Paul Vellacott and Bob Ell, Honeywell Process Solutions, UK, explains how, in time, the industrial Internet of Things will transform oil and gas pipeline operations.

Connecting the dots

The number of connected 'things' used worldwide will reach 6.4 billion this year according to research group Gartner. Approximately 5.5 million devices will be connected to the Internet of Things (IoT) everyday – up 30% on 2015. By 2020, this number will have grown to 20.8 billion.[1]

Just as the IoT is transforming everyday life, it also promises to revolutionise industry. Consultants Accenture forecast that the industrial IoT (IIoT) could be the biggest driver of growth and productivity in the coming decade, with the potential to add US$14.2 trillion to the global economy by 2030.[2]

The process industry is no exception. The IIoT has the potential to be the most significant development

in our automation systems since the introduction of microprocessor based distributed control systems. It offers a wide range of potential uses and benefits:

- Enabling businesses to leverage the vast amounts of data provided by modern automation and control systems.
- Providing operations personnel with improved remote monitoring, diagnostic and asset management capabilities.
- Enhancing data collection, even in the most dispersed enterprises.
- Improving decisions about the actual health of assets.
- Reducing the time and effort required for configuration and commissioning.
- Minimising the need to troubleshoot device issues in the field.
- Bringing new production fields online faster.
- Improving collaboration across the company.

However, the economic benefits of adopting the IIoT are not guaranteed. Firstly, businesses must ensure they are harnessing the potential of the billions of sensors and other devices already in place. As Accenture's research recently noted: "There is a difference ... between the availability of these technologies and capitalising on their full potential by applying them effectively within organisations."

Further research has found that there are a number of significant barriers to benefiting from the IIoT, in terms of concerns rightly focusing on safety and security, interoperability, the lack of a clearly defined return on investment (ROI) and legacy equipment.[3]

Connectivity, compatibility with existing network technologies, connecting to existing automation devices and making effective use of the mobility and increased access to data that the IIoT enables; these are key challenges in the process industries generally and for pipeline operators.

In some cases, these barriers lead operators to conclude that it is simpler to just avoid connecting devices. To do so, however, is to forego the substantial benefits the technology can bring. It is also unnecessary, since the challenges to adoption are readily surmountable with the right technological partners.

Moreover, as solutions become standardised, they are increasingly cost effective. Given the pressures on margins for operators facing low oil and gas prices, the costs of foregoing the benefits and efficiencies the IIoT can bring could be far greater.

Defining terms

At least part of the problem in defining the ROI from the IIoT applications is that the concept of intelligent devices, and the machine-to-machine interfaces underpinning them, is not new to pipeline operators or the process industries in general. Indeed the Internet itself – then ARPANET – was first deployed in 1969, the same year Honeywell first conceived a microprocessor-based totally-distributed control system (TDC-2000) – technology relying on a complex network of sensors, actuators, controllers and computational capabilities.

The IIoT is essentially an extension of this concept. However, the two vital ingredients that distinguish the IIoT are use of connectivity to the Internet and IP-based protocols such as HTTPS and Internet-based cloud computing.

The IIoT relies on the edge and gateways, controllers, networks and storage – components familiar to most industrial systems. The location of these components is significantly different, however (Figure 1):[4]

- The edge comprises the plant or pipeline based sensors, actuators, and controllers – the 'things' of the IIoT, as well as the human machine interfaces (HMIs). Some devices are connected directly to the network via 3G/4G cellular or Wi-Fi, while others are connected through the edge gateway, which provides connectivity to one or more devices that support only local connectivity.
- The network connects the components of the architecture together through IP-based protocols.
- The cloud combines both storage and computing, as well as applications for analytics, reporting, control and user interfaces when these are not at the edge.

The use of the Internet as the system's network, and cloud for its storage, enhances the capabilities of traditional control systems in two key respects.

Firstly, the cloud dramatically increases the volume of data that can be feasibly stored, and therefore drawn on, while also massively increasing the elasticity of computing capabilities to do so. It removes the need for firms to manage their computing infrastructure, and reduces the costs associated with adding CPUs and disk space.

Secondly, it has a similarly profound effect on connectivity, both the ability to connect far greater numbers and more widely dispersed devices, as well as sharing their data with more and more remote and mobile users.

As well as enabling connections in both directions, wherever an Internet connection can be established, the IIoT removes complexity and cost from this connectivity. For example, while a traditional point to point radio connection to a device would often be configured inside the SCADA system, this layer of complexity is removed. The SCADA system simply needs the IP address of the server, wherever that is located.

Challenges of wider, deeper data and connectivity

These benefits are directly related to some of the key challenges of the IIoT.

The focus on security in industrial control systems is more intense than ever. The potential vulnerabilities of SCADA systems have been increasingly well recognised since the discovery of the Stuxnet worm in 2010. The recent successful attack on Ukraine's power grid[5], the first of its kind, has also heightened concerns. Fears about increasing connectivity and access to SCADA systems through the IIoT are understandable.

The increased connectivity brings another challenge too. By increasing the ability of workers to connect remotely and

through mobile devices, organisations face the difficulty of ensuring co-ordinated activity and responses. Workers not only need to connect to be effective, but also to collaborate, which is made more difficult when they are increasingly based miles – or thousands of miles – apart.

An increased storage capability also brings its own challenges. A key recognition of recent years has been that few operations suffer from an insufficient amount of data. In fact, the growing mass of data is a defining characteristic of most modern automation and control systems. However, the challenge has been to process, organise, analyse and prioritise this data in order to transform it into actionable intelligence.

Finally, there are practical concerns about the journey towards increased connectivity, and the impact on legacy investments in traditional architectures, devices and systems. Operators are keen to protect investments and avoid huge upheavals in control strategies, supervisory applications and HMI graphics as the automation system evolves.

Solving the puzzle

There is undoubtedly still work to be done in all these areas. However, considerable progress has already been made to allow industrial control system users to gain the benefits of the IIoT while also controlling the risks.

To take connectivity first, a key part of the development of the IIoT will be the development of standards to support the connection of data from a wide range of disparate devices and systems. OPC Unified Architecture (OPC UA) responds to this, extending the widely used OPC communication protocol to allow products to easily interconnect and share data in meaningful and effective ways. As a result, an increasing number of manufacturers are embedding OPC UA in their devices, ready to connect to the IIoT.

Powered by open data standards such as OPC, this layer correlates plant data from point sources, puts it into context, pulls it together into graphics, reports and trends, and then makes these materials available to the people who need it. This leaves the challenge of existing devices, however, that do not have OPC UA embedded.

OPC UA proxies or UA wrappers provide an effective answer. These allow traditional OPC servers to communicate with a new UA client, or an HMI without an OPC UA to interface with UA devices. Using this technology, operators can continue to use current systems, while gradually benefiting from newly added UA-enabled devices.

Similar progress is also being made in terms of security. Indeed, security is at the heart of the development of OPC UA. At the same time, many of the general approaches to security remain unchanged, even in the context of an IIoT environment. They include effective physical security, procedures and policies, combined with software and hardware defences, and can mitigate risks using a 'layers of protection' approach.

The risks are also controlled by employing a suitable architecture. Figure 2 shows a traditional Purdue Enterprise Reference Architecture model: the physical process (Level 0), basic control (Level 1), area control (Level 2), site manufacturing operations and control (Level 3), business planning and logistics (Level 4), and enterprise wide business systems, such as ERP systems (Level 5). In this model, a Level 3.5 demilitarised zone (DMZ) helps segregate the system to better control access and cyber security.

For the IIoT, the model would look slightly different. However, this system can still be secured by ensuring automation system functionality is placed either in hardened edge computing environment, which benefits from traditional, existing cyber security protections, or in the cloud, where economies of scale and centralised control enable extremely tight access control and communications security to be built-in.

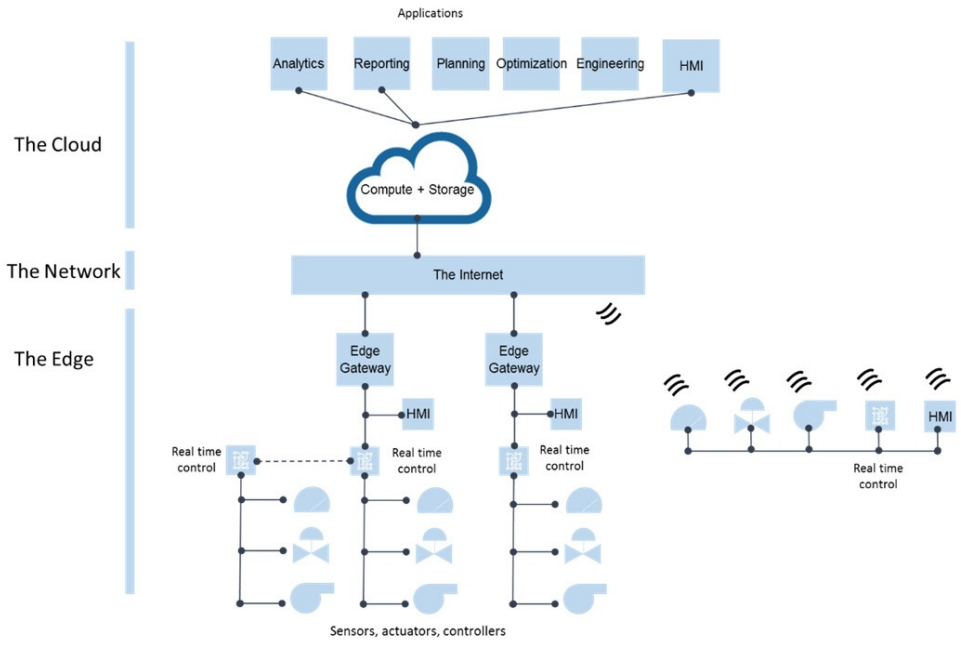

Figure 1. An architecture of the IIoT.

Making sense of the data

Arguably the greatest determination to the success of an IIoT deployment will be what is done with the data.

Two aspects here are key. Firstly, ensuring data is organised and interpreted in a way that is useful for users. A number of technologies help with this. An important one is templating to automatically detect the type of device or instrument connected, and organise the key information into a useable format. Practically, this ensures flowmeters from different manufacturers located in different places will be detected by the system for what

they are, so that the measurements and metrics are correctly displayed for users.

This provides the base for further enhancements, such as setting up a range of control algorithms and configuration capabilities built into the template to define a range of proper operating conditions and parameters. These can then be used to trigger automatic alarms or even responses from the control system when values breach limits.

Templating enables systems to rapidly sort through vast amounts of data to extract useful information, and eliminates the need for engineers to configure and organise the system and data. It is, however, just part of a wider development that is key to the success of the IIoT: big data analytics.

Data analytics has the potential to transform operations. Consider condition monitoring for example, which traditionally relies on developing a model of the processes and tracking process variables against this, in order to detect anomalies that might indicate a fault. However, over time process and plant changes can render the model inaccurate. Using big data analytics rather than trying to understand and map the process, raw data can be simply analysed for patterns and correlations identified from past incidents, without reliance on a model. Such approaches could radically enhance operators' capabilities in areas such as leak detection.

Only connect

Closely related to this are enhancements to collaboration. Data needs to not only be interpreted and organised; it must also reach the right people, and bring people together where a range of input is needed. IIoT technologies are key to this. On the one hand, the availability of data results in operations able to run with a dispersed workforce. On the other, Internet-connected mobile devices can run increasingly sophisticated HMIs to enable users to manage and make sense of that data flow.

Honeywell's Pulse mobile app is a good example: it allows plant managers, supervisors and engineering staff to remotely access real time plant performance notifications sent from industrial automation software and tailored to their role. Pulse delivers relevant metrics staff need to see, as well as the tools to resolve issues directly on their mobile device. At the enterprise level, meanwhile, Honeywell's Collaboration Station leverages the Internet to connect people with each other as well as devices and instruments across the pipeline, plants and facilities. Combining video conferencing, collaborative workspaces, instant messaging and real time SCADA data and analytics, Collaboration Station enables faster, better decisions and co-ordinated action.

In practice, the IIoT comprises billions of devices and thousands of applications. It potentially includes technologies such as Honeywell's wearable IoT connected safety solutions developed with Intel. In these solutions, a variety of sensors worn on the worker that monitor for toxic gas exposure, breathing, heart rate, posture and motion, and send the data and actionable intelligence for display remotely on a visual, cloud-based dashboard for plant managers and incident commanders. It also includes augmented reality solutions for mobile workers, who can use the cameras and connectivity of their phones to

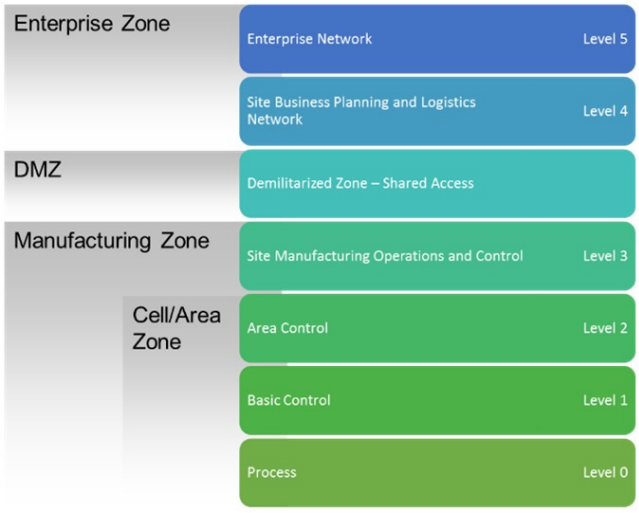

Figure 2. The traditional Purdue model.

display detailed information about the components and parts on a device they are looking at.

More widely, the technology allows an overhaul traditional service models. Instead of businesses buying equipment with a warranty insuring against failure, for example, remote monitoring and connectivity allows firms to agree guaranteed service levels with vendors, and effectively outsource servicing, updates and maintenance. Remote access to real time and contextualised information for workers, meanwhile, brings opportunities to radically decentralise decision-making.

The IIoT includes a vast array of technologies, not all of which will be adopted at once. However, in time, and together, they will transform operations. Let's take a common scenario of a fault on a pipeline. In this situation, increased sensor data will quickly identify and locate a problem on a pipe. Wearable devices, intelligent vehicles and connected enterprises will then identify the location of the staff and vehicles best placed, equipped and trained to fix the issue. Meanwhile, other experts will be contacted remotely to collaborate with workers on the ground to resolve the problem faster. On the customer side, enhanced connectivity will automatically inform them how long the interruption to their service is likely to last.

IIoT operations have yet to achieve this level of sophistication. However, as the technology develops and solutions become standardised, costs are reducing and the potential benefits grow. The limits to the potential of the IIoT are no longer practical, but imaginative.

References

1. http://www.gartner.com/newsroom/id/3165317
2. https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Digital_1/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdf
3. http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf
4. McLAUGHLIN, Paul and MCADAM, Rohan, "The Undiscovered Country: The Future of Industrial Automation", 2016.
5. http://intersys.co.uk/2016/01/23/2016-national-critical-infrastructure-affected-by-malware-for-the-first-time/