Deliver on the Industrial IoT’s Promise With Honeywell Technology Today

Digital Transformation: A Pragmatic Approach, p2
An IIoT-enabled Vision for Process Automation, p4
OPC Unified Architecture: Key Enabler of the IIoT, p10
PLUS: A DevOps Case Study in IIoT Servitization, p13

A Secure Foundation for Digital Transformation

Deliver on the Industrial IoT’s Promise With Honeywell Technology Today
Honeywell’s vision for the Industrial Internet of Things builds enterprise optimization, ecosystem analytics and domain expertise on a secure foundation of seamless data access and information transparency.

A pragmatic approach to digital transformation

Honeywell Process Solutions is no stranger to helping its process industry clients harness digital innovation for business benefit. Indeed, the company’s digital firsts include both the distributed control system (DCS) and the “smart,” digitally communicating transmitter. Today, the Industrial Internet of Things (IIoT) represents only the latest advance in the evolution of digital technology through which Honeywell has continuously supported its customers since the 1970s, according to Andrew Hird, vice president and general manager of the company’s newly minted Digital Transformation organization.

Honeywell’s approach to the IIoT is a pragmatic one, Hird says. “It’s still all about finding out our customers’ challenges and problems, then applying technology to solve them,” he says. “And while the IIoT can help solve important, previously unsolvable problems, our fundamental approach hasn’t changed.”

CONTROL recently caught up with Hird to discuss the IIoT by Honeywell and why the company is uniquely positioned to help the process industries to realize the IIoT’s transformative potential.

Q What do you see as the essential aspects of the IIoT as applied to the process industries?

A There are three important aspects to the IIoT, and if you get all three right you can extract huge value. The first is data consolidation. Multiple disparate systems of data have to be brought together. Only then can you identify the root causes of problems that simply weren’t visible before. Second, you need to be able to move that data, in a secure fashion, from the plant into enterprise systems where you can leverage the advanced analytics and expertise that exists across the organization. The third essential aspect of the IIoT is the ability to securely tap the domain expertise of a whole ecosystem of partners in the cloud, where other organizations such as process licensors and original equipment manufacturers (OEMs) can help solve additional problems. It’s not just about monitoring, it’s about taking that diagnostic knowledge of the OEM and embedding it in an application that can predict and prevent failure.

Q What business benefits can processors expect to realize by investing in the IIoT?

A The IIoT can help solve a range of historically difficult problems. The first has to do with reducing plant downtime. Most customers I know are happy with 88% plant availability. They plan to lose 5% on planned shutdowns, and the other 7% “just happens.” So, there’s a big payback if you can go after this 7%. The second problem where the IIoT can help involves staying on spec. Product that doesn’t meet specifications—or an in-process batch that has to be thrown away—might represent millions in lost revenue for a pharmaceutical manufacturer. A third key area where the IIoT can help business is in the integration of supply chains, which run far more efficiently with real-time visibility among participants.

Q Honeywell has a long-standing industry leadership position in measurement, control and optimization. How has the company evolved the range of its portfolio in order to help clients realize the promise of the IIoT?
Through our consistent evolution philosophy, we’ve never left a platform—or a customer—behind. No matter when you bought a control system from Honeywell it can coexist under the current architecture. For example, a TDC 2000 customer from 1975 is able to run that technology inside Experion, preserving their intellectual property. And because Experion is Ethernet-based, it’s also IIoT-ready. It’s very, very easy to pull data from it. Further, the Experion Orion operator console itself is a fantastic device for consolidating data and giving operators the information they need to make better decisions.

Our IIoT capabilities also are supported by several key technologies including Intuition Executive, the platform in which our data models reside. OPC Unified Architecture (UA) allows stranded data from all sorts of devices to be brought very securely and simply back into the DCS, or directly into the cloud. The third key enabler is rock-solid cyber security. Without it, customers are reticent to put data up into their own enterprise systems—let alone into the cloud. All the investments we’ve made into making our systems and our customers’ networks secure is accelerating the IIoT’s uptake.

You’ve been tapped to lead the newly formed Digital Transformation business unit within Honeywell Process Solutions. Can you explain why that organization was formed and how you envision it working to deliver results for your process industry clients?

We’ve actually been solving these sorts of problems for a long time. We’ve collected data, we’ve done analytics and we’ve written advanced software applications. What’s different now is that we have to do it much more rapidly and we have to allow our customers to use these capabilities in the cloud—to run not only their individual sites but their enterprises.

We also are focused on developing partners, finding those OEMs and process technology companies that have that depth of domain knowledge on particular assets and bringing them into the Honeywell ecosystem.

What distinguishes Honeywell’s approach from that of other technology suppliers?

The process industries need a partner that has foundational technologies in process automation and advanced software applications, but also secure integration and communication technologies like OPC UA and cyber security. We invented the DCS; we own MatrikonOPC; we’ve got the most progressive cyber security organization of any process automation supplier; and we’ve been building software for 40 years, particularly around advanced solutions.

Our control systems are in 10,000 plants around the world, and we’ve already solved many of these problems for our customers at individual sites. Now we’re solving bigger problems for them by getting data up into the enterprise layer where they can optimize not only individual sites but entire businesses. Further, the IIoT by Honeywell is securely bringing that data into the cloud where we can bring to bear Honeywell’s expertise as well as that of a larger ecosystem of process licensors and OEMs—all to better solve our customers’ particular problems and challenges.

“Without rock-solid cyber security, customers are reticent to put data up into their own enterprise systems—let alone into the cloud.”

– Andrew Hird, Vice President and General Manager, Digital Transformation, Honeywell Process Solutions
The Industrial Internet of Things (IIoT), has the promise and potential to be the most influential and disruptive influence on automation since the advent of the microprocessor-based distributed control system (DCS). Early architectural styles are emerging for the broader IoT in which ubiquitous sensing is coupled to cloud-borne data analytics and storage systems. While these approaches are certainly viable for a broad-class of IoT solutions—such as for smart grid and consumer-grade appliances—industrial automation systems require a more considered approach.

A fundamental difference is that the IIoT aims to enhance the operation and management of industrial production processes, many of which involve exothermic reactions for which safety is a primary concern. Security of IIoT-based systems is also of paramount importance not just from a safety perspective, but also in cases of the production of essential and strategically important goods and services. This concern results in more stringent security, reliability and availability requirements as well as the ability to continue operation with intermittent access to Internet resources. When failures do occur, the system must continue operation where possible or degrade gracefully, deterministically and safely.

Integration with legacy systems a given
Another distinction of the IIoT is that a factory or processing plant is a very long-lived, capital-intensive asset requiring long-term support in the face of rapid technological advances. This reality requires support for existing, ageing equipment and infrastructure and a means of protecting investments in intellectual property. As a result, many devices that will form part of the IIoT will continue to communicate via existing, often older protocols and will need special mechanisms to integrate them into the wider IIoT environment.

Bringing IoT ideas to the industrial enterprise means reconciling and integrating them with existing automation systems. Indeed, the IIoT is, in spirit, an extension of concepts that Honeywell pioneered in the 1970s with the introduction of the Totally Distributed Control system (the TDC 2000 distributed control system, or DCS), a precursor to the IoT concept of edge computing. The lower layers of a DCS tend to be autonomous, with responsibility for the real-time control of the process, while the layers above provide various supervisory capabilities including advanced control and human-machine interface (HMI) plus data historian and planning and scheduling activities.

It is tempting to draw a direct comparison between the DCS of today and the IIoT-based...
automation system of the future and claim that we are already doing IIoT, but to do so ignores the significant changes to the DCS, as we understand it, that will occur with the introduction of the IIoT. The IIoT arises from the combination of core DCS concepts such as local, high availability real-time control of industrial processes together with the technologies and architectures that enable the IoT (Figure 1).

Some of the key differences between an IIoT architecture and a conventional DCS architecture can be illustrated by comparing the architectures at their highest levels (Figure 2). The structure of a DCS and associated applications typically conforms to the well understood Purdue Enterprise Reference Architecture developed in the 1990s. This abstract model typically has a corresponding realization in the topology of the system in which boundaries between levels are often expressed as network boundaries across which security can be enforced. The IIoT architecture illustrated in Figure 1 is, at the highest level, separated into two major subdivisions—the edge and the cloud. This structure can be further broken down into the seven-level model shown in Figure 2.

Applying an IIoT architecture to an industrial enterprise requires reconciling these two different organizational structures so that the key architectural qualities provided by the Purdue model (safety, security, reliability, efficiency) are maintained and enhanced within an IIoT-based structure. Level 1 of the Purdue model, basic control, moves to the edge in the IoT model, while Level 4, business planning and logistics, moves to the cloud. There is also a strong argument for moving much of Level 2, area control, to the edge for performance, security and reliability reasons. The functionality represented by Level 3, site manufacturing operations, will be split between cloud and edge depending on the balance of key system quality attributes. History, advanced process control, batch and alarm management are all examples of functions that can be deployed either in the cloud, on premise in embedded devices, or both.

Moving functionality to either the cloud or the edge represents a tradeoff amongst a number of system qualities. For example, moving functionality to the edge can improve performance and reliability at the expense of having to provision and manage functionality distributed across a large number of devices. On the other hand, moving functionality to the cloud makes it easier to install, scale up, upgrade and retire at the expense of the functionality being remote from the devices and controllers on which the functionality may depend. In general, the move to an IIoT-based

Figure 1. The Industrial IoT arises from the combination of core DCS concepts such as local, high availability real-time control of industrial processes together with the technologies and architectures that enable the IoT.
Improved support for key operational objectives

The overriding concern in any industrial enterprise is safety, for which there are well-developed sets of practices and standards. For example, the safety integrity level (SIL) model provides a quantitative measure of the risk reduction provided by safety instrumented systems (SIS) that are responsible for the basic safety of a process and formalized in IEC 61511. There will continue to be a key role for SIS at the edge in any IIoT-based automation system.

A concern closely related to safety is that of security—both physical and cyber. Unless an automation system is secure from unauthorized access and activity its safety cannot be guaranteed. Cyber secure operations require a combination of protective measures, inherently secure communications and active monitoring systems to detect and mitigate any unauthorized activity across the network. Aside from preventing compromises to the safety of the plant, security also serves to protect the intellectual property inherent in an industrial process itself and the procedures for planning, scheduling, executing, maintaining and optimizing production on the process.

Many existing DCS components have no inherent security built in. For example, they may lack any explicit access control mechanism and may transmit data on the network in plain text. Such legacy components do not disappear in an IIoT-based system but are confined to the edge computing environment to which access is strictly controlled. Access to legacy DCS components, via edge gateway devices, involves both access control and secure communications.

Another vulnerability in current automation systems stems from the use of open systems platforms, particularly in Levels 2 and higher in the Purdue model. These platforms pose risks due to their widespread use across many domains, making their vulnerabilities and associated exploits well understood. The IIoT helps address these issues by pushing automation system functionality either down into the hardened edge computing environment or up into the cloud. The cloud computing environment has rich access control and communications security mechanisms built-in, and the centralized nature of the infrastructure makes it much easier to maintain in order to address vulnerabilities that are discovered.

Overall reliability of the automation system can be enhanced both by pushing functions out to the edge and into the cloud. As with safety, pushing functions, especially control functions, out to the edge allows those functions to act more autonomously, reducing potential causes of failure. Moving functions into the cloud allows them to be more easily managed, maintained and upgraded. Further, the decoupling of edge and cloud-based functions allows them to be managed more inde-
Cyber security requires a combination of protective measures, inherently secure communications and active monitoring systems to detect and mitigate any unauthorized activity across the network.
CLOUD-BASED DATA ANALYTICS
Fast Answers for the Toughest Problems

1. OPERATOR: 01:00 AM
"Oh, there's a product quality alarm on the fractionator. The feed and controls look normal. What is causing this problem? Better contact the Process Engineer."

Experion® PKS process graphics show process upset.

2. PROCESS ENGINEER: 08:00 AM
"It is easy to search and explore visual data to confirm the off-spec problem has happened before. I will contact our Corporate Expert."

Overhead Quality

Overview: Uniformance® Insight visualization tools allow navigation to the fractionator data without knowing cryptic tag names.

Uniformance® Insight creates Operator alerts.

Flexible visual data exploration on all fractionators across sites is enabled with the common asset model.

Product quality and reliability in a process plant impacts company profit. Honeywell’s cloud-enabled Uniformance® Suite, with advanced analytics, enables rapid discovery of the root cause and deployment of an online, predictive monitoring solution.

PROCESS ENGINEER:
"It is easy to search and explore visual data to confirm the off-spec problem has happened before. I will contact our Corporate Expert."

CORPORATE EXPERT:
"I have isolated similar off-spec issues in other plants with new visual pattern searches and discovered relationships in the data we didn't see before. We can solve this problem."
Product quality and reliability in a process plant impacts company profit. Honeywell’s cloud-enabled Uniformance® Suite, with advanced analytics, enables rapid discovery of the root cause and deployment of an online, predictive monitoring solution.

**PROCESS ENGINEER:**
“With this insight, a predictive alert from Uniformance® Asset Sentinel can provide early warning so operations can respond. Look at the minor upset in overhead quality now.”

**CORPORATE EXPERT:**
“I have isolated similar off-spec issues in other plants with new visual pattern searches and discovered relationships in the data we didn’t see before. We can solve this problem.”
The list of technologies that make possible the Industrial Internet of Things (IIoT) is lengthy and includes technologies such as cloud computing, big data analytics, embedded systems, wireless sensor networks and security protocols. But communication standards form the backbone of the IIoT in that they enable the secure integration and interoperability of the many devices and software applications that participate in the system of systems that is the IIoT.

OPC Unified Architecture (UA) offers a compelling solution for connecting applications within the IIoT. It provides for a layered model that separates the configuration, format and packaging of the information from the underlying security and communication protocols. Further, OPC UA is broadly supported by both device manufacturers and software developers across the industrial automation space. Importantly, the specification continues to evolve, with the addition of publish-subscribe connectivity common to cloud-side participants in the Industrial IoT.

**Scalable and ‘future-proofed’**

The need for application interoperability and standardization in the control realm drove a consortium of automation suppliers to develop the original OPC specification in the early 1990s. Based on Microsoft DCOM technology, “OPC Classic” was extended to a suite of specifications for a variety of task such as data acquisition (OPC DA) and alarms & events (OPC A&E). But DCOM technology proved limited, for example, in its ability to facilitate cyber secure communications. To address these and other issues, OPC Unified Architecture (OPC UA, also IEC 62541) was created to enable secure and reliable data acquisition, information modeling and communication among plant-floor devices, applications and the enterprise.

A key OPC UA design objective was to prevent technology “lock in,” ensuring that OPC UA could embrace future technologies. To that end, OPC UA defines services and related concepts in an abstract manner, then further defines “mappings” between the abstract specifications and the technologies that can be used to implement them.

Central to the design of OPC UA is scalability. The specification defines the many complex feature sets available with OPC UA client and server applications. However, OPC UA is designed in such a manner that individual implementations need not support all possible feature sets in order to be compliant with the specification. For example, implementation within a small, embedded device may support a profile that mandates only data-read capabilities together with a small set of address-space constructs. PC-based OPC UA servers, however, can support a profile that includes many more features such as alarms and history.
OPC UA technology mappings are organized into three groups: data encodings, security protocols and transport protocols (Figure 1). Different mappings are combined together to create a profile. Client and server applications can support one or more profiles; however, a client and server must each provide an implementation for at least one profile in common in order to communicate.

The OPC UA security model is a three-layer approach where each layer has specific security-related responsibilities (Figure 2). The application layer is responsible for transmitting plant information and real-time data from devices and between a client and a server within a session. A session provides for user and authentication and authorization and runs atop a secure channel that both signs and encrypts the data. The secure channel also is responsible for mutual authentication and authorization between client and server applications. The transport layer is responsible for transmitting and receiving the secured data, including mechanisms for error recovery.

The OPC UA object model describes how clients access information on the server. The model defines a set of standardized node types which can be used to represent objects within the address space, object properties, methods, events and relationships between objects. By building on these elementary concepts, OPC UA enables the modelling of any object. Related objects and their relationships are grouped together to form information models.

**Companion specs for particular domains**

Standardization committees associated with many areas within automation and process control technologies have created or are creating OPC UA companion specifications. These companion specifications extend the base OPC UA information model to describe objects and relationships of relevance to a particular domain. Examples include OPC UA for FDI (Field Device Integration).
In addition to the generic information models specified by OPC UA and in companion standards, individual vendors are free to define new information models or extend existing information models tailored to their systems.

The OPC UA specification was created with the goal of enabling interoperability among products from different vendors. In order to ensure that a product is actually compliant to the specification, it must undergo a series of tests that certify compliance to the specification. The OPC Foundation maintains an independent certification test laboratory that validates compliance to the specification, including fault and stress scenarios, as well as verifying interoperability against a number of reference clients and servers.

For developers, tools such as Honeywell’s MatrikonOPC UA software development kit (SDK) can facilitate a fast track to specification-compliant OPC UA connectivity. The SDK allows developers to quickly add pre-engineered OPC UA connectivity to all their products—from small embedded devices to powerful PC-based servers—without having to become OPC UA experts.

**Pub-sub extends client-server model**

While these features form a solid foundation as IIoT enablers, an additional key enabler is required—a data exchange model that is efficient, performant, robust as well as scalable for use with one-to-many, many-to-one, or many-to-many configurations.

To address this need, work is underway within the OPC Foundation to create a publish-subscribe model that complements the specification’s original client-server model. With the OPC UA server acting as publisher, data is published to a global space governed by existing middleware such as Microsoft Azure. In contrast to the client-server model where the UA client decides what to subscribe to, the published datasets are configured on the OPC UA server. Subscribers are recipients of published dataset data and may or may not be OPC UA client applications. Subscribers must simply understand the message-oriented middleware and the rules for decoding messages. Evaluation of candidate protocols currently is underway, including Advanced Message Queuing Protocol (AMQP) and UDP Multicast as well as Data-Distribution Service Real-Time Publish-Subscribe Protocol (DDS-RTPS).

When this pub-sub functionality is incorporated within OPC UA, one can conceive of domain-specific usage scenarios including peer-to-peer controller/device communication and delivery of process messages to advanced application clients connected via an enterprise service bus (where clients likely reside outside of the local area network).

OPC Unified Architecture is an information-centric layered architecture that is at once secure, platform-independent, scalable, interoperable and object-oriented. The OPC Foundation’s agile ability to enhance the base information model to include publish-subscribe is further evidence of its commitment to be a leading technology for enabling the IIoT for years to come. ●
Much has been written in recent years about the accelerating transformation of manufacturing companies into organizations that sell not only products, but new services or outcomes closely aligned with those products—often enabled through the deployment of technologies exemplified by the Industrial Internet of Things (IIoT).

Honeywell Process Solutions already is a pioneer in this ongoing “servitization” of industry, and has for many years delivered to its customers a range of services related to its instrumentation, control systems and advanced software, as well as standalone, product-independent services in arenas such as industrial cyber security. The company’s Assurance 360 program, for example, is a two-tier service contract for managing the system maintenance of customer systems. Customers can choose to complement the capabilities of its own maintenance staff with those of Honeywell, or choose to fully outsource responsibility for system maintenance.

In both cases, contract performance is measured against established key performance indicators (KPIs), as now continuously monitored and measured in the company’s new Assurance 360 Dashboard application. Honeywell’s development and deployment of the Dashboard for monitoring the performance of these contracts clearly demonstrates how the company continues to digitally transform its own value proposition, quickly bringing to market solutions that leverage secure cloud technologies and the integration of information from multiple applications to deliver value for its customers.

The Assurance 360 Dashboard (Figure 1) pulls data from customer sites as well as Honeywell business systems, delivers a consistent user experience, and is integrated into the Honeywell Process Solutions e-presence site, HoneywellProcess.com. The

![Figure 1. Honeywell’s Assurance 360 Dashboard provides customers with a transparent, KPI-based view of system status as well as service contract fulfillment.](image-url)
solution was developed using an agile continuous delivery approach that brought the solution to market in a very short period of time by combining the engineering and IT teams together in a collaborative DevOps engagement. DevOps, short for “development and operations,” is a methodology designed to bring efficiency and speed-to-market to the application deployment process.

As part of the Assurance 360 Dashboard program, the development and IT teams adopted a new DevOps methodology that allowed them deliver the initial public release four months earlier than initially scheduled as well as new capabilities every few weeks (see sidebar).

From manual spreadsheets to online KPIs
Previously, Assurance 360 contracts were managed via a partly manual, spreadsheet-based KPI reporting process. Now, system and contractual performance KPIs are automatically brought together with detailed system performance reports, drill-down screens for details influencing the actual KPI scores as well as a roadmap of planned maintenance activities into a single view hosted on HoneywellProcess.com, where customers have a single point of access to all information relevant to their Honeywell systems. It provides customers with improved visibility of KPIs while reducing the chance of manual-entry induced errors.

System performance KPIs are computed based on actual system performance of the customer’s servers, stations, network, controllers, process control network (UCN/LCN) as well as the currency of antivirus definition files. This information is captured at the customer’s site and securely transmitted to one of Honeywell’s two Secure

DevOps methodology speeds time-to-market

DevOps is a concept or software development methodology that promotes the collaboration among solution development and IT operations teams with the goal of faster time-to-market and increased efficiency of application update delivery. A key element in the timely release of Honeywell’s Assurance 360 Dashboard—and in subsequent eight-week release cycles—was the identification of smaller sets of functional content that can, given the cloud deployment nature of the solution, be released more often.

From a process perspective, the Assurance 360 Dashboard was the first to pilot Honeywell Process Solutions’ Agile Iterative Process, or Agile HIP, which enabled the team to tailor the process deliverables and tools to better match the needs of the program, removing duplication and non-value added tasks. From a DevOps perspective, Honeywell established a shared deployment sandbox where both development and IT teams deploy their changes to a security-restricted common system on the Honeywell network. This new, agile approach allowed the teams to significantly reduce the initial delivery time, and to get customer feedback sooner and more frequently so that it could be incorporated into incremental updates.

Not having a formal DevOps model in place or experience in doing a cross-functional development, Honeywell first identified an integrated development team and established a daily global ‘stand-up’ call to identify blocks for any of the team’s activities. The goal of this meeting wasn’t to formally track progress on program tasks or to solve specific problems, but rather to identify if there was anything blocking someone from making progress and what resources they needed to connect with to resolve the problem. By focusing only on the blockers, the global team often was able to hear from all members well within the 30 minute scheduled call, ensuring that all team members were able to be productive during regular work hours.

The results proved outstanding. The integrated team delivered top-priority functionality four months early (on an original 10-month schedule), representing a 40% schedule reduction. Functional updates originally planned for eight-week intervals now go live when ready, increasing the rate of continuous feedback and improvement. The eight-week planning cycle also enables the team to be more responsive to changing business priorities.

Honeywell credits the program’s success to an integrated development and IT operations team that was committed to demonstrating a new breakthrough development approach as well as an enthusiastic, customer-focused business team that was able to articulate a practical path for initial and incremental functionality. Further, the full team picked up and solved problems regardless of whether they were development- or operations-focused. This has worked well so far, but has introduced some inefficiencies in hand-over, development and support. To further enhance its own best practices, Honeywell is engaging its suppliers and partners to learn from their DevOps journeys.
Service Centers via a Secure Service Node provided as part of Honeywell’s Remote Monitoring solution. The solution also pulls data related to the performance of service requests and completion of planned maintenance activities from Honeywell’s Siebel customer relationship management (CRM) system. Integration with HoneywellProcess.com not only influenced the dashboard presentation to conform to the experience presented by this portal, but also leveraged the existing Honeywell Common Web Authentication (CWA) and User Profiles held within HoneywellProcess.com. Figure 2 illustrates the various information sources that have been integrated together and now feed the Assurance 360 Dashboard.

**Development continues**

While the Assurance 360 site today is suitable for the current customer base, the prospect of increasing demand for such services over the coming years has the development team looking to transition the solution to a cloud-native, platform-as-a-service (PaaS) offering for improved scale and support. The Assurance 360 Dashboard supports mobile devices today through an HTML5-based responsive design, and as Honeywell continues to develop its mobile worker support, push-style notification, workflow and a more optimized experience for smaller devices are in the works.

Honeywell started this journey with a goal of improving time-to-market, and with the belief that a joint collaboration between development and IT operations would enable the company to leverage the unique skills of both organizations. And while the solution was brought to market well in advance of original estimates, the company believes that more productivity gains are to be had—not only in improved collaboration between the teams but also in the more efficient handover of responsibilities and ownership between development and operations teams.

The speedy launch and accelerated enhancements to Assurance 360 Dashboard demonstrate Honeywell Process Solutions’ commitment to leverage the Industrial Internet of Things to deliver business value for its customers. Honeywell clearly is committed to its own digital transformation, even as it seeks to help its customers transform themselves.
7%-10% of total production is lost due to unplanned downtime. This can now be avoided. IIoT by Honeywell is solving the industry’s biggest challenges, once thought to be unsolvable. Helping you avert unplanned plant downtime before it occurs.

For more information, please visit www.hwill.co/IioT