INTERNET

THINGS

2017: State of the IIoT

Key Trends and Predictions for the Industrial Internet of Things

OPTO 22
www.opto22.com

Opto 22

43044 Business Park Drive • Temecula • CA 92590-3614
Phone: **800-321-6786** or **951-695-3000**
Pre-sales Engineering is free.
Product Support is free.
www.opto22.com

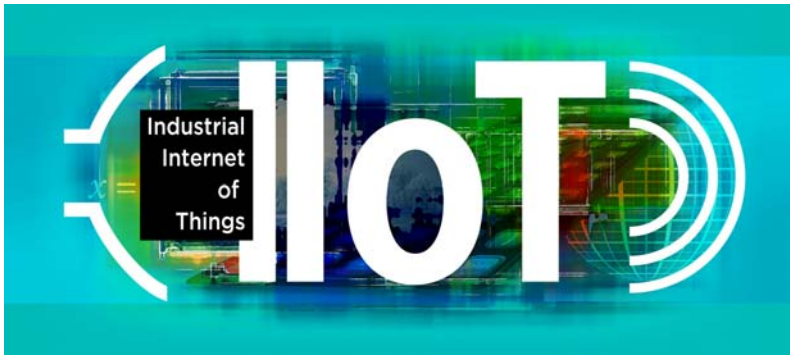
Form 2215-170303

2017: State of the IIoT

Key Trends and Predictions for the Industrial Internet of Things

The next industrial revolution, the Industrial Internet of Things, is happening now.

Here is a summary of the key IIoT trends from 2016, with predictions and recommendations for 2017.



State of the IIoT

Across the world, the industrial, manufacturing, and automation industries are in the midst of a massive shift in technology and culture.

Terms like predictive maintenance, artificial intelligence, smart manufacturing, and augmented and virtual reality are no longer buzzwords. They're ideas, technologies, and concepts that are being adopted and applied to these industries every day.

From the intelligent building that automatically optimizes its HVAC and lighting systems for occupancy and reduced energy usage, to the heavy machinery that predicts internal part failure and schedules its own maintenance call, the Industrial Internet of Things (IIoT) is here. And it's only picking up momentum as time passes.

Through 2015 and 2016, the number of IIoT market-growth predictions only increased. And the size of the market seemed to increase with each prediction.

In 2015, research firm Accenture claimed that the IIoT could increase GDP in 20 economies by a total of $10.6 trillion by the year 2030. Their research was based on 2015 IIoT investment trends. Accenture further stated that with more investment, the potential growth is even greater.

Industry giants like General Electric® are making significant investments in IIoT technology. GE® expects total industry investment in the IIoT to top 60 trillion dollars over the next 15 years.

Adoption accelerates, but challenges remain

In March 2016, a Gartner® survey reported that 43% of organizations were already using or planned to implement IIoT applications during the year.

Early adopters of the IIoT have identified competitive advantages and new business models to increase revenue, cut costs, and improve customer service and support. But IIoT adoption challenges remain.

A continuing trend in the IIoT is the need for two different organizational groups within the enterprise to begin working together. For the potential benefits of IIoT applications to be realized, the information technology (IT) and operations technology (OT) teams need to begin leveraging and applying each other's technology and skillsets. This continues to be a challenge on both the technical and cultural fronts.

OT and IT teams exhibit significant cultural differences within their organizational units.

IT

IT lives in a world of constant change and never-ending upgrade cycles, seeking the newest, fastest computing hardware and software to gain some competitive advantage the enterprise can use to its benefit.

IT is tasked with protecting the enterprise's digital presence and assets, which are under constant attack from both internal and external cyber security threats.

2017: State of the IIoT

The IT team's technology comes from a world of open specifications and well-documented and widely adopted protocols. The IT team operates in the realm of information sharing, securing, and preservation.

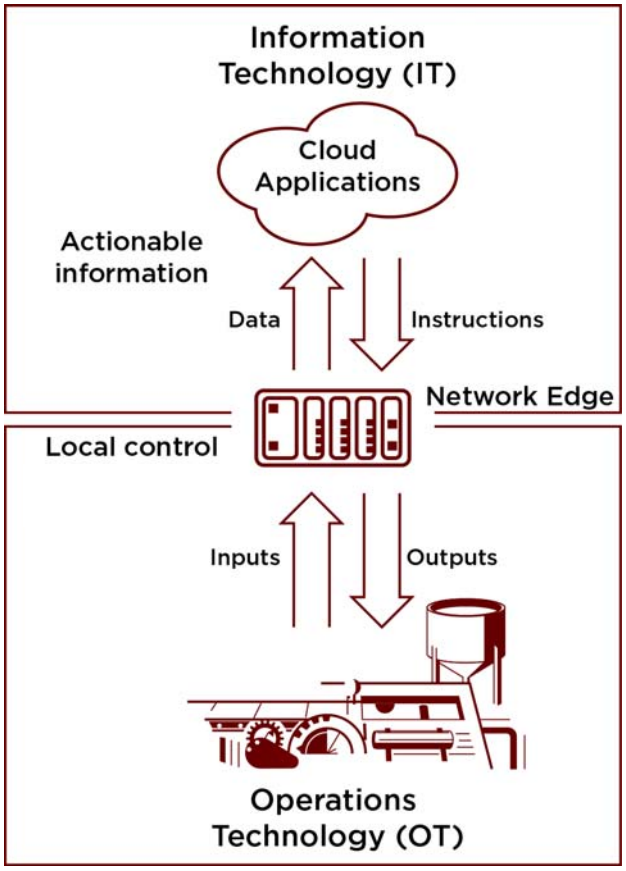
OT

The OT team functions in the realm of physical value creation within the enterprise.

This team handles the installation, maintenance, and occasional upgrade of equipment designed to produce goods that the enterprise sells.

Their capital equipment upgrade cycle is 10, 20, sometimes even 30 years or more. The equipment itself is expensive and often proprietary, having been designed for a specific application or task.

Often this equipment was not designed to interface with systems outside of the application the equipment was designed for. This makes bridging the gap between the physical world of industrial devices and systems and the digital world of the Internet a significant hurdle.



The ongoing challenge lies in connecting these two very different technologies and disciplines. But the primary objective remains: to obtain a holistic historical, real time, and predictive view of enterprise-wide operations, in order to identify opportunities to develop competitive and comparative advantages.

Recommendation

Bringing the IT and OT teams together is a challenging task. Each team uses a different set of technology and tools, and their cultures and missions are drastically different from one another.

With the current IIoT adoption rate and its projected growth only increasing, organizations that intend to remain competitive—or to surpass their competition—must research, design, and roll out an IIoT strategy.

One recommendation to help streamline this process is to have a single individual within the organization own the overall development of an IIoT strategy, with supporting efforts coming from all organizational units.

The individual responsible for leading this effort should not come from a strictly OT or IT background. Instead, this person should be well versed in both the OT and IT realms and be able to understand the overall business objectives and long-term value in connecting OT assets and IT assets together.

It's also imperative that this individual be well versed in information security, to ensure that the organization's assets and systems on both the OT and IT sides of IIoT applications are protected against cyber security threats.

This individual might have a job title of DevOps Lead, Data Engineer, IIoT Architect, Emerging Technologist, or IIoT Manager. A potential organizational architecture is to have both the OT and the IT team roll up under one single IIoT department.

An IIoT strategy is half baked if it comes from only one of these two organizational units, because both are required for a successful IIoT strategy development and rollout. The key to successful management of OT and IT teams for IIoT is that both the teams have an equal seat at the engineering, design, production, and support tables.

The adoption of open IIoT standards, specifications, and architectures will also help streamline teamwork between OT and IT.

An IIoT strategy is half baked if it comes from only OT or only IT. Both teams are required for a successful IIoT strategy development and rollout.

Standards, specifications, and architectures

During 2015 and 2016, two organizations dominated the IIoT headlines:

- **Industrial Internet Consortium (IIC)**, which takes a cross-domain approach to the IIoT
- **Plattform Industrie 4.0**, rooted in the concepts of efficient manufacturing and the smart factory

Both groups developed reference architectures to help streamline the standardization and adoption of IIoT technology. While similar in some respects, they also differ on many points.

Industrial Internet Consortium and the Industrial Internet Reference Architecture

Founding and contributing members of the Industrial Internet Consortium (IIC) include Bosch, EMC2, General Electric, Huawei, Intel®, IBM®, SAP®, Schneider Electric™, and over 150 other companies. The IIC is primarily focused on developing a standard reference architecture to address the overall enterprise that could be adopted globally as opposed to regionally.

The IIC's Industrial Internet Reference Architecture (IIRA) was first published in 2015 and is a standards-based architectural template and methodology that IIoT system architects can use to design their own systems, based on a common framework and concepts.

The IIRA is designed to address the intelligence and connectivity now being built into the sensors, actuators, and other low-level devices deployed in a variety of applications, including smart manufacturing, the smart grid, the connected hospital, smart transportation, and many others.

The objective of the IIRA is to develop an architecture that securely addresses connectivity and communication from sensor to cloud, interoperates between vendors, and works across all industries.

A key component of the IIRA is connectivity. The IIRA's connectivity portion includes a core data bus with gateways to other standards. The central data bus with gateways connects smart machines together into large-scale intelligent systems.

This data-centric connectivity architecture relies on quality-of-service attributes like data delivery, timeliness, ordering, durability, lifespan, fault tolerance, and most importantly, security.

The Industrial Internet Consortium aims to advance the adoption of the Industrial Internet on a global scale with a cross-industry approach. Plattform Industrie 4.0, on the other hand, is shaping a digital structural shift of industry specific to Germany.

Plattform Industrie 4.0

Industrie 4.0 began as a German government project to promote computerized manufacturing. As a result, the primary focus of Industrie 4.0 is to optimize production in an effort to develop what the organization has deemed the smart factory.

For a factory to be considered smart, it must be designed and operated around four key pillars:

- **Interoperability**—Machines, devices, sensors, and people connect and **communicate with one another.**
- **Information** transparency—The systems create a virtual copy of the physical world through sensor data in order to contextualize information.
- **Technical assistance**—The systems support humans in making decisions and solving problems and assist humans with tasks that are too difficult or unsafe.
- **Decentralized decision-making**—Cyber-physical systems make simple decisions on their own and become as autonomous as possible.

Using these four pillars of design and operation, Industrie 4.0 attempts to build smart factories that can mass produce customized products flexibly. Automation technology deployed in smart factories conforming to the Plattform Industrie 4.0 standard would have technology built in to allow for self-optimization, self-configuration, self-diagnosis, cognition, and intelligent support for workers as their work becomes increasingly complex.

2017: State of the IIoT

Recommendation

Conversations between the IIC and Industrie 4.0 have been ongoing since 2015. While there has historically been frustration between the two organizations as to which standard makes the most sense for IIoT architecture, today the IIC and Plattform Industrie 4.0 have developed an ongoing collaboration to:

- Benefit from interoperability of industrial Internet systems from the different domains and maintain a technical exchange
- Identify mappings, differences, and enhancements on both sides
- Formulate requirements for standardization bodies together
- Create a joint testbed for testing architectural elements
- Work together to increase the adoption of the industrial Internet

There is still much debate between the organizations, leaving many companies unsure of where to invest.

At this point a wait-and-see approach is recommended. While it's likely a combined effort between the organizations will eventually materialize and an overall industry standard will be developed, the timeline is currently unknown.

Platforms rising

While the standards bodies continue to debate which protocols, architectures, and terms are best for the Industrial Internet of Things, industry is already beginning to answer the calls of customers looking for IIoT platforms that offer ease of use, security, and interoperability—leading to the rise of the IIoT platform wars.

In a recent developer survey conducted by the Eclipse IoT Working Group, IEEE IoT, and Agile IoT, 40.8% of respondents indicated that the IoT solutions they were either currently building or planning to build are IoT platforms or IoT middleware. Almost every large IT or OT company today has some form of IoT platform or middleware, with the current number of self-described IoT platforms exceeding 150.

IoT platforms and middleware are the software that must exist between physical devices (sensors, actuators, relays, etc.) or data endpoints, and higher-level software applications like artificial intelligence, predictive analytics, and cognitive computing.

IIoT platforms and middleware move data between the physical and digital realms and provide software resources powerful enough to cope with the big data generated from the billions of IIoT devices the industry is planning to ship.

While middleware is not a new technology, the IIoT has given rise to a need for a new type of middleware specifically designed for IIoT applications. IIoT applications require a middleware platform that addresses new concerns, including:

- Scalability
- Edge computing
- Efficient communication architectures
- Protocol support
- Cognitive computing

Scalability

The sheer volume of devices and other data endpoints involved in IIoT applications requires advanced and flexible scalability.

IIoT platforms and middleware need to be optimized to support tens of thousands of devices, all trying to exchange not just information with a central hub server or application but with each of the other devices in the application.

Addressing, configuring, and managing thousands—even tens of thousands—of devices must be accounted for.

Edge computing

Centralized intelligence and control topologies are being reevaluated in favor of distributed architectures, with intelligence pushed into each edge device or data endpoint.

IIoT applications involve thousands of devices intercommunicating, often with the requirement for near-real-time communication and control between devices.

Edge computing uses intelligence at the edge of the network to decrease network latency, deliver real-time control and monitoring, and offer report by exception to reduce data volume.

Efficient communication architectures

Many IIoT applications will be deployed in areas with unreliable and low-bandwidth networks. As a result, a more efficient network and communication architecture will be required.

Protocols like MQTT (Message Queue Telemetry Transport) that employ a publish/subscribe architecture and low-overhead packets can reduce network latency and improve real-time communication speed between devices and endpoints. (More about MQTT later.)

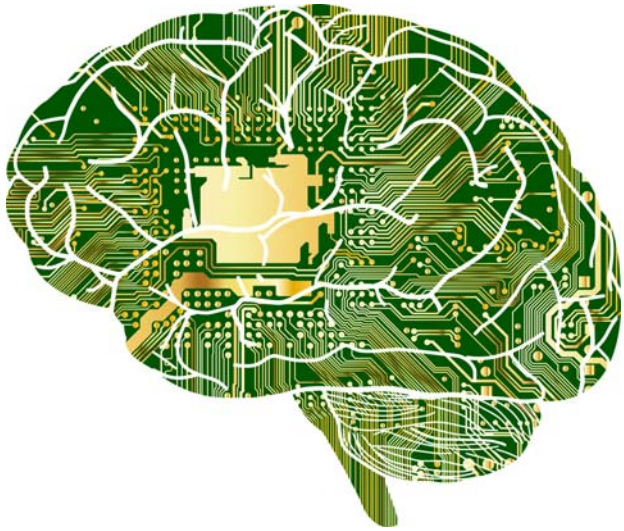
Protocol support

Combining OT and IT technologies requires wide support of different OT and IT protocols.

At least in the short run, both OT and IT protocols need to be translated through middleware, so that OT devices can communicate with IT devices and software.

In the long run, it is likely that OT devices will adopt IT protocols and communication standards, as they've already adopted Ethernet and TCP/IP as the main bus and data transmission protocols.

Knowing when a part is going to fail before it actually fails can bring almost immeasurable value to IIoT applications through reduced truck rolls, safety improvements, and optimizing overall equipment efficiency (OEE).



But there is still a massive installed base of legacy industrial systems that will always require some form of middleware for protocol conversion and connectivity to the IIoT.

Cognitive computing

The key value-add of IIoT applications is predictive analytics.

Knowing when a part is going to fail before it actually fails can bring almost immeasurable value to IIoT applications through reduced truck rolls, safety improvements, and optimizing overall equipment efficiency (OEE).

The basis of predictive analytics is cognitive computing—essentially, computers that mimic the way the human brain works. For IIoT platforms to perform predictive analytics, they'll need support for cognitive computing.

Today and for some years to come, our root problem is that IIoT applications inherently require connecting legacy systems and devices to cutting-edge IT systems. And a massive gap exists in technology, communication protocols, and standards between equipment designed several decades ago and the equipment shipping today.

That's the gap IoT middleware is trying to fill.

Current platform contenders

But IIoT applications are not and should not be designed as a one-size-fits-all solution. Choosing the right IIoT platform depends on what you are trying to achieve in your application.

2017: State of the IIoT

Here are the major IIoT platforms in the market today, their key strengths, and their potential weaknesses.

GE Predix™

Predix uses a platform as a service (PaaS) model and is a cloud-based operating system designed for IIoT applications. According to GE, Predix is built on Cloud Foundry®, an open-source platform, and is optimized for secure connectivity and analytics at scale, both in the cloud and on the edge.

Key Strengths: Predix targets system-wide optimization. Rather than making one piece of equipment better, the software aims to create a detailed model that spans the entire system. The view created by this model allows both improved optimization of each part of the system and optimization of the entire system.

Potential Weakness: Predix in its current form is fairly new to the market, having been released in February 2016. Reports have surfaced claiming that core parts of GE's Predix software rely on partnerships with other companies, including PTC.

Cisco® IoT Cloud

Cisco's offering is designed around six pillars of technology: network connectivity, fog computing, data analytics, security (cyber and physical), management and automation, and application enablement. The Cisco IoT Cloud addresses challenges across a wide variety of industries, including manufacturing, utilities, oil and gas, transportation, mining, and the public sector.

Key Strengths: Cisco has a strong background and support for IIoT applications at layers 1 through 4 and potentially 5 of the OSI model of interconnectivity. This is a wide product offering for general networking and Internet connectivity.

Potential Weakness: Cisco's IoT Cloud lacks direct support for legacy endpoint devices including sensors, instrumentation, and other OT-specific assets. The core function of the Cisco IoT Cloud appears to be network connectivity, with OT integration needs being a lower priority.

IBM Watson IoT™

Another platform as a service based on open standards (Cloud Foundry, Docker®, OpenStack®), Watson IoT Platform is designed to simplify cognitive IoT development. The platform connects sensors to cloud applications using IBM Bluemix®, which includes the Node-RED development environment (an open-source tool for wiring together hardware devices, APIs, and online services).

Key Strengths: IBM Watson IoT leverages both open technologies, such as RESTful API architecture, and in-house-built advanced cognitive computing and artificial intelligence capabilities.

Potential Weakness: Constant internal IBM development cycles can slow down users during application development; current documentation can be missing or hard to find.

PTC® ThingWorx®

PTC Thingworx was recently named by BCC Research as the Internet of Things application enablement platform market share leader with 27% market share. Thingworx has three pillars of technology: core application enablement, connection services with device and cloud adopters, and edge connectivity using the Edge MicroServer and Edge "Always On" SDK.

Key Strengths: PTC's platform architecture takes a holistic approach to connectivity, from end data points and devices all the way to the cloud. Thingworx integrates with cloud providers such as AWS® IoT Service, Microsoft® Azure® IoT Hub, Salesforce® IoT Cloud, and many others and has vast OT protocol support through recent acquisition of Kepware® Technologies.

Potential Weakness: Core features include software tools and products acquired through company acquisitions; internal technology integration pitfalls are a potential concern.

Recommendation

The market is still forming in IIoT platforms. Two considerations to take into account:

- PTC Thingworx currently holds the largest market share for IIoT platforms
- IBM Watson IoT has strong cognitive computing capabilities.

No matter which platform is chosen for any given IIoT application, the key to successful IIoT application development and rollout lies in system interoperability and overcoming software and hardware integration challenges.

Open source and open standards for interoperability solutions

In the recent developer survey conducted by the Eclipse IoT Working Group, IEEE IoT and Agile IoT, almost a third of respondents indicated interoperability as a major concern related to developing IIoT solutions.

While there has been widespread adoption of open communication bus standards like Ethernet for industrial networks and TCP/IP for addressing and data transmission, software applications in the OT and IT realms still lack interoperability.

Here are some current technology solutions to help overcome these hurdles in 2017.

Opto 22 SNAP PAC automation controllers come with a built-in RESTful web server and API.

RESTful APIs

RESTful (REpresentational State Transfer) APIs are the tools that stitch together the Internet and mobile computing as we know them today. Almost every modern application built for the Internet or mobile devices is built using RESTful APIs.

REST is an architectural style for software development. It provides developers with a set of constraints to write their software code against and is the baseline for critical interoperability in IIoT applications.

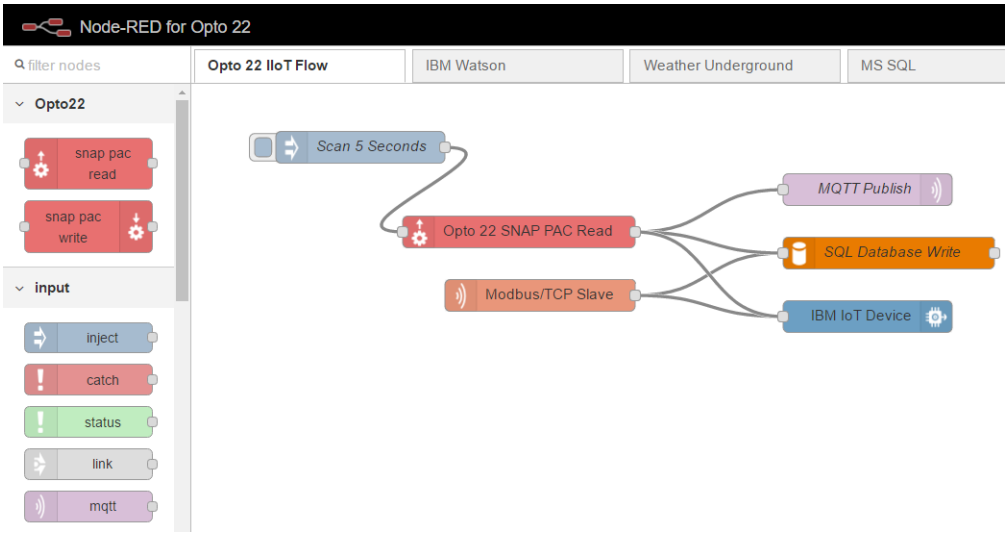
Automation manufacturer Opto 22 chose the REST architectural style when developing its industrial controller API, to ensure interoperability between other web and software applications.

Node-RED

Node-RED is an innovative visual wiring tool to connect edge computing systems such as industrial automation controllers to cloud services such as Amazon Web Services™ (AWS) IoT, IBM Watson IoT, and Microsoft Azure.

An open-source, cross-platform technology available on GitHub.com and npmjs.org, Node-RED is currently available for a variety of platforms, including OS X®, Microsoft Windows®, Linux®, and Raspberry Pi®, and for cloud offerings like IBM Bluemix and AT&T® Flow.

Node-RED benefits from a large library of prebuilt JavaScript(applications—over 500 prebuilt nodes—allowing IIoT application developers to leverage existing software code and deploy it directly into their applications.



A Node-RED flow uses prebuilt nodes to make programming the IIoT easier.

2017: State of the IIoT

Opto 22's *groov* Box includes Node-RED, installed and ready to use.

Opto 22's *groov*® IIoT application development appliance comes with Node-RED natively built in and offers developers a way to rapidly build IIoT applications and mobile operator interfaces.

OPC

In 1996, automation vendors Fisher-Rosemount®, Intellution™, Opto 22, and Rockwell® Software formed a task force to develop a standard for industrial device data access based on Windows COM and DCOM. They named it OLE for Process Control, later shortened to OPC.

OPC was designed to connect applications running on Windows operating systems to industrial automation devices.

The major drawback to OPC in its original form (-DA, -HDA, and so on) is that it uses a mandatory client-server architecture, where a Windows server brokers device-specific custom drivers and protocols from many different devices up to standard OPC clients, again running only on Windows systems.

The recent OPC UA specification attempts to overcome requiring a dedicated Windows PC by removing reliance on COM/DCOM and permitting a server to be embedded into an edge product like a PLC or PAC.

Unfortunately, few hardware vendors take this approach, and there are few OPC UA software clients available (a notable exception is Opto 22's *groov*).

In addition, OPC (and OPC UA) include a large set of specifications spanning more than 13 documents and 1000 pages. The standard specifies many aspects, including transport protocols, security, services, information models, profiles, and others.

As a result, vendors who choose to embed an OPC UA server into their products should consider development cost and time to market, flash and RAM footprint size, CPU utilization, and ongoing support costs.

When considering OPC for an IIoT application, end users must address routers, firewalls, and VPNs (virtual private networks).

All in all, OPC is an excellent solution for Windows software to exchange data with legacy systems, particularly on a local area network. However, an alternative protocol may be a better fit for IIoT applications where data is being transported among different types of devices with different operating systems, constrained hardware footprints, and varying network architectures.

MQTT

MQTT is a transport protocol that pushes data using a publish/subscribe (pub/sub) architecture. In a pub/sub architecture, clients subscribe to topics that contain data, which are hosted on an MQTT broker.

In a typical IIoT application where MQTT is used, you might see a PAC (programmable automation controller) at a remote site publishing its I/O status under a given topic to a broker located at a headquarters location.

Then other systems, such as HMIs, can subscribe to the topic on the broker and be updated as the state of the I/O changes.

MQTT offers some distinct advantages in IIoT applications.

Open standards—MQTT is an open protocol and OASIS™ standard. This means system developers can adopt MQTT as a communication protocol in their designs no matter what OS their systems are built around.

Adding MQTT to a newly designed device is generally easier than embedding OPC UA into a device.

Suitable for remote or tenuous connections—MQTT is also an extremely lightweight protocol, which means it uses less bandwidth to send data than other protocols, such as OPC.

This is important in IIoT applications, where things may be deployed in remote locations with network constraints such as low bandwidth, high latency, data limits, or generally fragile connections.

Good for devices behind a firewall—MQTT's pub/sub architecture also makes it ideal for IIoT applications, because it pushes data to a broker using an outbound connection.

Most firewalls block inbound traffic (for example, an external OPC client requesting data from an internal OPC server), but they allow outbound connections over secure TCP ports, such as 443 for TLS/SSL.

So in an IIoT application, for example, a PAC deployed on a remote oil well could open an outbound connection through a firewall and phone home to report its data to an MQTT broker that resides at headquarters.

Roadblocks ahead

Cyber security threats

The number one concern associated with IIoT application development and rollout today is security.

In 2016 the Internet experienced the largest cyber attack in history. Many popular websites went off line for the better part of a day as three waves of cyber attacks hit the DNS infrastructure company DynDNS. And the attack was perpetrated by a botnet of malware-infected IoT devices, shipped with poor cyber security features to a customer base uninformed on cyber security threats and best practices.

Recommendation: According to Gartner, spending on IoT security is expected to reach $547 million in 2018. As investment in IIoT security continues, it's important to establish best practices for cyber security no matter what industry an IIoT application is being deployed to.

- No device should be connected to a network without having had a full security audit performed.
- OT professionals need to begin adopting IT security policies and technology, as their technology is increasingly becoming a participating member of the IT realm.
- OT hardware and software vendors need to establish cyber security as their highest priority in product development.

Engineering talent shortage

There is a systemic lack of experience and manpower to create and implement IIoT systems.

"Perhaps the hardest challenge to overcome is that of breaking silos between different disciplines and departments," notes Gary Mintchell, an industry-leading writer on automation, control, software, manufacturing, marketing, and leadership.

"The famous IT/OT Convergence that has been discussed for many years must happen. Control engineers must upgrade their skills so that they in the very least understand networking and security. And IT engineers and architects must understand the difference between business processes and manufacturing processes."

Recommendation: OT engineers can increase their knowledge of IT technology through vendor certification programs from companies like Cisco, Microsoft, and CompTIA.

IT engineers can increase their knowledge of OT technology through university extension courses specifically designed for operations technology, like control system design and management.

Identifying and quantifying ROI

For any enterprise IIoT project to be successful, it's important to build a business case before the project can be started. However, the challenge with IIoT projects is that defining the return on investment (ROI) can be difficult.

And the new technology resources the IIoT offers, like big data and predictive analytics, require hardware and software investments to tap into the benefits IIoT applications offer. IIoT applications offer different possibilities with different end results to each organization in each industry. A significant investment in technology is difficult to make without a proven track record of the new technology providing a significant ROI.

Recommendation: To determine ROI, start with a pilot project—which is also a learning experience that will provide insight into the ROI of future IIoT projects. Cloud-based platform providers often provide reduced-cost evaluation licenses of their products to prototype applications and help calculate fully scaled return on investment.

In addition, software development tools like REST APIs and the Node-RED development environment can help

accelerate IIoT application prototyping and piloting, reducing the time and expense required to reach return on investment.

Conclusion

The value proposition for many consumer IoT applications has dwindled over the past year, but the opportunity for industrial IoT applications is only growing.

While the details of how to connect IIoT building blocks together are still foggy, it is clear that industry has already delivered the blocks themselves. The hardware and software products required to design, build, and deploy IIoT applications are here.

And the market is only poised to grow as time passes.

How can Opto 22 help you?

For over 40 years, Opto 22 has brought commercial, off-the-shelf technologies to industrial systems all over the world. We pioneered the use of PCs in controls back in the 1980s, Ethernet networking at the I/O level in the 1990s, and machine-to-machine connectivity in the 2000s.

Today, our engineering focus is on building the hardware and software tools you need to realize the benefits of the IIoT—simply, reliably, and securely.

At the lowest level, our SNAP Ethernet I/O system offers an easy and cost-effective way to bridge the real world with the digital world, through a comprehensive collection of input and output modules designed to connect with virtually any electrical, electronic, mechanical, or environmental device. This I/O system converts these raw signals to useful digital data and shares it over the standard networks and protocols understood by IT.

Where edge computing, decision making, autonomous control, data collection, and logic solving need to occur, consider programmable automation controllers such as our SNAP PACs. Complete with a built-in HTTP/HTTPS server and RESTful API, easy-to-use flowchart-based programming, significant processing power, and a large library of protocol and communications capabilities, PACs can help you get your IIoT project up and running, quickly and affordably.

When it comes time to visualize, notify, and mobilize your information, our *groov* platform offers a simple, effective way to build operator interfaces that can be viewed on any screen, from your smartphone to big-screen HDTV. *groov* logs events and notifies you when events occur in your plant, in your remote assets, or within your building. The *groov* Box includes Node-RED for easy, open-source IIoT programming.

All Opto 22 products are backed by decades of expertise in applications like process control, discrete manufacturing, remote telemetry, data acquisition, and supervisory control. All our products are supported by Opto 22 engineers at no charge and available worldwide.

About Opto 22

Opto 22 was started in 1974 by a co-inventor of the solid-state relay (SSR), who discovered a way to make SSRs more reliable.

Opto 22 has consistently built products on open standards rather than on proprietary technologies. The company developed the red-white-yellow-black color-coding system for input/output (I/O) modules and the open Optomux® protocol, and pioneered Ethernet-based I/O.

In early 2013 Opto 22 introduced *groov,* an easy-to-use IoT tool for developing and viewing mobile operator interfaces—mobile apps to securely monitor and control virtually any automation system or equipment.

In addition to SSRs and *groov,* Opto 22 is best known for its high-quality I/O and SNAP PAC programmable automation controllers, which include a RESTful API.

All Opto 22 products are manufactured and supported in the U.S.A.

Because the company builds and tests its own products, most solid-state SSRs and I/O modules are guaranteed for life.

The company is especially trusted for its continuing policy of providing free product support, free training, and free pre-sales engineering assistance.

For more information, visit opto22.com and groov.com or contact **Opto 22 Pre-Sales Engineering**:

Phone: **800-321-6786** (toll-free in the U.S. and Canada) or **951-695-3000**

Email: systemseng@opto22.com

Form 2215-170303 • Opto 22 • 43044 Business Park Drive • Temecula, CA 92590-3614 • www.opto22.com
SALES 800-321-6786 • 951-695-3000 • FAX 951-695-3095 • sales@opto22.com • SUPPORT 800-835-6786 • 951-695-3080 • FAX 951-695-3017 • support@opto22.com