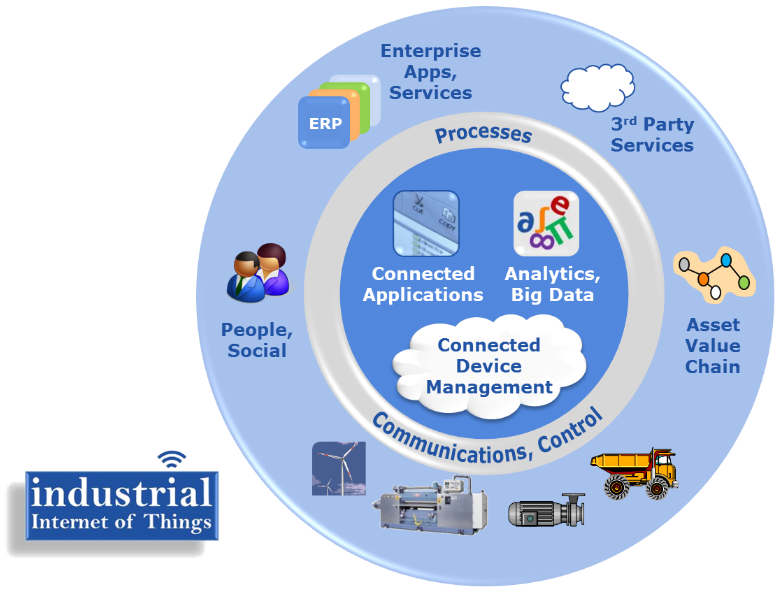
ARC WHITE PAPER

By ARC Advisory Group

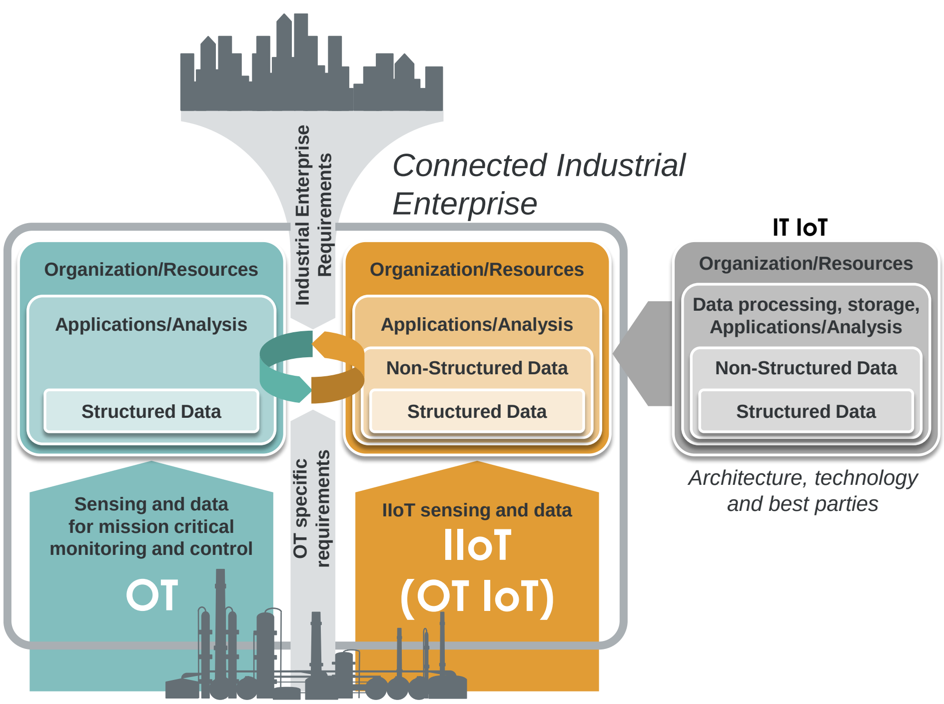
FEBRUARY 2015

Process Automation and the IoT: Yokogawa's VigilantPlant Approach to the Connected Industrial Enterprise

ARC Advisory Group



Industrial Internet of Things (IIoT) Enables New Business Models (Source: ARC Advisory Group)



IoT Integrates Operational Technology with the Enterprise (Source: Yokogawa)

Executive Overview

Connecting industrial devices, systems, and applications to provide plant and enterprise personnel with actionable information is not a new concept. Leading automation and software suppliers have been working diligently to address this requirement for decades. These efforts have not always been entirely successful, due in large part to poor interoperability between operational technology (OT) and information technology (IT). This has hampered business performance.

> Executives from Yokogawa recently briefed ARC on the company's perspective on IoT. The company's VigilantPlant approach provides a solid foundation for the OT side of the equation. For the IT side, Yokogawa is partnering with Cisco Systems.

Today, ARC Advisory Group is seeing a profound change in approach. Intelligent field devices, digital field networks, Internet Protocol (IP)-enabled connectivity and web services, historians, and advanced analytics software are providing the foundation for an Industrial Internet of Things (IIoT). The cost of connectivity is dropping dramatically, providing powerful potential to connect people, assets, and information across the industrial enterprise. Now, rather than having to build, integrate, and support purpose-built industrial solutions, automation suppliers and end users alike can reach out and embrace a wide variety of lower cost, fully supported commercial technologies within their industrial connectivity solutions.

However, since in most industrial environments, production continuity safety, and both physical and cyber-security are paramount, extreme vigilance must be employed to ensure that the omnipresent connectivity and openness implied by the IIoT does not compromise any of the above or overwhelm users and/or applications with too much raw data.

Clearly, an industrial approach is required, one that enables manufacturers and other industrial organizations to enjoy the benefits of commercial, Internet-based technologies, but without the potential pitfalls that could include overwhelming people with irrelevant data and information, compromised data security, operational disruptions, and/or safety and environmental issues. Avoiding pitfalls such as these requires appropriate integration of both operational technology (OT) and information technology (IT), with an emphasis on maintaining effective safety and security approaches and practices. ARC refers to this as the *Industrial Internet of Things* (IIoT).

> Yokogawa's industrial automation (IA) product and service offerings, industry domain knowledge, and VigilantPlant approach – which emphasizes safe, secure, and uninterrupted operations -- provide a solid foundation for an Industrial Internet of Things that specifically addresses the requirements of process automation, particularly for the OT side of the equation. To be able to provide an equally solid foundation for the IT side, Yokogawa is partnering with Cisco Systems and other industry leaders.

Executives from Yokogawa, a pioneer in both process automation and digital communications for field networks, recently briefed ARC on the company's perspective on the IIoT. Clearly, Yokogawa's industrial automation (IA) product and service offerings, industry domain knowledge, and VigilantPlant approach – which emphasizes safe, secure, and uninterrupted operations – provide a solid foundation for an Industrial Internet of Things that specifically addresses the requirements of process automation, particularly for the OT side of the equation.

To be able to provide an equally solid foundation for the IT side, Yokogawa has announced a number of strategic collaborations and will be partnering with Cisco Systems, a leading global IT, networking, and security supplier and a strong enabler of IoT technologies, processes, and concepts.

Yokogawa, Cisco, and other partners/collaborators are also working closely with end users across a variety of industries to identify specific requirements and develop appropriate IoT-enabled solutions. In many respects, this represents a departure from past practices that often displayed poor alignment between OT and IT suppliers and the end user community.

Yokogawa and Cisco have already worked together to deliver service content and solutions for a major global oil company. These solutions incorporate Yokogawa's deep domain knowledge of OT and well-proven industrial automation solutions built on top of Cisco's Secure Ops solution. The joint solution provides a secure ICS/SCADA platform incorporating best practices for information technology, security, and processes to support more effective operational decisions.

The two companies are working together to roll out similar solutions for clients across a variety of industry sectors. By partnering with Cisco, Yokogawa can leverage its own strengths in industrial automation and other OT technology and in industrial applications; while taking advantage of Cisco's strengths in IT infrastructure (including embedded cyber security and remote/local connect/access capability), best practice processes, IoT applications, and IoT-enabled innovation.

What is the Internet of Things and Why is it so Important?

> ARC defines the Industrial Internet of Things as connecting intelligent physical entities, such as sensors, machines, and other assets to each other, to internet services, and to applications. The IIoT architecture builds upon current and emerging technologies. IIoT-enabled solutions, which combine appropriate elements of both OT and IT, have the potential to bring plant and business performance to a new level.

The transformation of the industrial sector has begun. Information-driven systems based on increased connectivity, real-time data, advanced analytics, and execution software can deliver better performance and enhance competitive advantage — not only in the plant, but across a global industrial enterprise and out to its value chain. Many suppliers are developing and deploying new Industrial Internet of Things (IIoT) solutions. Thanks to intelligent, connected production assets and new service models, companies are improving performance, reducing operating costs, and increasing reliability.

However, we still have a long way to go. Large portions of industry have yet to discover these new solutions. Industry organizations (some newly formed) have begun proof-of-concept and test bed projects. Standards and best practices are slowly emerging from the innovative stew of technologies, products, services, and ideas that characterize the IIoT today. Many thought leaders forecast dramatic growth in the number of connected industrial "things" in the coming years.

The Industrial Internet of Things (IIoT) serves up data from connected devices in the plant or in the field and then processes those data using sophisticated new analytics and execution software systems. This sets the stage for operational improvements and for implementing new and innovative business processes. Smart connected products and machines can be more flexible and perform better than their unconnected predecessors. However, achieving the transformational potential of the IIoT is not as simple as deploying, say, a "smart" compressor. Getting significant benefits from IIoT requires a collection of software, hardware, communications, and networking technologies, all working in concert.

Basic IoT Architecture

Today, the Internet of Things is in a chaotic emerging state, with no widely agreed upon standard systems, networks, or interfaces. Multiple communications technologies are used and a variety of embedded intelligence technologies and sensor and actuator solutions are available. Numerous IoT research and development activities are currently under way.

While the IoT can add value to an immense variety of consumer and commercial applications, ARC research focuses on the Industrial Internet of Things (IIoT). This has a unique set of requirements due to operational, safety, security, and regulatory issues associated with most industrial applications, which also stand to benefit greatly from the technology.

Four Main Parts of Industrial IoT

ARC believes that an Industrial IoT system contains four main parts: intelligent assets; a data communications infrastructure; analytics and applications to interpret and act on the data; and, of course, people.

Intelligent assets include plant instrumentation, equipment, machines, systems or other assets enabled with sensors, processors, memory, and communications capability. In certain cases, these assets may have an associated virtual entity or support software-defined configuration and performance. Intelligent assets will generate more data and share information across the value chain. Some intelligent assets will eventually be self-aware or operate autonomously.

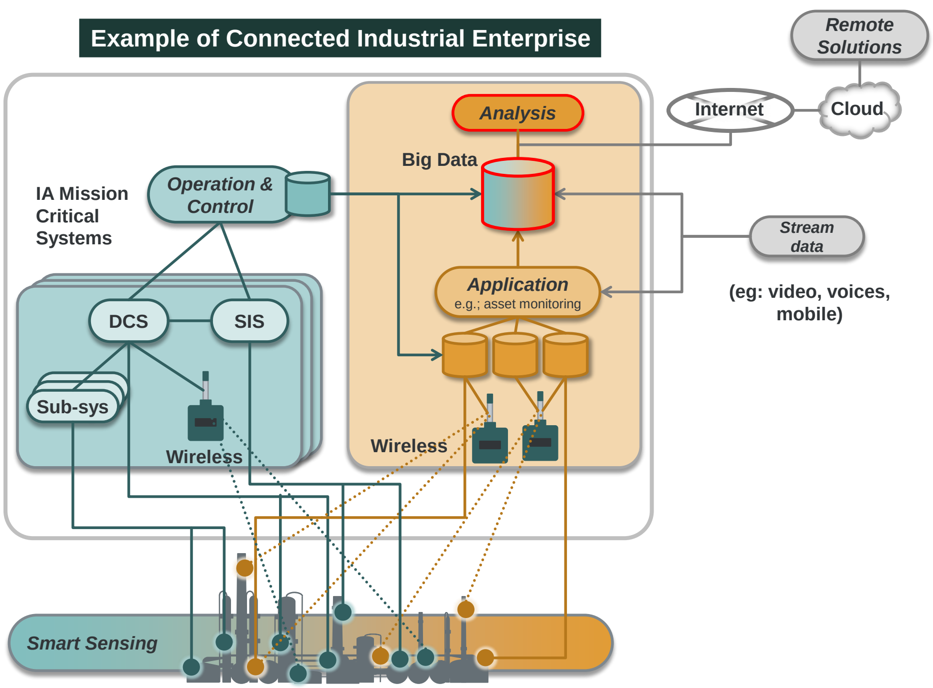
In addition to the Internet, data communications between these assets and other entities will often leverage network technologies such as LTE, ZigBee, WiFi, IEEE 802.15.4, and cloud-based computing infrastructures with storage to accommodate Big Data requirements.

Powerful analytics and other software will help optimize both assets and systems. Predictive analytics will be deployed to reduce unplanned downtime. Newly available information generated by these tools will lead to new, transformative business models supported by new applications. Instead of offering physical products for sale, companies will increasingly offer products "as a service."

People will participate by having access to much more data, better analytics tools, and better information, and will increasingly make decisions based on the analysis generated by these resources. Quantified decision making will become much more common, with appropriate, in-context information available when and where people need it. But people will also continue to become better connected to others and to plant equipment, machines, and systems through social and mobile tools and applications.

Key Technical Components

Operational Technology-Related Components



Yokogawa View of Connected Industrial Plant

At the OT level, a large number and variety of difference sensors, intelligent field devices, controllers, systems, mobility devices, application software, networking, and security components come into play relative to the Industrial Internet of Things. While these come in a wide variety of "shapes and sizes," all feature some degree of built-in intelligence, self-diagnosis capabilities, connectivity, and support for analytics. Examples include:

- Equipment-mounted sensors (temperature, pressure, vibration, etc.)
- Soft sensors
- Process variable transmitters
- Analytical transmitters
- Analyzers

- Controllers (embedded and standalone)
- HMIs
- Mobility devices (smartphones, tablets, etc.)
- Smart positioners and drives
- Sensor, field device, and control networks (wired/wireless)

With traditional automation architectures, most of these intelligent, connected devices communicate directly with a host controller, control system, or safety system or PC-based application located right in the plant; with appropriate production- or asset-related data then passed up to supervisory or business networks at the plant and/or enterprise levels. This largely remains the case, particularly for mission-critical process control and plant safety functions.

Structured vs. Unstructured Data

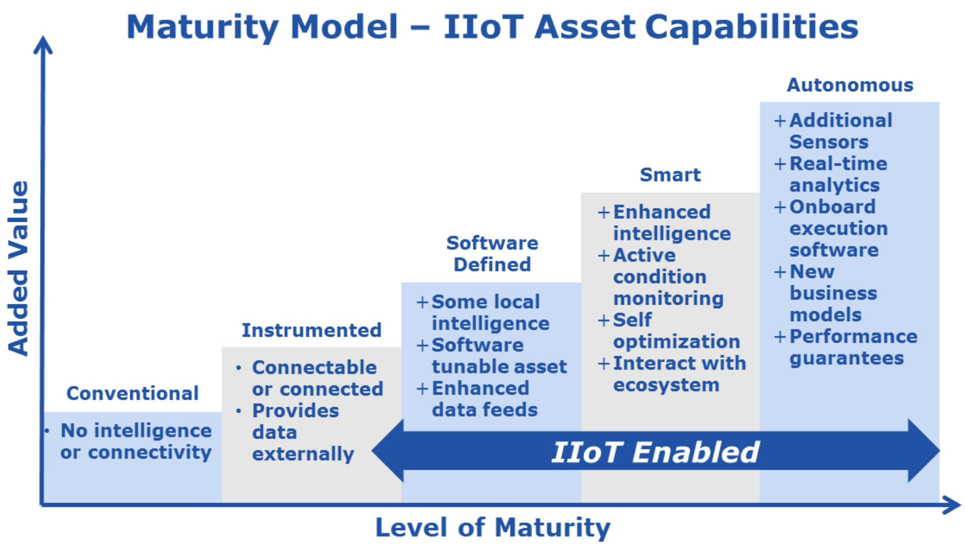
So what's the difference between "structured" and "unstructured" data? Structured data has a predefined data model and thus can be easily organized, understood, and interpreted. It's the kind of data (often numeric) that many OT users are familiar with from plant historians and CMMS systems. Spreadsheets and relational databases are other common structured data sources. Unstructured (typically non-numeric) data, in contrast, does not have a predefined data model. Social media content, Word documents, PDFs, audio and video files, images, and messaging are all sources of unstructured data. Sensor-based data is often referred to as "semi-structured" data, since it is not inherently organized, but can be organized in plant historians. The challenge for industrial organizations is to make sense of and extract value from the massive amounts of structured and unstructured data now available to them, without overwhelming people and applications. This is where IIoT-enabled analytics come into play.

However, as IoT technology migrates into industrial environments, we're seeing an increasing number of primarily non-control or safety-related sensors and devices communicate directly with remote, often cloud-based systems and analytics applications through the Internet where the data are transformed into actionable information and timely alerts for operations and maintenance personnel. Today, this is particularly true for sensors that relate to asset health or status and applications that relate to condition monitoring and predictive maintenance.

In some cases, such as for smart field instrumentation, process control-related variables will communicate with local controllers through digital plant networks, while secondary asset-related measurements can be communicated directly to appropriate remote, IoT-based applications, bypassing the control system entirely. One of the challenges here is to effectively manage, merge, and utilize the increasing variety, volume, and velocity of both structured and unstructured data available from the profusion of smart, connected plant and automation assets.

Maturity of IIoT Asset Capabilities

Within the IIoT context, an industrial asset evolves in steps from being a dumb, unconnected conventional machine to an intelligent, connected machine. In some cases, the asset eventually becomes a completely autonomous actor.



The first step, "Instrumented," involves making the asset connected or connectable, and providing the capability to share certain data. The next level is a "Software-Defined" machine, or a machine with some local intelligence and mechanical systems that can be tuned or adjusted by changing software parameters. The next level is "Smart." These machines also incorporate condition monitoring, enhanced onboard intelligence, and self-optimization. Smart assets also have the ability to interact with elements of their ecosystem, and especially with other smart assets.

The Industrial Internet of Things starts with intelligent, connected things. In practice, this means deploying assets and devices designed and delivered with local intelligence and communications capability, or adding these capabilities to legacy assets. The following section discusses and prioritizes some of the technologies that make assets and devices smart.

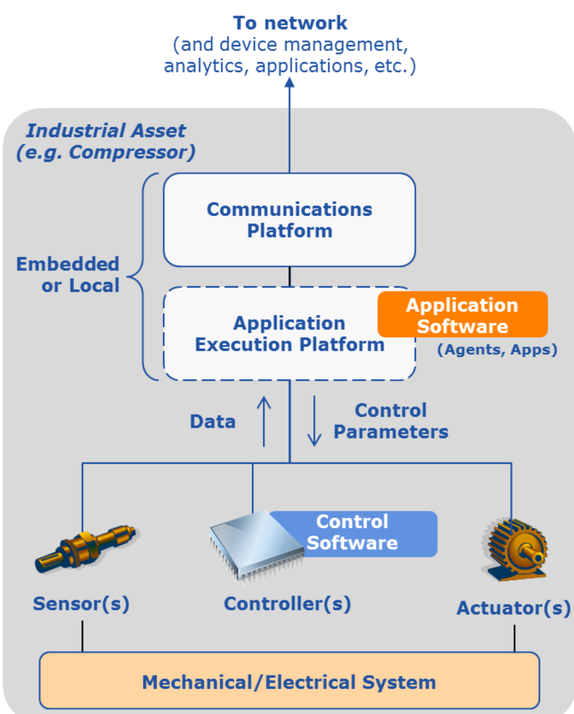
Smart Sensors

As used here, a "smart sensor" is one that is easily deployed to provide new data from existing assets (for example vibration or bearing temperature sensors), or easily incorporated into new or existing machines in a way that is readily accessible externally using common protocols and communications technologies. Sensors are critical to any IIoT solution, but require suitable network connectivity and platforms to provide the desired functionality. All kinds of sensors -- from simple temperature sensors to advanced vision sensors -- can be smart sensors.

Embeddable Compute and Communicate

Onboard intelligence, combined with the ability to communicate, is another hallmark of a smart industrial asset. This requires an embeddable computer, typically with processor, memory, OS, and communications capability. The system should have the capability to monitor sensors and drive actuators. In addition, it should be capable of running local analytics software, agents, or other software applications, as well as streaming data in real time.

Smart Gateways and IPCs



Basic Elements of the Smart Industrial Asset

Another approach to gathering data from assets is to use a gateway to connect to the asset sensors on one side and to a cellular network via a SIM card in the other. This approach is well-suited to simple data collection and exchange, but doesn't provide any local intelligence or the ability to run applications or agents in the asset. In some cases, this limitation may be overcome by using a local industrial PC (IPC) rather than a gateway, but may require use of Ethernet connectivity instead of a cellular network.

Smart Digital Controllers

An example of a smart digital controller is the digital servo drive. The digital servo drive functions as both an active compensator and intelligent sensor. As manufacturers seek to extract more digital data and improve machining, the digital drive is essential.

As an active compensator, the digital servo drive incorporates adaptive control algorithms to optimize the dynamics of the mechatronic system. Advanced algorithms can adjust the parameters of the proportional integral derivative (PID) controller in the servo drive based on its dynamic performance (following error, settling time, etc.).

Modern DCS controllers also employ digital technologies to perform basic PID control as well as advanced regulatory control functions. Increasingly, automation suppliers are also embedding more sophisticated advanced process control (APC) capabilities into their DCS controllers to support optimization schemes at the unit and/or plantwide levels. Some automation suppliers have also taken advantage of available fieldbus-based control to distribute some control functionality out to intelligent actuators and other fieldbus devices, which can maintain loop control even if communications with the DCS should be lost.

Smart Machines

The next generation of smart industrial machines is already being designed. In addition to providing the expected functionality of an industrial asset, these smart assets also provide a platform for new applications and services. They are designed to be remotely manageable and secure and to operate as part of an ecosystem. This is possible due to the addition of local or embedded capabilities including computing (processor, storage, and OS); communication (Wi-Fi, Ethernet, Bluetooth, etc.); the ability to monitor sensors and drive actuators; and the ability to run analytics software, agents, applications, etc., and stream data.

Wearable Devices

Employee badges, wristbands, smart goggles, and other wearable devices can connect humans to systems in interesting new ways. They can interact with the local environment to bring new information directly to the worker or can track and quantify movements and limit access to authorized areas. These devices can also be incorporated into safety systems. For example, it is possible to use employee badges and a crane collision avoidance system to avoid putting heavy loads down on top of workers at a construction site.

RFID

As the IIoT matures and product component parts acquire the capability to interact with available industrial machines to coordinate and execute the required manufacturing processes, RFID will play an important role. RFID tags will be incorporated into component carriers and components, and RFID read/write modules will be deployed at workstations throughout the plant.

IPv6

In the connected industrial enterprise, it's critical to be able identify every device that provides data. This is particularly true for distributed sensors. TCP/IP provides the identification, location, and routing that are core components of the IoT architecture. TCP/IP is also important because it can support virtually any media type, which is important for industrial implementations. Most applications already support TCP/IP.

The Internet Engineering Task Force (IETF) developed IPv6, the latest revision of the Internet Protocol, to replace IPv4, which still carries over 90 percent of Internet traffic. IPv6 simplifies network management and addresses the larger problem with IPv4, which ran out of available new addresses. IPv6 further promises the ability to support differing network types and offers improved security provisions.

Information Technology Components

Typically, the IT supplier will be responsible for:

- IT infrastructure (including embedded cyber security)
- Non-control-related networking (including both wireless and wired infrastructures)
- Mobile device management
- Remote access management
- Data storage, management, and analysis
- IoT application infrastructure
- IoT communication infrastructure

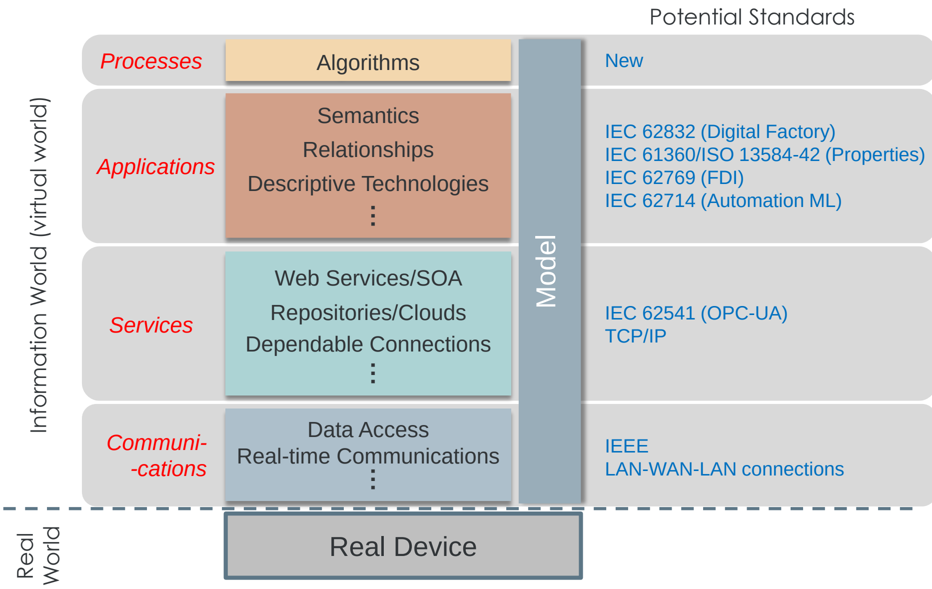
Standards and Organizations

Standardization of core components of the IoT architecture is a primary enabler to realizing its potential benefits. Widely adopted standards, particularly in key areas such as data exchange, architecture, and security, will make industrial IoT solutions easier and simpler to implement and manage. Standards are important for "future-proofing" installations and protecting users from becoming locked into a specific vendor or technology. In the fast-moving IoT universe, however, it will be difficult for standardization efforts to keep up with the rapid pace of new technology developments.

Standardization of the Industrial IoT architecture is one of the most important, and most challenging, issues affecting adoption.

Industrial device-level connectivity remains one of the most fragmented interface areas, with many proprietary and/or de facto standard protocols in use. Industrial manufacturers are well aware that proprietary supplier protocols continue to enable suppliers to retain customers and deflect third-party involvement in their installations. In the industrial IoT world, this trend is not just limited to manufacturing applications, as even the Smart Grid and smart electrical meters are being implemented as closed systems.

Core Topics and Potential Standards



Source: IEC TC65 Forum, Measurement and Control Show Osaka 2014

Numerous efforts to standardize IoT components and develop standardized IoT architectures and implementation approaches are under way around the world. Developments with the most near-term potential impact for manufacturers are likely to come from the IT world. This is particularly due to the emphasis placed on IP-based devices, interfacing to higher level architectural components, and the overall faster pace and more widespread adoption of technology in this space. This scenario is not new to manufacturers, since most have adopted Ethernet and wireless networks, commercial operating systems, and other carryovers from the COTS technology world.

Beyond the IoT-specific standardization activities, several standard development organizations have formed or focused resources on IoT architecture and implementation. For industrial automation applications, the focus of the emerging IIoT, several standards development organizations discussions have started to determine the best architectural fit for OT. Currently, IT- and OT-focused standards development organizations are collaborating to define an appropriate architecture. While ARC is following a large number of different standardization efforts relative to both the IoT and the IIoT, two efforts that ARC and Yokogawa believe are particularly relevant to industrial automation include the IEC/SG8 Smart Manufacturing initiative and the IEEE SA P2413 architectural framework.

IEC/SG 8 Industrie 4.0 Smart Manufacturing

ARC considers Industrie 4.0 to be an important subset of the overall IIoT. According to the IEC website, the proposed scope of the SG 8 Industry 4.0 Smart Manufacturing initiative, formed in September 2014, includes:

- Defining the terminology for Industrie 4.0
- Summarizing the status of standardization in this field
- Enhancing cooperation and establish new liaisons between a variety of relevant IEC, ISO, ISA, and IEEE committees
- Making an inventory of existing standards and standardization projects in progress
- Developing a function model/reference architecture based on established IEC models

IEEE SA P2413: Architectural Framework Standard for IoT

According to the IEEE website, the IEEE SA P2413 standard will provide a cross-domain architectural framework and reference model for the IoT can be applied to multiple vertical domains, including industrial automation. The working group supports extensive liaison with groups inside and outside of IEEE. The standard, will aid system interoperability and functional compatibility to encourage IoT adoption.

The plan is to leverage existing applicable standards and identify and liaise with planned or ongoing projects with a similar or overlapping scope.

Lifecycle Perspective

Ongoing ARC research clearly indicates that IIoT will play an important role across the entire lifecycle of an industrial plant; from initial design and engineering during the upfront, capital expenditure-based project stage, through the much longer operational expenditure-based operations and maintenance lifecycle phase, where value is achieved from industrial assets.

In the capex phase, significant IIoT-related benefits will be derived from remote engineering and design, which can improve collaboration between engineering resources located around the world to help compress project schedules and encourage innovative approaches. In the operational phase, value is obtained through predictive maintenance work processes, access to real-time diagnostic information from critical automation assets, and reduced barriers to information.

Since IIoT fundamentally represents a new model for how information flows throughout an enterprise, owner-operators will have to rethink how the new model can adapt to their business requirements. They will need to work closely with their engineering procurement, and construction contractors (EPCs), IT suppliers, main automation contractors (MACs), main instrument vendors (MIVs), main electrical contractors (MECs), and other suppliers at a very early stage in capital projects to determine the best fit and to identify future areas for value-building innovation.

Design and Engineering

With increasing pressures to compress the time schedules and reduce the costs required to complete today's megaprojects across both the upstream and downstream sectors, major automation suppliers are working diligently to meet their customers' demands to reduce automation project costs and compress time schedules to increase ROI and speed time-to-value.

Yokogawa also believes that the Industrial Internet of Things can significantly reduce upfront project costs and compress time schedules in the capex (project) phase by incorporating IoT-enabled innovations into the company's IA architecture in the form of highly efficient and secure remote engineering approaches and remote integration testing.

Operations and Maintenance

In the operational phase, the profusion of IIoT-connected sensors and intelligent assets will provide a wealth of new data that can be collected, analyzed, and acted upon to improve asset availability and performance significantly. By applying advanced analytics to this "Big Data," users and applications can obtain the actionable, in-context information needed to improve or optimize process operations. Yokogawa believes that IIoT can help improve plant performance in the opex phase by:

- Facilitating visibility in operations
- Enabling proactive maintenance for integrated open systems
- Enabling proactive asset management
- Enabling IA experts around the world to share intelligence and knowledge
- Gathering and analyzing data to transform Big Data into actionable intelligence

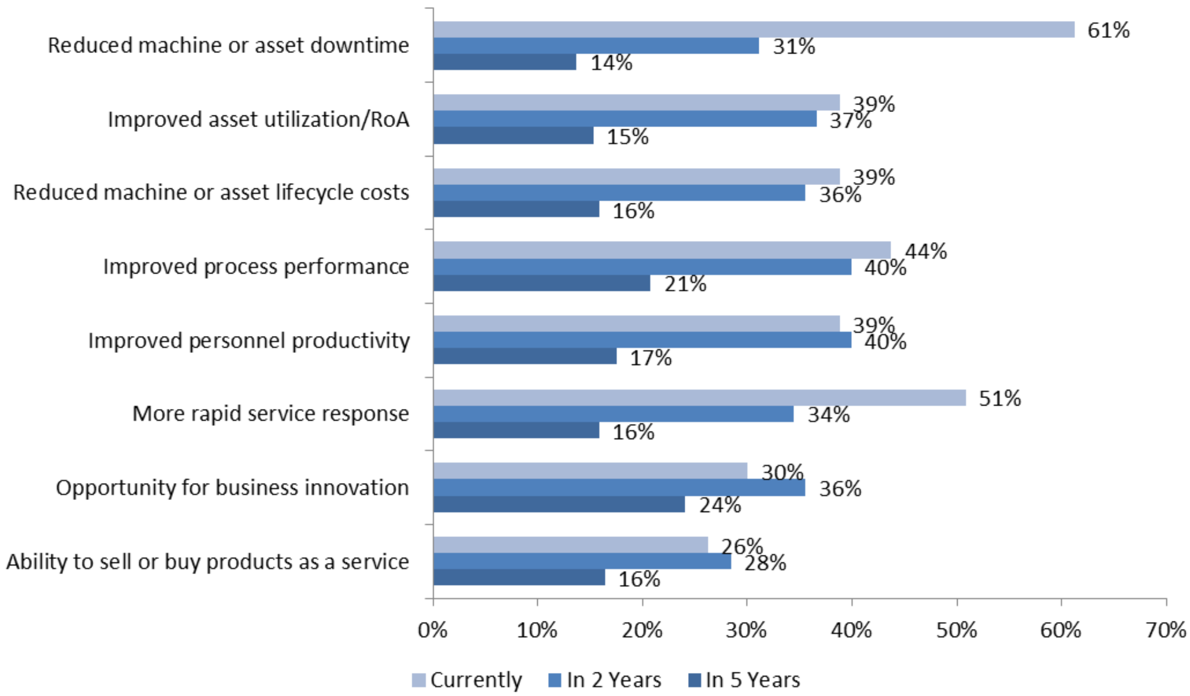
Proactive, predictive, condition-based maintenance helps owner-operators avoid costly, unneeded maintenance and identify and remediate process or equipment issues before they can negatively affect production, product quality, safety, or environmental performance.

What Users Hope to Achieve with IIoT

ARC, in conjunction with *Automation World* magazine, conducted a short web survey in the second quarter of 2014 to gauge the industry's perspective on prospects for adoption of the Industrial Internet of Things. Among other objectives, the survey aimed to provide insight into current and projected use of internet-connected devices, level of enterprise integration for connected devices, and potential drivers and inhibitors impacting IoT adoption. Most questions asked respondents to indicate what was currently employed versus what they planned to deploy in two to five years. A total of 216 responses were received from a wide spectrum of industry participants, although not all respondents answered every question. The continuous process industries -- including oil & gas, electric power generation, water & wastewater, and chem/petrochem -- were well represented among the survey respondents currently installing or planning to install IoT solutions.

From Connected to Integrated

While device connectivity is inherent in the term "Industrial Internet of Things," the ability to integrate data from connected devices and provide performance-enhancing feedback is integral to its primary value proposition. This is true whether the goal is to reduce industrial asset downtime, improve productivity, or speed service response; all reported as primary business drivers behind prospective IoT adoption.



Drivers for Implementing Industrial Internet of Things (Source: Joint ARC/AUTOMATION WORLD Survey)

Responses to our survey reflect this migration from simple connectivity to true Internet-based integration with enterprise solutions. Numerous respondents reported current use of legacy M2M solutions. These are typically point-to-point or use connected devices that are not integrated with enterprise solutions. Forecast responses, however, indicated definitive intent to migrate toward the use of internet-connected devices integrated with enterprise solutions.

Integrating enterprise software components, particularly Big Data, cloud computing, and analytics, is a core component of the IoT vision. This capability represents a step change from traditional point-to-point connectivity of industrial devices and helps distinguish the IoT from legacy remote monitoring solutions.

Survey responses reflect a distinct trend away from point-to-point, standalone device connectivity and toward connected devices integrated with enterprise applications.

Respondents' intention to integrate connected devices with these enterprise software components was evident in the survey results. Use of analytics software with future IoT solutions was one of the most distinct changes anticipated as far as what components will be employed in future IoT solutions. This is consistent with the industry's vision of analytics' role in the IoT, one that relies on integrated analytics capabilities to achieve incremental performance gains.

Survey responses indicated a migration over the next two years from remote monitoring and telemetry implementations to more remote asset management and remote service applications. Respondents were more reticent regarding prospects for five years out, however. Most likely, this reflects the justification of initial IoT solutions on the basis of these remote maintenance and remote service applications, rather than the farther-out potential of initiatives like product-as-a-service.

Industrial IoT with Intelligent Devices Enables Proactive Maintenance

IIoT connects intelligent physical entities (sensors, devices, machines, assets, and products) to each other, to internet services, and to applications. The IIoT architecture builds on current and emerging technologies such as intelligent equipment with an IP address, machine-to-machine (M2M) communications, mobility, cloud computing, analytics, and visualization tools. No substantial technological breakthrough is needed for industrial solutions to utilize IIoT technologies.

Analytics Combined with Focused, Structured Data

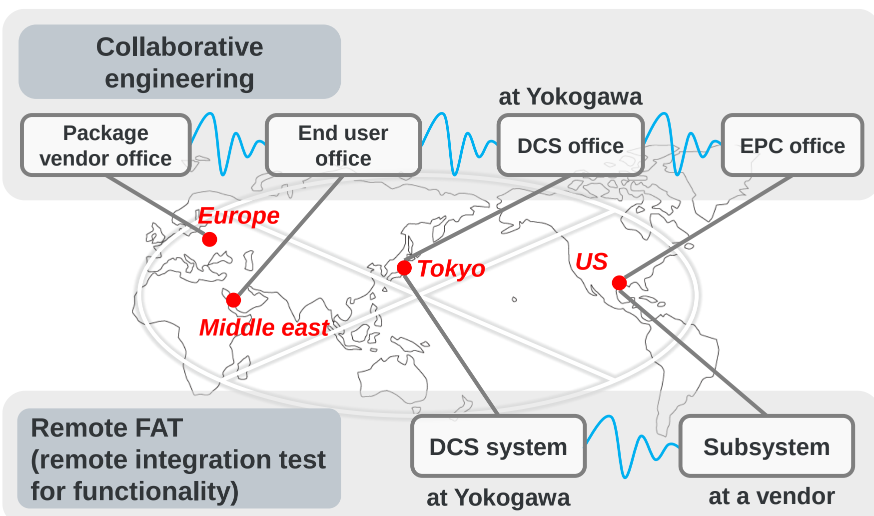
As explained in several recent ARC reports, with the growing adoption of device networking, more assets have the capability to provide data for proactive asset management. The more focused, structured data coming from a particular machine or class of assets can be combined with advanced analytics to offer new opportunities for improving asset reliability, uptime, and longevity. Device data combined with algorithms designed for that specific type of equipment, provide a means to assess condition with higher fidelity (identify specific components and failure modes with longer advanced notice) and reliability (detect a higher portion of pending failures with fewer false alarms). It can significantly improve uptime and reduce maintenance costs by recognizing a problem long before it can cascade into a catastrophic failure with a much larger impact on business performance.

Yokogawa IIoT Use Cases

Major automation suppliers, such as Yokogawa, are focused on the potential project, operations and maintenance benefits that IIoT can deliver for their customers across a broad cross section of industries. While much of the technology needed to support IIoT is already available, if not yet fully implemented in industrial facilities, the specific use cases are being developed. ARC looks forward to identifying and reporting upon a rapidly growing number and expanding variety of Industrial IoT use cases in the coming months and years.

Yokogawa has already identified, implemented, and/or is in the process of implementing a number of relevant use cases and has shared several of these with ARC. Use cases span the lifecycle of the project from engineering and design to operations and maintenance.

Collaborative Engineering



Yokogawa IIoT-Enabled Remote Engineering Supports Concurrent Engineering and Remote FAT to Help Compress Project Schedules

To reduce engineering times during the design phase of automation projects and reduce travel time and costs for engineers and designers, Yokogawa is developing effective and secure methods for performing simultaneous, remote collaborate engineering via the Internet. This includes the ability for engineers and designers based in different competency centers around the world to "meet" in cyberspace and share data, information, and design documents via web-enabled applications. This represents the true application of concurrent engineering practices to automation projects, where multiple engineers and project personnel can have access to up-to- date project information regardless of where they reside.

In the example provided, DCS engineers located in Yokogawa's Industrial Automation (IA) center in Tokyo could collaborate effectively with EPC engineers in the US, engineers from a packaged equipment supplier based in Europe, and engineers and other end users from the owner-operator based in the Middle East.

Remote Integration Testing

In a similar manner, rather than having to physically ship a variety of different subsystems to a central site before critical integration testing can be performed, Yokogawa is developing methods that would allow integration testing between multiple components of a total automation solution to be performed remotely via the Internet.

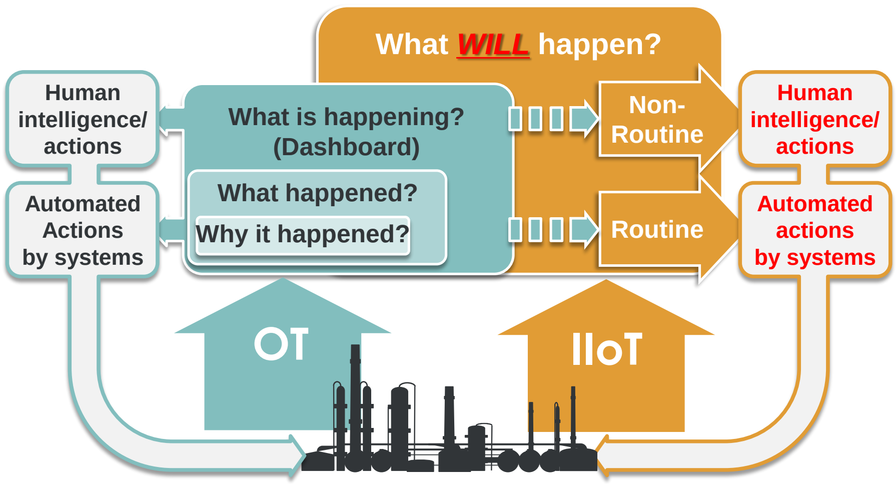
This not only saves a significant amount of time and expense, it also speeds any retesting that might be required to ensure that any issues have been resolved and that all sub-systems are fully functionality with the appropriate interoperability prior to shipment. This would eliminate the need for the respective suppliers' technical experts to have to travel to the FAT site to perform the needed fixes, saving travel time and expenses and helping avoid costly project delays.

Big Data Analysis Provides Intelligence for Both Routine and Non-Routine Operations

Today's industrial facilities generate tremendous amounts of data from connected devices, machines, plant equipment, systems, and software applications. As more "things" become smart and connected, the volume and variety of data that must be collected, managed, stored, and parsed will only increase, creating new challenges at both the OT and IT levels.

To gain value from this "Big Data" and improve the total cost of ownership (TCO) for industrial assets, owner-operators will have to take full advantage of the advanced analytics solutions now coming onto the market for industrial applications.

Yokogawa believes that by analyzing the OT-related Big Data generated by IoT-connected plant assets and providing the resulting analysis to the right people, applications, and systems in an appropriate timeframe and context, industrial organizations can optimize their operations to both improve TCO and achieve operational excellence (OpX).



Big Data and Analysis Enable Industrial Organizations to Move to a More Proactive, Information-Enabled Operating Environment

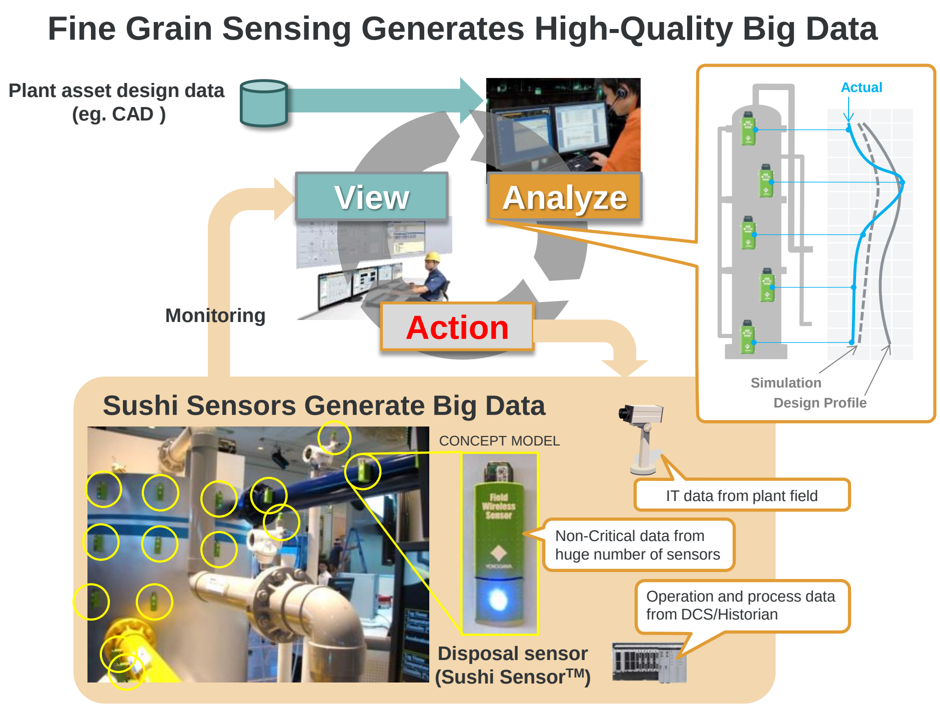
Yokogawa's efforts here focus on two areas:

1. Providing feedback for intelligent humans to interpret and act upon for non-routine OT-related work processes
2. Develop real-time logic and intelligent applications to trigger the appropriate automated responses in mission-critical systems for routine processes. This builds upon Yokogawa's leadership in modular procedural automation (MPA). Big Data analytics offer exciting potential to bring MPA to the next level.

Over the years, Yokogawa industrial automation has enabled organizations to move from the inflexible, one-dimensional reports of the 1980s that simply indicated *what happened*; to the multi-dimensional analysis of the 1990s that provided valuable insights into *why something happ*ened. In the early 2000s, we began to see more intuitive dashboards, providing performance "scorecards" of *what is happening right now*. The next step, IIoT-enabled predictive analytics applied to the Big Data collected from connected "things," offers the potential to predict *what will happen* to enable appropriate actions to optimize plant and business performance.

Verifying Design vs. As-Built Performance Profiles

This innovative Yokogawa use case, which employs disposable, wireless temperature sensors with location awareness capabilities (in this case, called a "Sushi sensor") in combination with IoT-enabled analysis and simulation capabilities, spans the project and operational lifecycle phases. In this application, a large number of inexpensive, disposable wireless temperature sensors are installed at critical points throughout a distillation column or similar process unit.



IIoT-Enabled Sensing, Big Data, and Analytics Provides Actionable Decision Support (Source: Yokogawa)

Both the temperature measurements and associated sensor location data transmitted from these location-aware wireless sensors can be monitored in real time or collected by a local or remote historian and used to generate a highly accurate temperature profile model that can be used to view and verify the as-built performance of the process unit against the as-designed performance. These data can then be used to create simulations that process engineers can use to fine tune the unit's physical configuration and control engineers can use to fine tune the control strategy to help continuously optimize unit performance.

Improving Fuel Efficiency in a Furnace

Big Data is useful, but determining the smaller data sets needed to solve specific issues to improve plant operation performance is often even more useful. For example, to improve fuel efficiency in a furnace, process engineers and mechanical engineers can work with data scientists to analyze large sets of structured and unstructured process-, asset-, and energy-related plant data over time (such as at three-month, six-month, or twelve-month intervals). Over time, the team should be able to reduce the amount of data that must be analyzed, gradually narrowing in on the key players.

According to Yokogawa, the resulting analysis of the small data set can be used to determine where excessive energy is being consumed and the root causes. With this knowledge, monitoring and control strategies can be implemented to achieve the desired energy savings.

Critical Success Factors

While the emerging IIoT offers significant potential to help improve operational excellence, due to the unique requirements of industrial applications and the previous disconnects between both internal OT and IT groups within the same enterprise, as well as between OT and IT suppliers, a number of critical success factors come into play relative to designing, implementing, supporting, and fine-tuning IIoT-enabled solutions over time in industrial enterprises.

Yokogawa believes that it's important to understand that one of the key differences between mission-critical functions (such as real-time process control and safety shutdown) and less mission-critical functions (such as gathering, storing, and analyzing data for industrial automation intelligence/decision support purposes) is that most of the requirements for process control and safety must be clearly defined in advance. In contrast, data, information, and decision-support requirements often evolve over time.

This can make it difficult to define the requirements for IIoT systems and solutions in advance. Thus, when embarking on an IIoT-related project, it's critical to carefully select the desired architecture, standards selection, technical components selection, and partners.

Yokogawa also believes that IIoT solutions must be driven by OT requirements and targeted at resolving OT-related issues, problems, and challenges. These can include operational and maintenance challenges, process design challenges, and mechanical design challenges, which all require close cooperation between these disciplines. This makes appropriate organizational and resource planning critical for success.

Other critical success factors include:

- Appropriate domain knowledge in both OT and IT
- Clear understanding of operational requirements, including need for flexibility and expandability
- Close integration between OT and IT
- Close cooperation between OT and IT suppliers; between suppliers and end users; and between plant engineers, process engineers, and data scientists when developing and implementing solutions
- Careful consideration of how the solution will be maintained and fine-tuned over time
- Ability to adapt to new business models
- “Bulletproof” cybersecurity
- Secure and robust networks (wired and wireless)
- Close internal cooperation between internal IT and OT groups as well as between plant engineers, process engineers, and data scientists

What Yokogawa Brings to the Table

In the company’s vision for the Industrial Internet of Things, Yokogawa believes that it can add significant value in the operational technology (OT) domain, while helping ensure the prerequisite integration of OT by working closely with both IT suppliers and end users.

In addition of supplying a wide variety of related industrial hardware, software, and services, this includes taking advantage of the company’s deep knowledge of industrial organizational issues; real-time data processing, data storage, and analysis; and managing data from devices, machines, and other “things” in the plant and in the field.

Perhaps even more importantly, the company’s VigilantPlant approach helps ensure the appropriate rigor required to make sure that IIoT solutions meet the demanding safety, security and availability requirements for mission-critical industrial automation.

The company's specific strength's related to the OT side of the IIoT equation include:

Sensing

Yokogawa is a leading global supplier of wireless and wired sensors for both primary and secondary variables and product composition. This includes distributed wireless temperature sensors; temperature, pressure, and flow transmitters; and analytical instrumentation.

Yokogawa is also a leading supplier of industrial wireless and FOUNDATION fieldbus technologies, both which come into play for many IoT-enabled solutions.

Systems

Yokogawa introduced one of the world's first distributed control systems (DCS) almost 40 years ago and remains a leading global DCS supplier. A combination of both centralized controllers and remote field controllers make the company's flagship CENTUM VP DCS well-suited to supporting the OT side of many IIoT-enabled solutions.

The company also offers supervisory control and data acquisition (SCADA) systems and remote terminal units (RTUs) to support remote operations. Yokogawa's FAST/TOOLS SCADA data and analysis platform is well-positioned to meet customers' remote data acquisition and analysis requirements.

As previously mentioned, safety is a key requirement in industrial process plants and other industrial operations. Yokogawa's ProSafe-RS safety integrated system (SIS) meets the strict safety requirements of both the IEC 61508 and ANSI/ISA 84 international standards. For offshore and subsea oil & gas operations, both of which are particularly well-suited for IIoT solutions, the company offers the ProSafe-SLS high-integrity safety system to help meet the severe environmental conditions and mitigate risk in these upstream operations.

Services

Yokogawa offers a variety of well-proven local and remote engineering services, performance services, asset management, and other services that span both the upfront (capex) phases of a project and the much longer (opex) post-installation operations and maintenance project phase.

The company's various service capabilities – up to an including providing comprehensive main automation contractor (MAC) services - can both contribute to and benefit from IIoT implementations. Good upfront engineering provides the foundation for any industrial automation solution, and IIoT-enabled remote engineering and FAT services can help compress project schedules and reduce costs.

Remote performance services, that both support and are enhanced by IIoT solutions, can help industrial organization improve performance at the unit, plant, and enterprise levels.

And, as previously mentioned, predictive asset management services, enabled in part by IIoT-connected sensors and analytics, represent a key value proposition for the IIoT.

Conclusion

While IoT concepts and enabling technologies are well understood and widely accepted in the enterprise space, in many respects, they represent a new frontier for industrial automation end users who are far more familiar with operational technology than with information technology. In the enterprise space, several large technology suppliers have already carved out leadership positions.

While this is not yet the case in the industrial automation space, all things considered, it appears that Yokogawa is well-positioned to assume an OT leadership positon in developing the overall vision and strategy for the IIoT.

Analysts: Paul Miller and Larry O'Brien
Editor: Dick Hill

Acronym Reference: For a complete list of industry acronyms, please refer to www.arcweb.com/research/pages/industry-terms-and-abbreviations.aspx

API	Application Program Interface
B2B	Business-to-Business
BPM	Business Process Management
CAGR	Compound Annual Growth Rate
CAS	Collaborative Automation System
CMM	Collaborative Management Model
CPG	Consumer Packaged Goods
CPM	Collaborative Production Management
CRM	Customer Relationship Management
DCS	Distributed Control System
EAM	Enterprise Asset Management
ERP	Enterprise Resource Planning
HMI	Human Machine Interface
IOp	Interoperability
IoT	Internet of Things
IIoT	Industrial Internet of Things
IT	Information Technology
OT	Operational Technology
OpX	Operational Excellence
PAS	Process Automation System
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
RFID	Radio Frequency Identification
ROA	Return on Assets
RPM	Real-time Performance Management

Founded in 1986, ARC Advisory Group is the leading research and advisory firm for industry. Our coverage of technology from business systems to product and asset lifecycle management, supply chain management, operations management, and automation systems makes us the go-to firm for business and IT executives around the world. For the complex business issues facing organizations today, our analysts have the industry knowledge and first-hand experience to help our clients find the best answers.

 This research has been sponsored in part by Yokogawa. However, the opinions expressed by ARC in this paper are based on ARC's independent analysis.

You can take advantage of ARC's extensive ongoing research plus experience of our staff members through our Advisory Services. ARC's Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For membership information, please call, fax, or write to:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA
Tel: 781-471-1000, Fax: 781-471-1100
Visit our web pages at www.arcweb.com

ARC
arcweb.com

3 ALLIED DRIVE DEDHAM, MA 02026 USA 781-471-1000

USA | GERMANY | JAPAN | KOREA | CHINA | INDIA | BRAZIL | ARGENTINA