process modeling, simulation, and visibility
- maximized operator performance.

Roland Smith, senior director, Digital GxP Systems, Moderna, described the architecture at the AWS re:Invent 2019 event. See the video from the event, Modernizing pharmaceutical manufacturing with IoT and AI/ML [MFG203], for more details.
About Facility of the Year Awards

Established in 2004, the Facility of the Year Awards (FOYA) recognize state-of-the-art projects using innovative technologies to improve the quality of products, reduce the cost of producing high-quality medicines, and demonstrate advances in project delivery. The FOYA program is a platform for the pharmaceutical science and manufacturing industry to showcase its accomplishments in facility design, construction, and operation, while sharing the development of new applications of technology and cutting-edge approaches.

The International Society for Pharmaceutical Engineering is a large not-for-profit association serving its members through leading scientific, technical, and regulatory advancement across the entire pharmaceutical life cycle. The 18,500 members of ISPE are building solutions in the development and manufacture of safe, effective pharmaceutical and biologic medicines and medical delivery devices in more than 90 countries. Founded in 1980, ISPE has its worldwide headquarters and training center in North Bethesda, Md., and its operations center in Tampa, Fla. Visit http://www.ISPE.org for more information or view the video of the 2019 ISPE Facility of the Year Awards Category Winner for Facility of the Future – Moderna, Inc.

Key success factors

Smith noted key factors for success in his presentation at the event:

- Top management’s support of the digital commitment really makes the discussion of digital at Moderna not an “if” but a “when.” Removing those headwinds allows the company to move faster and with lower costs in its digital transformation.

- A unique operating model removes organizational silos. For example, Smith’s group owns digital, shop floor automation,
and analytics. That allows them to rapidly improve as they see opportunities to streamline or make data more consistent.

- The company strongly believes the user experience and lean principles go hand in hand. If you make an operator’s job easier, the process will inherently be more efficient.

- Be very data-driven; believing in the value of collecting data is key to the company’s future success.

- Design a future-proof ecosystem built on AWS.

- There are no members of the team who are not currently working on at least one side innovation project that will disrupt how they will normally work.

- From the start, the company has tried to integrate all of its systems to eliminate nonvalue added manual transcription and to improve data consistency. Currently, it has more than 200 integrations across the digital systems.

- The company has more than 40 integrated robots and 100 integrated pieces of process equipment. Analytics and learning are built into everything. Integrating data into everything accelerates insight and improves data quality.
Bringing cloud to operations

Smith discussed how many of his peers are trying to take operations to the cloud, but at Moderna they are bringing the cloud to operations. Smith noted about 95 percent of their digital landscape computing capacity resides on the cloud, primarily on AWS. Data is housed in Amazon Redshift cloud data warehouse or in what some would term a “data lake.”

Democratization of manufacturing data

Integrated analytics strategy

Lessons learned

- Lesson learned 1: Start with a strategy based on a shared landscape and vision of the native digital manufacturing site.
- Lesson learned 2: Partner with quality early, define common operating procedures and a clear testing methodology, and set guidelines to ensure compliance.
Lesson learned 3: Integrate vendors into your culture. Most vendors want everything completely defined before starting, but when you are trying to do something innovative and new, this approach will not achieve the goal. Working collaboratively and trying new things, including some that failed, actually improved results and meeting our timelines.

This story was originally posted on Automation.com.

ABOUT THE AUTHOR

Bill Lydon brings more than 10 years of writing and editing expertise to Automation.com, plus more than 25 years of experience designing and applying technology in the automation and controls industry. Lydon started his career as a designer of computer-based machine tool controls; in other positions, he applied programmable logic controllers and process control technology. In addition to working at various large companies (e.g., Sundstrand, Johnson Controls, and Wago), Lydon served a two-year stint as part of a five-person task group, where he designed controls, automation systems, and software for chiller and boiler plant optimization. He was also a product manager for a multi-million-dollar controls and automation product line and president of an industrial control software company.

More Information from AWS

A video from Amazon Web Services re:Invent 2019 provides more information on modernizing pharmaceutical manufacturing with IoT, artificial intelligence, and machine learning. View the video.
IT/OT Convergence Delivers a Growing Range of Benefits

By Masaru Yamazaki and Chigusa Akana, Yokogawa

New digital technologies can provide significant operational improvements, but connectivity and cybersecurity concerns must be addressed.

As digital technologies for process industries have evolved, they have brought a growing number of benefits to process plant operations and operators. The pace of change started picking up in the 1990s when distributed control systems (DCSs) and supervisory control and data acquisition (SCADA) systems began to switch from proprietary operating systems to general-purpose environments such as UNIX and Microsoft Windows. This made it possible to shift to available commercial off-the-shelf (COTS) products and to store large amounts of data over long periods on large-capacity hard-disk drives.

Powerful Windows-based software platforms, borrowed and adapted from the commercial domain, made it far easier to create reports and analyze data. This made it possible to create applications including plant information management systems (PIMS), along with manufacturing operations...
management (MOM) and manufacturing execution systems (MES). Tools became available to capture operational data, store it for long durations, process it, analyze it, and utilize the improvements it yielded in daily operations. Expanded networking capabilities combined with COTS software created hazards in the form of a larger potential cyberattack surface, but this software also provided new types of tools to protect networks and harden applications and platforms.

By using the combined effects of the network technology improvements, process plants and facilities can now be monitored over a wide area. SCADA systems are used to monitor far-flung oil and gas wells, extensive pipelines, and other assets (figure 1). As a result, it is possible to share information with multiple functional areas simultaneously:

- on-site operators
- field specialists, regardless of their location
- engineering specialists (process, mechanical, electrical, etc.)

Figure 1. New networking capabilities make it easier for SCADA systems to cover far-flung assets.
information and operations technology (IT and OT) software and networking specialists

business divisions.

Maintenance tasks have also evolved through this time. In the 1990s, communication standards for field equipment, such as FOUNDATION Fieldbus and HART, were born, providing new ways for maintenance and operations to obtain data through the network. Maintenance data are now used in plant equipment management (PAM) software applications. PAM captures, historizes, and analyzes data from field instruments, control systems, and various sensors—making it possible to predict potential equipment failures.

The ways in which plants and companies use the tools and embrace the benefits resulting from this evolutionary process vary widely, although the direction industrywide is positive. Knowing the extent to which these benefits can be effectively utilized occupies an important role in plant operations, and the tendency toward their utilization is expected to become even stronger in the future.

Yokogawa provides software and services that use data handled by DCS and SCADA platforms. These are built on the FAST/TOOLS software for CENTUM VP and SCADA integrated production control systems. We think that their importance will continue to increase, because they not only provide significant benefits but also address connectivity and cybersecurity concerns.

Digital transformation

Let’s think about several developments of the past decade or so and see how they work together.

The Internet of Things (IoT) and its industrial version (IIoT) have added millions upon millions of devices connected by the Internet.

Countless terabytes of operational data can be easily stored in the cloud.
Functions using artificial intelligence (AI) are now operating in industrial environments.

Software is increasingly supported in the cloud and utilized as a service rather than purchased.

When those changes are brought together and used in concert, we call it digital transformation (DX). This has become a crucial issue for many companies as they explore how to utilize these new digital technologies. Such discussions often have a high sense of urgency stemming from a belief that companies unable to make sufficient progress will lose competitive strength and business continuity.

So how can DX be realized in a process manufacturing environment? Often a first step is using the IIoT to connect all the equipment to plant networks for mutual communication among all nodes. By installing IIoT sensors for maintenance on all equipment and manufacturing assets in the plant, it is possible to acquire data such as vibration, surface temperature, pressure, and a wide range of other variables. Based on this acquired data, equipment condition can be determined, which delivers multiple benefits. It reduces the need for manual inspections, and it helps detect equipment abnormalities early, thereby avoiding downtime due to unexpected equipment failures.

Many industrial plants and facilities are also actively looking at other new digital technologies such as virtualization, moving more functions to the cloud, creating digital twins, and using AI as a data analysis tool. However, according to a report by the Japanese Ministry of Economy, Trade, and Industry, many companies have not quite been able to realize transformation using these new technologies alone.

The key to successful DX is to not only utilize plant operation data with digital technology but to also apply the results obtained. Data must be analyzed on a continuous basis to improve plant operations, and the results must be fed back for digital processing, with continuous improvement resulting from this feedback loop structure. The key to making it happen is the convergence and fusion of IT and OT.
Collaborative information server

To facilitate this fusion Yokogawa has launched its Collaborative Information Server (CI Server) as a new product that achieves IT/OT convergence. The CI Server is a software platform (figure 2) that applies plant operation support technology, which was cultivated through the development of Yokogawa’s CENTUM VP DCS and FAST/TOOLS SCADA systems. The CI Server was developed to create mechanisms so plant operations can effectively utilize digital technology.

The platform comprises several key elements:

- a web server that acts as a data server for sending and receiving data to and from external applications and systems
- a human-machine interface (HMI) that supports HTML5 and various work environments
- connectivity between the data server and the HMI
- cybersecurity functions to control access and detect unauthorized network activity.

The CI Server supports redundant configurations and provides a reliable and highly stable environment. Wide-area communication is possible, as well integrating distant plants and remotely monitoring their operations. It comes with communication protocols such as Modbus and IEC 61850, communication drivers for controllers such as major PLCs, and an MQTT interface that is growing in popularity for supporting data gathering from IIoT sensors. Therefore, not only can process data and alarms be acquired from the control system, but also data from the facilities and systems that manage various other equipment and devices.

The CI Server supports OPC UA, which is also gaining attention as a versatile communication protocol. OPC UA enables efficient interconnection and information linkage between a control system and external systems, applications, and devices. Compared to conventional OPC Classic, the information-model function is greatly improved.

The information-model function takes operations data, which was previously treated as grains of individual numerical values or character strings, and handles it as a collection that is organized and structured through mutual associations. Deciding in advance on the information model to be used eliminates the work of associating address numbers and I/O numbers. Previously, this work was required for interconnection, but now OPC UA enables connectivity among external systems, applications, devices, and other entities with very high efficiency.

Building an information model reduces the subsequent cost and labor of organizing information. This makes it possible for IT to handle OT-specific information in a mutually shared format, where previously this was difficult for IT technology to address. It improves efficiency and brings benefits obtained on the IT side back to the OT side.
The CI Server realizes IT/OT convergence through highly efficient cooperation between the two sides via OPC UA. It is now possible to provide the right information to the right person quickly to support more effective decision making. Companies can optimize costs, improve quality, improve operational efficiency, and respond rapidly to market changes.

Protection against cyberintrusions comes from a combination of strategies to provide defense-in-depth. First, networks have compartmentalized access, balanced to provide information to those who need it while limiting unnecessary access. Second, new software platforms have more protections built in. Third, network traffic is monitored to detect suspicious activity outside of normal operations. Industrial networks generally have routine patterns of activity, and when odd things happen, they may signal unauthorized access.

**Fusion of the CI Server with digital technology**

New value is created by fusing the data collected on the CI Server with new digital technologies such as the cloud, digital twins, and AI. For example, consider a digital twin Mirror Plant based on the Omega Land dynamic simulator developed by our Yokogawa group company, Omega Simulation.

A Mirror Plant acquires process and operations data in real time from the control system of its corresponding actual plant and uses
Figure 3. A Mirror Plant responds just like the real counterpart, allowing operators to test process changes and adjustments.

This information to perform a dynamic simulation (figure 3). Because all the state quantities of the Mirror Plant’s model are calculated, one can determine the flow, temperature, pressure, level, and composition in the equipment and piping. It is then possible to visualize state quantities that have not been measured in the actual plant and to create alerts.

Similarly, when an action is difficult to perform in an actual plant, or when it is necessary to change a specific parameter and check its effect, a high-speed simulation can predict the outcomes. Information obtained from the Mirror Plant can also be incorporated into the HMI of the CI Server.

A Mirror Plant makes it possible to visualize things inside the process that are not normally accessible, predict future behavior of the plant, reduce operator load, and promote stable operation. In this way, the CI Server has the potential to create new value by fusing with new digital technologies from a variety of providers.
Looking ahead

With the evolution of digital technology, plant control has begun to shift from traditional industrial automation systems, such as DCS and SCADA, to autonomous control. This change to industrial autonomy means that all processes, from startup to stop, are controlled by the judgment of the system itself, with greatly reduced need for operator intervention.

Figure 4. Robots are rapidly improving and taking on tasks too dangerous or repetitive for humans.
As autonomy advances, the routine work that humans have traditionally done can be reduced, with saved time and effort allocated to working on higher value-added tasks. Automating tasks that are difficult for humans to perform also leads to improved health, safety, and environmental results.

Two critical elements are required to reach these goals: proving the autonomous judgment of the system, and the development of robots that can perform the actual work in place of humans (figure 4).

Yokogawa is promoting industrial automation to industrial autonomy as a roadmap to realize this major advance. As a step toward reaching this goal, the CI Server helps improve the autonomous ability of systems by fusing plant data and digital technology, while simultaneously enabling IT/OT convergence.

This article originally appeared online at Automation.com.

All figures courtesy of Yokogawa

ABOUT THE AUTHORS

Masaru Yamazaki is the system business and products planning manager for Yokogawa Electric Corporation. He was a system and sales engineer for integrated control and systems for more than 30 years and is now responsible for system business and products planning. Yamazaki graduated from Seikei University with a master’s degree in information engineering.

Chigusa Akana has worked at Yokogawa for 10 years as the person in charge of web digital content for the marketing of products such as PLCs, DCSs, and other automation systems. Akana graduated from the University of Rikkyo with a degree in economics.