

The Industrial Internet of Things: An Evolution to a Smart Manufacturing Enterprise

by John Conway

Executive summary

The Industrial Internet of Things (IIoT) is not about ripping out current automation systems in order to replace them with new ones. The potential lies in the ability to link automation systems with enterprise planning, scheduling and product lifecycle systems. This paper analyses how the linkage can be implemented across the complete enterprise value chain in order to enable greater business control. Experts also offer perspectives regarding key aspects of IIoT deployment.

Introduction

The Industrial Internet of Things (IIoT) is often presented as a revolution that is changing the face of industry in a profound manner. In reality, it is an evolution that has its origins in technologies and functionalities developed by visionary automation suppliers more than 15 years ago. As the necessary global standards mature, it may well take another 15 years to realize the full potential of IIoT. Over this period of time the changes to the industry will be far reaching. The good news is that end users and machine builders can now leverage their existing investments in technology and people while taking advantage of available new IIoT technologies. Introducing IIoT solutions using a “wrap & re-use” approach, rather than a “rip & replace” approach will enable greater business control. In addition, this measured approach will drive the evolution towards a smart manufacturing enterprise that is more efficient, safer, and sustainable.

The emergence of the IIoT megatrend has created both hope and confusion among stakeholders responsible for operating industrial plants. Much of the early hype is focused on the impact of technological advancements on existing automation platforms.

However, one of the challenges in understanding the potential of IIoT is the very large scope of applications. In the area of smart enterprise control, for example, we will see self organizing machines and assets that enable mass customization and lot sizes of one. In the realm of asset performance, the collection and analysis of data from increasing numbers of cost-effective and intelligent sensors will increase business performance and asset uptime. A new generation of “augmented” workers will leverage cutting edge technologies, including mobile devices and augmented reality. With easier access to information across the enterprise, their work becomes simplified and production systems grow more profitable.

Some of these changes can be implemented in the short to medium term, others will require a gradual evolution with end users and OEMs incrementally adding functionality to their existing legacy systems as new international IIoT standards are established.

Definition

The IIoT vision of the world is one where smart connected assets (the things) operate as part of a larger system or systems of systems that make up the smart manufacturing enterprise. The “things” possess varying levels of intelligent functionality, ranging from simple sensing and actuating, to control, optimization and full autonomous operation.

The smart manufacturing enterprise is made up of smart machines, plants and operations all of which have higher levels of intelligence embedded at the core. The linked systems are based on open and standard Internet and cloud technologies that enable secure access to devices and information. This allows “big data” to be processed with new, advanced analytics tools and for mobile technologies to drive greater business value. This, in turn, enables improvements to efficiency and profitability, increased cyber security and innovation and better management of safety, performance with reduced CO2 emissions impact.

Smart Manufacturing Enterprise

While the long term impact of IIoT is at times difficult to predict, three distinct operational environments will set the stage for the smart manufacturing enterprise to emerge.

- **Smart Enterprise Control** – IIoT technologies will enable tight integration of smart connected machines and smart connected manufacturing assets with the wider enterprise. This will facilitate more flexible and efficient, and hence

profitable, manufacturing. Smart enterprise control can be viewed as a mid-to-long-term trend. It is complex to implement and will require the creation of new standards to enable the convergence of IT and OT systems.

- **Asset Performance Management** – Deployment of cost effective wireless sensors, easy cloud connectivity (including WAN) and data analytics, will improve asset performance. These tools allow data to be easily gathered from the field and converted into actionable information in real time. This will result in better business decisions and forward-looking decision making processes.
- **Augmented Operators** – Future employees will use mobile devices, data analytics, augmented reality and transparent connectivity to increase productivity. As fewer skilled workers are left behind to man core operations due to a rapid increase in baby boomer retirement, younger replacement plant workers will need information at their fingertips. That information will be delivered in a real-time format that is familiar to them. Thus the plant evolves to be more user-centric and less machine-centric.

While these three areas are closely related and share many inter-dependencies, they also have differences. For example the time scales on which they can be implemented and the kind of automation market segment that they address are not the same.

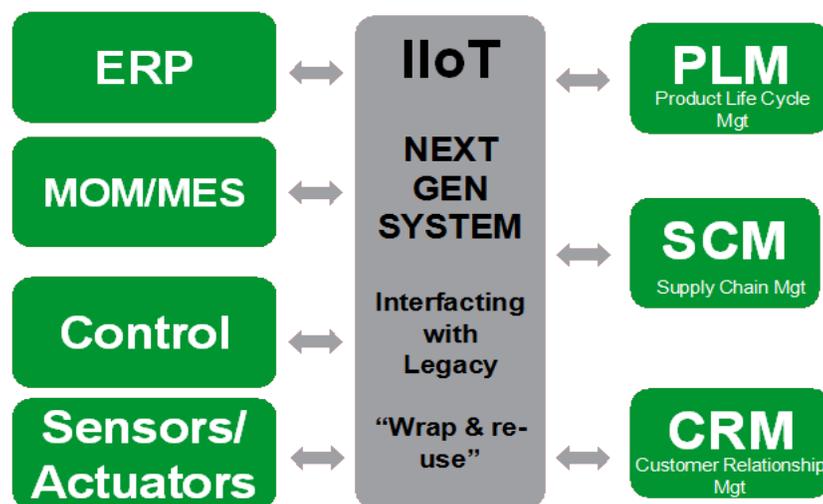
There are two other areas, collaborative robotics and 3D printing, which are also pertinent to the discussion surrounding IIoT, but these are not discussed in this paper as they are specific technologies that cannot be applied to all manufacturing enterprises.

Smart Enterprise Control

One of the biggest potential benefits of next generation IIoT systems is the breakdown of enterprise silos. The technologies will allow for closer integration of production systems and ERP systems, Product Lifecycle Management (PLM) systems, Supply Chain Management and Customer Relationship Management (CRM) systems (see **Figure 1**). Today these systems are managed somewhat independently of each other, which prohibit a holistic view of the enterprise. It is believed such a holistic approach could facilitate an enormous efficiency gain of up to 26 per cent¹ for enterprises.

Figure 1

Holistic enterprise control breaks down enterprise silos and facilitates better business control.



¹ McKinsey & Company Industry 4.0 - How to navigate digitization of the manufacturing sector

Smart enterprise control does not mean replacing current automation systems with completely new systems. Instead, it implies the connection of current automation systems with enterprise, lifecycle and value chain systems. This optimizes the entire manufacturing enterprise and enables a much greater degree of business control.

Tighter integration will allow enterprises to not only be more efficient, but also more profitable thanks to greater flexibility and responsiveness to volatile market conditions. The notion of control will expand from the real-time control of a physical parameter, to the right-time control of the whole business, including both physical and non-physical parameters. Benefits will include the ability to enhance protection against cyber threats, more innovation, and the ability to better manage safety, performance and environmental impact.

“Holistic enterprise control will be achieved through a ‘wrap & re-use’ approach rather than a ‘rip replace’ approach.”

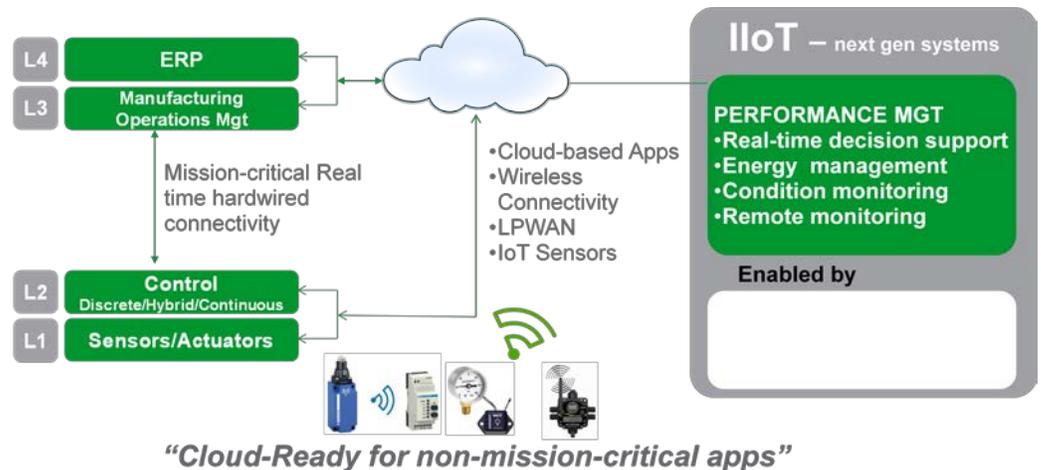
Examples of smart enterprise control include the following: mass customization and lot sizes of one, reducing the size of product recalls, detection of defective products earlier in the manufacturing process and modification of product design to eliminate root causes, modification of production planning based on weather forecasts, modification of production plan/recipes based on the spot price of raw materials.

Asset Performance

Asset performance management applications such as energy management and predictive maintenance are not new to industry, but have had limited uptake due to the cost of implementation. The costs of physical connectivity (the cost of cabling to the sensors) and logical connectivity (integration with existing systems) have been prohibitive. Wireless IP connectivity and cloud-based architectures now overcome these cost barriers. In addition, a new generation of simple, small and low cost sensors is emerging; As a result, next generation IIoT systems will deliver innovative solutions in the area of asset performance (see **Figure 2**).

Figure 2

Asset performance accelerates the adoption of new performance management applications leveraging big data and analytics, and cost-effective wireless technologies.



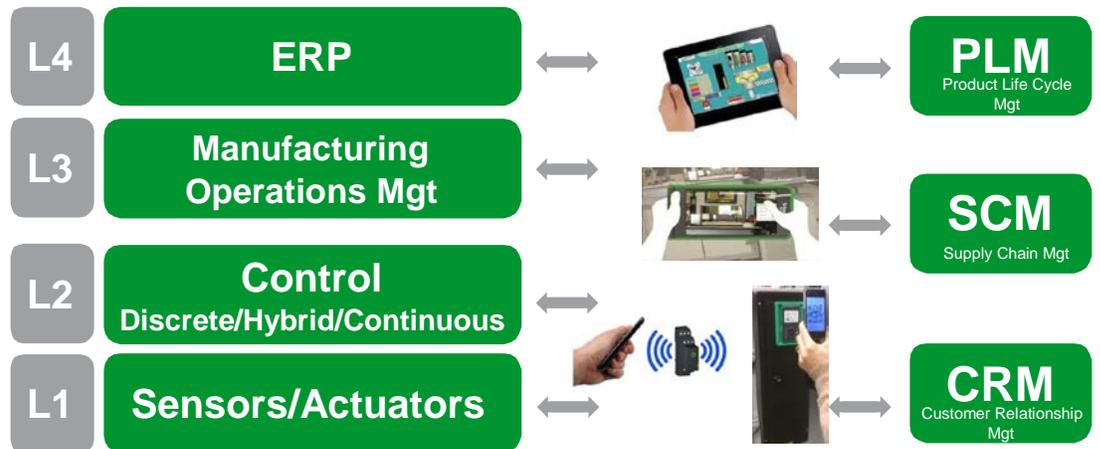
Consider the example of condition-based monitoring/predictive maintenance. Much money is wasted maintaining equipment that doesn't require maintenance, or by neglecting equipment that subsequently fails and causes unanticipated production downtime. Solutions such as condition-based monitoring do exist today, but uptake has been limited by cost. Next generation IIoT systems promise to significantly reduce implementation costs for such solutions.

Augmented Operator

The use of mobile Human Machine Interface (HMI) technologies such as smart-phones, tablets and wearable, combined with IP-access to data and information (analytics and augmented reality) will transform the way operators work. Portable wireless devices will expand their capabilities and technologies such as dynamic QR codes will improve the operator experience and render the “augmented” operator more productive (see **Figure 3**).

Figure 3

Augmented operators are more productive because they receive the right information at the right time.



Today, operators only have access to information from automation systems. Tomorrow, augmented operators will access information from all of the needed enterprise systems and will manage not just process performance/efficiency, but also process profitability.

Barriers to adoption

Several barriers will need to be overcome before next generation IIoT systems are widely adopted across manufacturing industries. These include the establishment of industry standards around IIoT, cyber security protection, and workforce adaptation to new sets of skills.

Standardization

Standards are required to allow smart connected products, machines and assets to interact in a transparent fashion. This goes beyond the simple communication protocols, and involves the creation of standard semantics and mechanisms that will allow smart devices to discover each other and interoperate. Some standards, such as PackML, do exist in this area, but they are incomplete and do not cover all aspects of manufacturing. The Industry 4.0 and the Industrial Internet Consortium initiatives are currently addressing the question of standardization.

Cyber security

The advent of the IIoT is accelerating the need for cyber security in industrial control systems. The complexity of IIoT will mean that cyber security must be designed into the components that make up the automation system.

The adoption of industrial security standards with certification will be essential to the advancement of IIoT because it will ensure the security not just of individual assets but also of the larger systems and systems of systems. These certifications

“The adoption of industrial security standards with certification is essential to the advancement of IIoT.”

will play a role similar to those which occur in the realm of safety certifications. Adherence to the certification means that the elements of a system hold the key security building blocks. The elements are combined in a secure way by security certified teams and are operated as a secure system by security trained operators.

The key to security certification is consistency and applicability. Worldwide, the IEC62443 series of security standards covers all elements of security from product development through to product features, system features, delivery and operation. It is important to note that while today some independent bodies offer certification to IEC62443, IEC itself has not yet endorsed any of these bodies for IEC62443 certification.

Complementary to IEC62443 security standards, existing industrial standards are also evolving to be more secure. DNP3 has evolved to DNPV5 to add security, OPCUA offers significant security enhancements, Modbus is evolving to Modbus Secure, and EtherNET/IP is becoming EtherNET/IP Secure. In addition many IIoT systems are adopting security features derived from existing IT standards such as HTTPS, certificates, and encrypted/authenticated protocols.

Worker competencies

The skill-sets required to design and operate an IIoT-based system are somewhat different from those needed to run a classical automation system (see **Figure 4**). A significant amount of re-training will be required for existing operators and maintenance staff to manage such systems. The good news is that the IIoT systems will use technologies that are familiar in everyday life, and the new generation of young operators will have no problems adapting to this new approach. The main challenge for automation suppliers will be to design and supply diagnostics/debug tools that can rapidly identify the root cause of problems. This will ensure that a malfunctioning or downed system can be restored quickly.

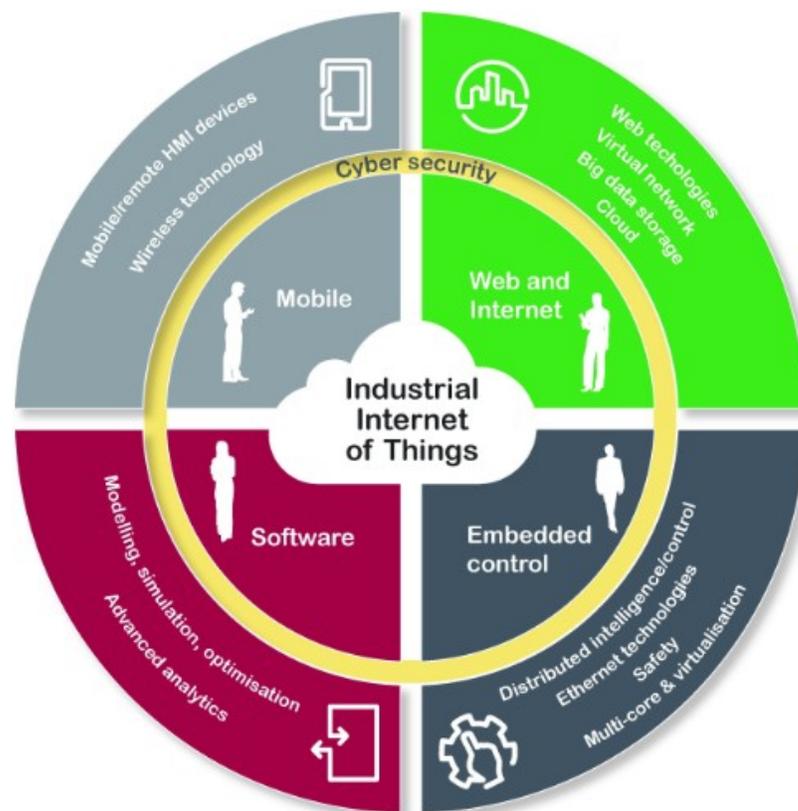


Figure 4

Many new skills will be required to design and operate IIoT systems.

Impact on automation architectures

Information driven architectures

As smart manufacturing enterprises start implementing smart enterprise control and asset performance systems managed by augmented operators, automation vendors will respond by implementing IIoT at all levels of the automation hierarchy. This will allow easy integration with next generation IIoT systems. In addition, with the increasing power of embedded electronics, connected intelligence will migrate down to the lower levels of the automation hierarchy – to the control level and to the sensors and actuators. As a result, operations technology (OT) systems will merge with information technology (IT) systems and the automation hierarchy will evolve to be a much flatter and more information-driven architecture. Since the future implications of this are still unclear, the technologies and architectures employed must be flexible, adaptable to change and capable of integrating with legacy systems. The monolithic, single-source, hierarchical approaches and architectures of the past will not work in the future.

The information-driven topology is shown below in **Figure 5**.

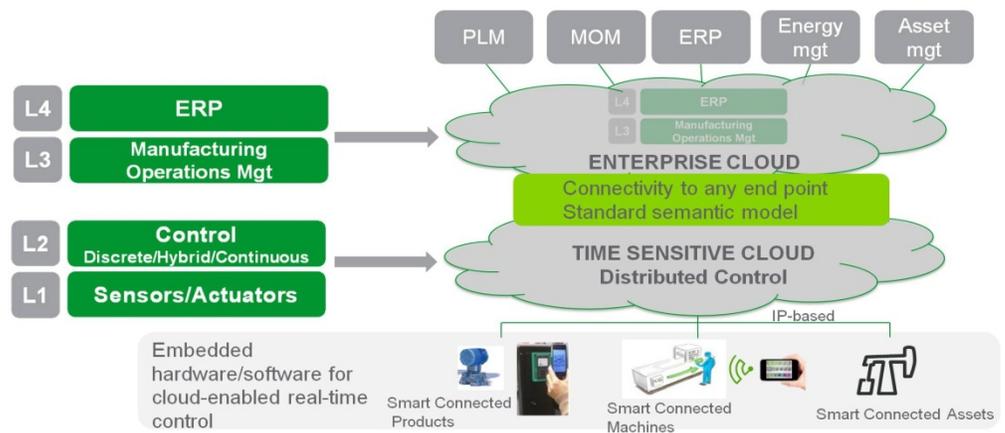


Figure 5

The information-driven automation architecture

"Monolithic, single-source, hierarchical approaches and architectures of the past will no longer be viable in the age of IIoT."

The architecture consists of two distinct layers. Information flow across both layers will be transparent using semantics and discovery mechanisms based on industry standards. Both layers are explained below:

1. A time-sensitive layer for real-time deterministic control. This layer is often referred to as "fog" or "edge". However using the term "time-sensitive IP-based" for this layer underlines the fact that the technologies included in this layer are fundamentally the same IIoT technologies used in the enterprise cloud layer, but are optimized for real time deterministic communications.

The OT devices that comprise this time sensitive layer (sensors, actuators and controllers) will be cloud-ready and capable of interfacing transparently with the IT business systems of the second layer. Those same devices will also have a high degree of intelligence. Consider the example of control valves with embedded temperature, pressure and acoustic sensors. They are able to operate autonomously using set points from the enterprise, determining their own needs for preventive maintenance, and informing the maintenance department of their condition in a timely manner.

2. A cloud enterprise layer where enterprise systems (ERP, MOM, PLM, SCM, CRM, etc) and next-generation functions including asset management and energy management interoperate with each other and with the time-sensitive cloud-ready systems.

The use of the term cloud above refers to the technologies used, rather than the physical location of the infrastructure. There are many reasons to believe that, in the industry automation business, “on-premise” clouds (commonly referred to as “edge”), will be the most widely used architecture.

Centralized versus distributed control

The arguments for highly centralized redundant control systems versus highly distributed control systems have gone on for many years. Proponents of each architectures fiercely defend their position with valid arguments.

The advent of IIoT does not resolve this long-standing debate. On the one hand, the use of cost-effective embedded electronics in field devices argues for more distribution of intelligence and control. On the other hand, the high speed IP-connectivity of field devices enables a more centralized architecture where all the sensors and actuators are connected to a highly redundant and powerful multi-core processor located in a secure on-premise data centre.

Today an application is programmed with a particular hardware target in mind, for example a PLC. Tomorrow, an application will be programmed independently of the underlying automation hardware, and the system will distribute the application transparently to the hardware, configuring all communication mechanisms automatically. This approach will allow users to choose either a highly centralized or distributed architecture, or a hybrid approach based on their specific requirements and concerns. A Distributed Control Standard (IEC 61499) exists that will facilitate this work and which can be used as the basis for an IIoT distributed control standard.

The distribution of intelligence into the field will allow smart connected products and smart connected machines to publish important information in a standardized format. Intelligent brokers will make this information available in a transparent manner to the systems and applications that require it. This approach will overcome one of today’s current challenges: the location of information is unknown and therefore cannot be discovered or exploited without custom programming.

Networked automation architectures

Networks will see an exponential increase in the number of smart connected devices. These devices will exploit a time-sensitive IIoT/Ethernet backbone to interoperate with each other and with devices residing in other enterprise systems.

An example of the sheer number of connected devices can be seen at the [Torresol Energy Gemasolar solar power plant](#) where 4000 Schneider Electric PLCs/drives are connected via Ethernet to control the displacement of solar mirrors. The large number of networked devices presented many new challenges not only in the area of network management and performance but also in the area of managing the overall configuration of the distributed control system and its application software.

Implementing such large networked systems with today’s classical automation techniques is complex. Tomorrow’s IIoT-based automation systems will require a new approach to simplify the design, the management, and the maintenance of networked automation architectures.

Expert perspectives

IIoT is often described as a revolution that will change life as we know it. In the areas of consumer goods, building management and others there is some truth to this. However, across industry, IIoT will be applied more slowly as different sectors of the industrial markets evolve their specific needs and address their unique challenges.

Technological elements leading the IIoT evolution

By Eric Farrugia, VP Strategic Marketing, Industrial Controls & Drive

IIoT is blurring the boundaries between physical and virtual objects. This is giving way to more flexible models of accessing process and machine data – bypassing rigid automation architectures and accessing user-friendly, mobile systems based on Internet standards. While generating and collecting data is an important aspect of IIoT, this alone will not enable manufacturers to realize the full benefit of IIoT – there are other components to consider:

1. Smart connected devices that are IIoT ready will deliver an “advanced sensing system” that generates information with the first level of data analysis completed by the device itself
2. An edge gateway to aggregate data, display information and connect to the cloud for advanced analytics
3. Applications and services to further analyze data and put it into context to help reach business goals
4. An open and collaborative environment to allow partners to develop on a common platform

Delivering smart connected devices that are IIoT ready means embedding Internet technologies like WIFI and web services natively into those devices. For example, Variable Speed Drives are essential to industrial processes by way of providing information on motor use and other devices like sensors and relays provide information on the device lifecycle. Embedded digital services also become critical to support process optimization. For example the new series of Altivar Process drives with built in web technology standards, Ethernet connectivity, intelligence and asset management or energy management features deliver additional contextual information, including real time events, alarms, drifts, and historical data.

“Delivering smart connected devices that are IIoT ready means embedding Internet technologies like WIFI and web services natively into those devices.”

An edge gateway will aggregate data collected from various sources and deliver real-time business information to the right people at the right time. This is the key interface between the Internet world and the process (the things). It also facilitates value-added services independent of the control system. Supporting this vision is the new Magelis GTU HMI which offers the flexibility of combining a CPU box with a choice of display, including a Wireless LAN enabled display. The edge gateway ensures a high level of performance and connectivity to address the critical needs of the IIoT platform.

Digital applications and services are critical to end users achieving the business performance gains promised by IIoT. Simple data collection must be extended to include analytics that deliver pertinent and valuable business information. Some examples of such applications and services include installation optimization, asset management and protection, condition based monitoring, augmented reality applications and OEE calculation, among others.

A platform built on an open and collaborative environment will allow selected partners to develop specific applications that extend offerings and reach to help deliver the promise of IIoT. A consistent development environment with governance and processes will enable easy integration of IIoT platforms.

Measurement and the art of “simply-complex”

By Matthew Carrara, VP, Field Devices, and Michael Davis, Senior Program Manager, FieldDevices

The technical capacity of the Industrial Internet of Things will provide the opportunity to redeploy the building blocks of industrial processing to measurement, control and connectivity. While these three building blocks iteratively rely on each other for balance, it all starts with measurement – which is the catalyst for process optimization and improvement. IIoT will not only rely on this historically fundamental component of processing, but will reach deeper and expect more. Measurements of the future will capitalize on technologies that will significantly reduce size and cost, increase computing storage and power, and eliminate wired connectivity (for power and communications). These changes will result in a game-changing increase in the volume of applied measurement. With extremely low cost sensors capable of real-time and predictive data connectivity, stakeholders will realize the value of employing massive numbers of measuring devices for control and process optimization.

Analogous to all living systems, where sensing is elegantly performed at the molecular level, IIoT sensors will evolve to single performance tasks. In living systems, each biologic sensor is a unique molecular configuration designed to measure a specific parameter (pressure, insulin, pH, temperature, etc.). There may be thousands of similar or different biologic sensors in a single microscopic cell. In a similar way, tomorrow's IIoT sensing elements will be tiny and comprised of very few unique parts while embedding far more data manipulating intelligence, passing along only relevant information to control cyber-physical systems (aka smart-connected assets).

“The market for measurement devices will explode in volume for the supplier that can deliver the true capability of IIoT using simple wireless sensors.”

Today's process sensors are marketed as 'smart' or 'intelligent', but while technical advancements have allowed for increasing embedded intelligence, the resulting sensors have become large and expensive, thus self-limiting volume deployment. Market purchases of sensing devices are not limited by the desire for less information but by the high cost of deployment (the sensor plus the installation cost of cabling). The market for measurement devices will explode in volume for the supplier that can deliver the true capability of IIoT using simple wireless sensors.

By driving simplicity to the fundamental components (measurement), driving differentiating analytics to the control level, and linking them using wireless connectivity and cloud-based architectures, there will be a directional shift in the Industrial Automation and Control model – one that can be defined as “simply complex”, where simple measurements plus complex analytics equate to customer value.

Capitalizing on IIoT opportunities will require a fundamental shift in culture, thinking, architecture, strategy and investment. With many of the IIoT technologies already available, and simple sensor designs currently under review, the journey to a smart evolution has begun.

SMART Machines: What they are and how they contribute to the future of the industry

By Dr. Rainer Beudert, Marketing Director, Machine Solutions.

The smart machine concept has a number of key enablers (from the technology perspective) and drivers (from the end user and market perspective). The combination of both will lead to machines that are safe, secure, self-aware, flexible and capable of meeting demands from both end users and consumers. The integration of internet connected devices, adoption of automated components and processes, and access to real-time production data, will empower end users to migrate to

smarter machines. As production benefits in terms of cost reduction, reduced downtime, quality, and throughput, are achieved and competitive advantage gained, so the drive to smarter machines will quicken and expand into a broader spectrum of industries.

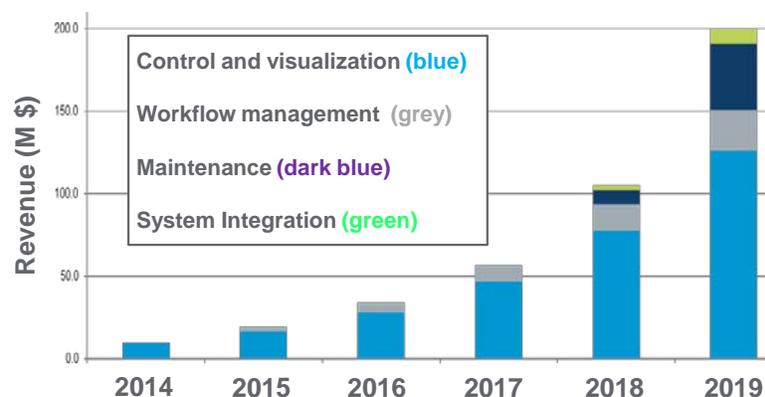
Key characteristics of smart machines include the following:

- **Self-awareness** – Any deviation from set parameters will be identified by the smart machine and communicated to the machine operator. Machines at the forefront of development will use sensors with embedded intelligence to distribute and automate decision making on the factory floor.
- **Plug & play** – Any new smart machines will need to be compatible with the existing installations or machinery from multiple OEMs; End users want devices that can be installed within a short timeframe. Integration into the rest of the system must be easy.
- **Safety & cyber security** – With security built into their fundamental designs, smart machines will improve safety of operators and minimize the security risk of increased networking.
- **Connectivity** – Smart machines will connect directly to the broader (IP-based) network. This enables data sharing and production planning, which goes far beyond the capabilities of traditional standalone machinery and automation. Smart machines will bridge the IT / OT gap, making available production data that can be used in numerous management settings (e.g., stock control, operator scheduling, maintenance, energy management, and product replacement).

Major trends that support the proliferation of smart machines include the acceptance of mobile devices to manage core business functions, and the ability to harness and interpret the mountains of data that are being captured by the smart devices.

- **Mobile devices** – Mobile technologies, which are experiencing rapid growth within the industry (see **Figure 6**), now free operations personnel from needing to be in close proximity to a machine in order to monitor or manage performance. Now, machine engineers can diagnose problems and offer guidance remotely. This cuts costs and also speeds-up solution implementation.

Figure 6
Global market projections for industrial mobile applications
(courtesy of HIS)



- **Data Management** – As sensors and other networkable components are added to machinery, huge amounts of production data are being generated. Even with relatively simple applications, this could easily lead to data overload and the inability to use production data to support real time decision making. Smart machines must have some level of intelligence to assess data quickly and in a decentralized fashion. Routing all data to a central control for analysis will quickly lead to delays, and is an un-scalable structure. Having sensors, components and machinery with the intelligence to only share data that falls within a set of pre-defined parameters, will lead to better data management. Reducing the level of data shared with the broader network/community, will speed up decision making and reduce backlogs (where critical information could be delayed or missed altogether).

Evolving instrument communications in the IIoT age

By Peter Sherwin, Global Marketing Manager, Eurotherm by Schneider Electric

Control and data recording instrumentation

Over the past 15 years, quality requirements in regulated industries started to evolve and influence the direction of instrumentation design and application. Digital data needed to be captured in a secure format and an evolution of accuracy specifications required better levels of repeatable process control. This affected the Aerospace and Automotive industries, Pharmaceutical and Biotech industries (driven by the FDA) and now is starting to impact the Food & Beverage industry through the Food Safety Modernization Act (FSMA).

Both early recording devices and more advanced devices that incorporated web servers and Ethernet provided a full view of the instrument screen at any PC on the plant network. In addition, security features were added to recording instruments to provide security management and audit trail functionality. These smart recorders evolved into miniproductivity stations enabling key information for thermocouple use, calibration tests and machine maintenance to be scheduled directly on the device.

Quality standards dictated that direct communication links be established between the control device and the recording instrument to eliminate errors created by conventional retransmission methods. Ethernet-based Modbus TCP was used for device-to-device communications to accurately transfer the control data to the process record.

For many years, instrument manufacturers have adopted the DIN standard for panel mounted instruments, with standardized panel cut-out dimensions for controllers, recorders, and other boxed mechanical devices. Devices since introduced that incorporated multi-loop control, secure data-recording, integrated Ethernet and built-in web servers can now be seen as one of the first range of IIoT mini-stations providing a necessary cost effective link between sensors and the internet.

Current developments on this type of smart device will enable widespread use in both regulated and non-regulated industries. Such a solution provides a cost-effective means for generating advanced calculations (including Overall Equipment Effectiveness) as well as a secure data link to the internet.

Power devices

Silicon controlled rectifier (SCR) power controllers (or thyristors) were developed to provide a precise method of electrical switching in the control of power circuits. They were also designed to overcome the limitations and lifetime issues of mechan-

ical contactors. The SCR technology is now being used to take an isolated controller and provide a system approach to managed power demand.

A number of SCR devices will fire randomly at what could be many times per second. If the units fire at the same time, then the load demand increases. By using power sequencing across an Ethernet backbone to enable automated load balancing and load shedding techniques it is possible to order the firing pattern and reduce the ultimate peak load demand. These smart connected devices can be used for single or multi-zoned equipment and also can be leveraged across multi-equipment cells. Communicating on an Ethernet backbone allows for future possibilities in automating the links between a utility supplier and the plant floor so that efficient power demand scheduling can benefit both parties.

Workflows

Instrument-to-instrument communication has been a feature of IIoT development over the past 10 years. It is recognized that to increase the value attributed to automation projects, the links between the equipment, operator and supply and delivery chain need to be developed. Workflow type applications are leading the charge in this area. Below are some examples:

- Production applications that embed regulatory IP into workflow solutions provide a link between machines and decision makers in real-time. This ensures regulatory requirements are constantly being achieved and that auto-alerts are raised for any standards breach.
- Dairy applications that link to their remote supply chain using cloud technology and regulatory parameters provide a control and data process to address all points in the supply chain from cow to table.
- Calibration applications that facilitate easy regular equipment calibration checks. This is a key requirement for many regulated industries. This can now be achieved with the introduction of online services using cloud storage of calibration records. Inputs include tablet entry and a link to secure files through QR codes from the instrument label (using a Smartphone/tablet QR reader).

Driving business value for process control industries through smart connected assets

By Don Clark, Senior Director, Industry Solutions, and Dr. Peter Martin VP Industry Solutions, Process Automation

Automation systems and technologies exist to drive improved value for industrial operations and businesses in a safe and environmentally responsible manner. New trends in automation should be evaluated on two levels – the technological level and the functional level. The technological level deals with the impact of technological advancements on the technology and topology of the automation platform. The functional level deals with the incremental functionality that can be delivered on the automation platform to improve operational and business value. The IIoT movement provides significant transformation at both levels, with the net impact being a significant increase in the value industrial companies derive from automation.

“These technologies create an environment which removes many of the traditional technological constraints imposed on automation systems.”

Most of the current fervour associated with IIoT has been at the first level. There are a number of technologies including connectivity, networking, big and small data analytics, cloud computing, fog computing, wireless communication, cyber physical systems and edge computing that are gaining a high level of acceptance in the industrial sector. Independently these technologies are promising. In combination, however, they offer an unprecedented opportunity. Together, these technologies create an environment which removes many of the traditional technological con-

straints imposed on automation systems. Automation systems designers now can design an automation system from a clean slate.

Cost, speed, and size limitations of older technologies have led to automation architectures and topologies being defined by the technological constraints. The result has been the development of two different industrial operations topologies; the automation system topology and the industrial operations topology. This has caused an increase in complexity in industrial operations as personnel had to learn both topologies to effectively operate a facility.

With new levels of agility offered by IIoT, the topology of automation systems can be perfectly matched to industrial topologies, drastically simplifying the application and operation of both.

These new automation systems topologies will be called natural topologies due to their natural alignment to industrial operations. The expected result of this alignment will be the application of automation systems to each asset and asset set in the industrial operation, from the simplest piece of equipment through to process units or work cells, trains, areas, plants, fleets and enterprises. This will lead to simplified environments with unified smart connected asset control systems combined into smart industrial enterprise control systems. Under such a system, the operation of each asset and asset set is controlled for optimal business results.

At the functional level, automation systems were originally developed to control processes in real time. Most real-time process control implemented to date has been focused on improving the efficiency of a process or machine, and not the operation as a whole. Although improving efficiency is important, it is far from the only domain to which real-time control should be applied in industrial operations. As the speed of industrial businesses has continually increased over the past decade, managing industrial assets on a human, transactional schedule has proven to be insufficient. Important industrial variables, such as profitability, safety risk, environmental risk, reliability and security risk that have traditionally been managed on a daily, weekly or monthly schedule have now transitioned to real-time. Therefore, it is no longer possible to keep managing them in the same way.

Real-time controls are needed to support these important business elements. Decisions influenced by either manual or automatic, feedback or predictive controls need to be made fast enough to positively impact the operation of a process. Real-time controls will need to be applied to improve the efficiency, reliability, profitability, safety risks, environmental risks and security risks for each asset and asset set in industrial enterprises. This will result in true asset performance control which will then lead to optimal enterprise performance.

Conclusion

While the interest in IIoT has reached fever pitch, there are several reasons IIoT should be seen as an evolution, not a revolution. End users have invested hundreds of millions in industrial automation and control systems and are absolutely unwilling to invest hundreds of millions more to replace those systems with new technologies. Even if a valid business case could be made for system “rip and replace” due to the benefits of IIoT, end users would nevertheless still resist the change because of the increased risk of downtime and associated costs.

In addition, visionary automation suppliers like Schneider Electric and select end users have been quietly working towards this goal for over 15 years. The concept of embedded web servers and the use of Ethernet as a real-time control network to allow ubiquitous access to information “transparently” from anywhere within the enterprise was first brought to the market by Schneider Electric in the late 1990s. Presented as “Transparent Factory”, the concepts are clearly echoed in the IIoT story of today.

Advances are still required in the area of standards to fully realize the potential of IIoT. Nevertheless, despite the slow adoption rate, the impact of IIoT on manufacturing will be farreaching. Suppliers and users must start adopting IIoT technologies in their products and operations if they wish to remain competitive in the marketplace. The good news is that technological maturity is such that businesses and enterprises can now introduce IIoT solutions by phasing in new technologies that shift their physical infrastructure base over time. The cost of connected sensors is dropping rapidly, open IP-based protocols are gaining traction at an accelerating rate and the adoption of cloud-based solutions is becoming a reality. Suppliers like Schneider Electric have the expertise to work with manufacturing companies to apply IIoT technologies to production systems and drive the evolution towards the smart manufacturing enterprise that is more efficient, safer and more sustainable.



About the author

John Conway is Schneider Electric's VP for Strategy & Partnerships. In this capacity, he is responsible for strategic intelligence, strategic planning and merger & acquisition activities for the Industry Business Unit. During his 17 years with the company, he has held a variety of roles, starting out as director of microelectronics key accounts. He then moved into the creation and deployment of automation solution centers in Asia and Eastern Europe before running the Advanced Services and Mergers & Acquisitions activities for Industry. Prior to joining Schneider Electric, John held sales and engineering management positions within the automation divisions of Siemens and Texas Instruments.

John has a Bachelor of Science in Mechanical Engineering and a Master of Science in the Design of Machine Systems. He is currently based at Schneider Electric's Horizon office in Carros, France.



Acknowledgements

Many thanks to the contributing expert perspectives:

- **Eric Farrugia**, VP Strategic Marketing, Industrial Controls and Drives, Schneider Electric
- **Dr. Rainer Beudert**, Marketing Director Machine Solutions, Schneider Electric
- **Matthew Carrara**, VP, Field Devices, Schneider Electric
- **Michael Davis**, Senior Program Manager, Field Devices, Schneider Electric
- **Don Clark**, Senior Director Industry Solutions, Process Automation, Schneider Electric
- **Dr. Peter Martin**, VP Industry Solutions, Process Automation, Schneider Electric

Special thanks **Roxanne Hughes**, Schneider Electric Marketing Communications Manager, Strategy and Planning, for supporting the writing, editing, and development of this white paper.