

# Industrial Internet of Things

A high-level architecture discussion

November 19, 2017

PCI Industrial Computer Manufacturer's Group

Prepared By: Doug Sandy, Vice President of Technology

## Introduction

The concept for the “Internet of Things” appears to have been born out of work within MIT and Berkeley in the 1990s and was coined as a phrase in 2004 in an article in Scientific American (Neil Gershenfeld, 2004). The original concept allowed everyday objects to connect with one another in order to provide added benefit to the user. In this vision, household appliances, vehicles, smart wearable devices, parking meters – virtually everything would be connected in order to provide additional layers of intelligence and guidance.

Over a decade has passed since the concept of IoT was introduced and the vision has yet to fully materialize. Some strides have been made with small wearable devices, thermostats, and smart phones, but the average consumer has yet to experience significant advantage from interconnected devices working together for their benefit. Cloud computing, big data analytics and artificial intelligence may help to change this trend, but each of these technologies also brings new challenges. The largest barriers to commercial IoT rollout today appear to be technological (security), sociological (privacy), and economic (cost vs benefit).

This is not to say that the future of IoT is bleak, but rather, its immediate application may be best suited to areas where these barriers are less significant. The industrial markets that PICMG serve are such a place. In military, medical, transportation, and industrial automation, the adoption and use of embedded computing and control solutions has long been commonplace. PICMG’s computing technologies today are used in ground, air and sea-based military applications, they control railroads and factories, and they provide critical functionality to scientific and medical equipment.

At PICMG we seek to accelerate the adoption of industrial internet of things (IIoT) in the markets we serve by providing meaningful open specifications and design guides to aid our member companies in creating high-quality, interoperable computing solutions. We are doing this by leveraging our historic strengths in industrial computing, expanding our community of practice to embrace a wider audience of IoT developers, and building partnerships with other IIoT-focused standards organizations.

## Distinctions of Industrial Internet of Things

If industrial market segments have been deploying automation for decades, what makes IIoT different? There really are only three main distinctions: ubiquitous sensing, advanced analytics, and IT methodologies. Each of these is described briefly below.

### Ubiquitous Sensing

Analogous to the broader IoT space, which envisions ubiquitous connectivity of intelligent devices, Industrial IoT is characterized by ubiquity of connected sensors and actuators. Where traditional automation employed sensors and actuators primarily for the most critical elements of control, IIoT includes sensors and actuators for facility operations, machine health, ambient conditions, quality, and a variety of other functions. Virtually everything that can be measured and controlled within the industrial context is fair game for IIoT. The ubiquity of sensing and control is key to enabling the next cornerstone of IIoT – advanced analytics.

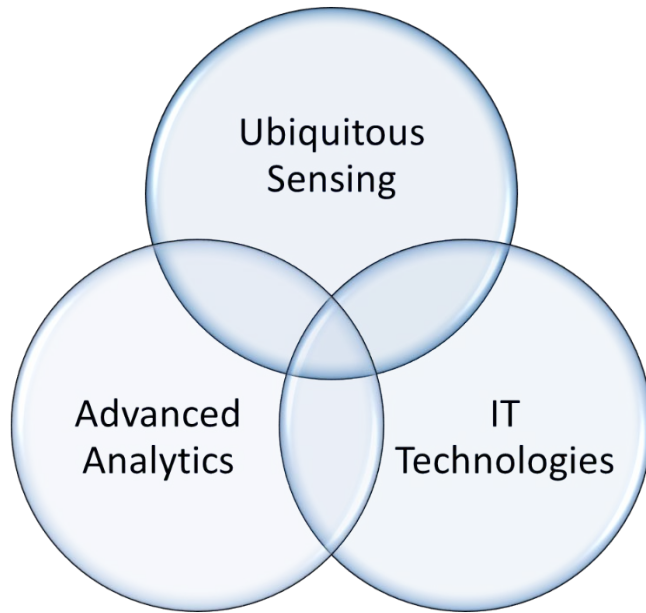


Figure 1- Key distinctions of IIoT as compared to traditional industrial automation

### Advanced Analytics

Advanced analytics enables the IIoT system to realize higher levels of operational efficiency by extracting meaning from a vast array of deployed sensors. Similar to cloud datacenters, where sensors data is used to optimize virtually every aspect of operational efficiency, smart factories and other IIoT applications utilize analytics to improve uptime, optimize asset utilization, and reduce overhead costs. Improved operational efficiency provided by advanced analytics is the primary motivator for IIoT adoption today.

### IT methodologies

The third defining characteristic of Industrial Internet of Things is the transformation of traditional automation techniques to utilize technologies that have been historically associated with information technology. This transformation has three key benefits. First, migration to IT technology enables the IIoT operator to utilize the large IT talent pool to deploy, monitor, and optimize their IIoT application. Second, standardization around IT practices helps to eliminate islands of proprietary equipment within the installation and provide tighter integration between the control domain and the operations domain. Lastly, adoption of IT methodologies enables IIoT companies to leverage the large existing base of IT hardware and software solutions when appropriate. Each of these benefits offers significant potential for capital and operational savings.

### Barriers to Adoption

A recent study by Morgan Stanley (Morgan Stanley, 2017) indicates the top three challenges to IIoT deployment in order are: cybersecurity, lack of standardization, and legacy installed base. Each of these is summarized briefly below.

### Cybersecurity

Cybersecurity in IIoT takes on new dimensions because the connected devices interact and control real world activities. Connected factories, power plants, aircraft and other vehicles pose significant threats

to public safety if hacked. Corporate and national economic impacts also cannot be overlooked. The collapse of a power grid or national transportation system has much farther reaching impacts than even the largest consumer data breaches. For these reasons, robust cybersecurity is an absolute essential in IIoT. It is expected that most IIoT applications will run on private, dedicated networks with strict physical access control protocols.

### Lack of Standardization

Historically, industrial automation has been accomplished using a variety of proprietary, vertically integrated automation solutions, or by open standards-based industrial computing solutions such as PICMG's CompactPCI. While the first of these solutions offers convenience of an integrated approach, each vendor's equipment may not work well with others. This causes islands of isolated equipment within the industrial deployment that is difficult to integrate and manage as a whole. The second solution, while offering many benefits such as scalability, flexibility, and less risk, often puts the burden of software creation on the operator. This can be cumbersome when attempting to assimilate the large number of dissimilar sensor types associated with IoT deployment.

Standardization of the upstream interfaces for controller devices and meta-data models for sensors would go a long way toward eliminating both of these problems. Standardized interfaces would allow dissimilar pieces of hardware to communicate with the IIoT command center in a uniform fashion and eliminate isolated islands within the installment. Likewise, an extensible standardized meta-data model for sensors would allow for systematic detection and control of sensors and control points without extensive code re-writes. From a hardware standpoint, IIoT would also benefit from greater standardization around communications interfaces, power, and environmental requirements.

Large industrial automation suppliers are not incentivized to embark on open standardization because it loosens the customer's dependence upon their proprietary solutions. Smaller automation suppliers lack the industry clout or size to take on such an ambitious undertaking. This is a task best suited for an industry standards organization, and one which PICMG is well equipped to handle.

### Legacy Installed Base

Very few technology transformations occur overnight. As a result, legacy equipment must be able to coexist with the new. Any successful IIoT strategy must incorporate this reality. Standardization can help bridge the gap in the short term and PICMG is preparing to apply its track record of backward compatibility and interoperability toward alleviating the worst of these issues.

## Architectural Overview

Because factory automation is projected to be the largest and fastest growing segment of the Industrial Internet of Things market, this section of the document focuses on an architecture for the smart factory. This selection was chosen merely as an example of a relevant application to which the IIoT architecture may be applied. Figure 2 shows an example of a smart factory layout.

### Smart Factory Example

The factory floor is the heart of the smart IIoT application. It contains multiple robotic assembly machines, automated test equipment and various other process-related pieces of equipment. Each of these is fully automated and integrated utilizing the same network interfaces and common data model

and protocols. In addition to control and monitoring of the actual manufacturing process, the machines are also instrumented with other sensors to help assess the health of the equipment and correlate operational dynamics with factory output quality.

In order to feed the automated factory, the warehouse and stockroom is also fully instrumented. Because the factory control and the inventory control systems both leverage IT methodologies, integration and analysis between the two domains is easily achievable, allowing actual factory production rates to factor into intelligent purchasing and inventory management algorithms.

Environmental conditions are monitored in real time providing useful information regarding energy usage from air conditioning, lighting and other resources. This function also monitors and controls other resources such as on-site power generation and backup generator status. This information, combined with deep analytics, may be used to prioritize workloads in order to optimize resource utilization and minimize operational costs.

All of these functions are interconnected with the factory control center via Ethernet (or industrial Ethernet when required). The control center provides visualization and control of the entire factory operations utilizing standard IT technologies.

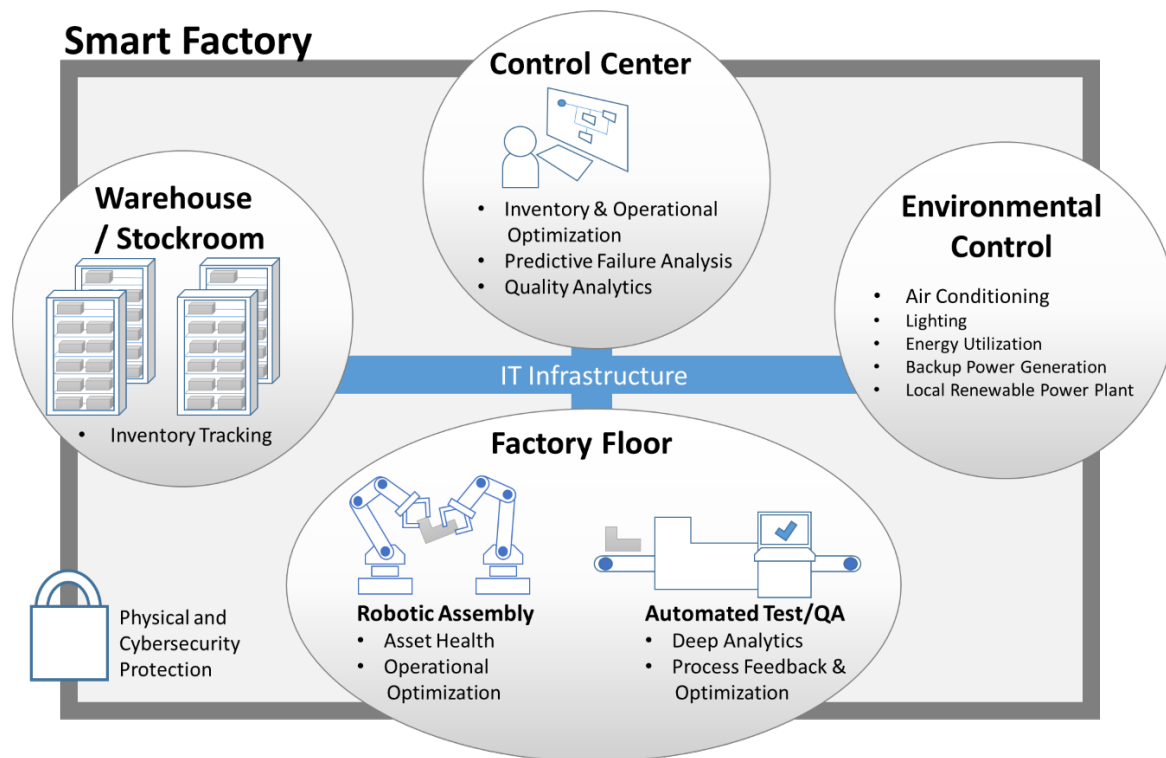


Figure 2- Smart Factory Layout

## Architectural Decomposition for IIoT

Figure 3 shows an architectural decomposition for Industrial Internet of Things. All components are connected via Ethernet (or industrial Ethernet) unless otherwise shown. Legacy equipment co-exists with newer equipment, though potentially at a lower level of functionality, and a common metadata model enables discovery and control of IIoT devices in a flexible and extensible fashion.

At the lowest level of the architecture, sensors and control points provide connectivity to physical phenomena within the factory. IIoT sensors present themselves as intelligent, managed devices over the factory network using the common meta-data model. Using RESTful application programming interfaces, sensors may be monitored and controlled using standard IT methodologies. Because these sensors operate in a live factory environment, ruggedization is an expected requirement.

For sensors and actuators that must respond in a hard, real-time fashion, it may be necessary to place a controller close to devices in order to monitor the devices locally. This reduces the latency and improves determinism over having the devices remotely controlled through the factory control center. These local IIoT controllers would present the connected sensor data models to the upstream control center. They would also introduce programmable “listener” functions that implement local policies when sensor events occur. Listener functions may also be directly implemented in sensors and actuators.

Legacy sensors and controllers may be connected to the IIoT control center. Initially, PLCs can be connected over their existing interfaces and be managed through legacy software. As an intermediate step to full IIoT functionality, the PLC can later be replaced by an IIoT control gateway. This device “translates” the sensor’s native protocols to a RESTful data interface using the common meta-data model. This allows the same sensors to be used while the control architecture is migrated to IIoT technologies. As a final step, sensors can later be replaced with fully IIoT-enabled sensors.

The final piece of the IIoT architecture is an aggregating network gateway. This device serves to aggregate and isolate traffic between zones on the factory floor and the rest of the network. In many cases, the bandwidth of traffic from the factory devices will be low so a ruggedized, 10/100/1000 switch will typically be more than sufficient.

## RESTful APIs

REST, which stands for REpresentational State Transfer, is a communication architecture style based on the IETF RFC 2616 protocol (Fielding, 1999). With REST, web resources provide textual representations of themselves that may be manipulated by using common verbs (i.e. GET, POST, PUT, DELETE). RESTful APIs are a necessary skill for any modern web designer and RESTful APIs built on HTTP and JSON and other protocols are common.

A RESTful approach was applied in systems management applications for cloud computing by the DMTF (Distributed Management Task Force) Redfish technology (DMTF, 2017). Building management interfaces using RESTful APIs allows operators to deploy a scalable interface that leverages existing web skills and taps into the momentum from a growing IT technology base.

Currently no RESTful APIs are defined to specifically meet the needs of Industrial IoT.

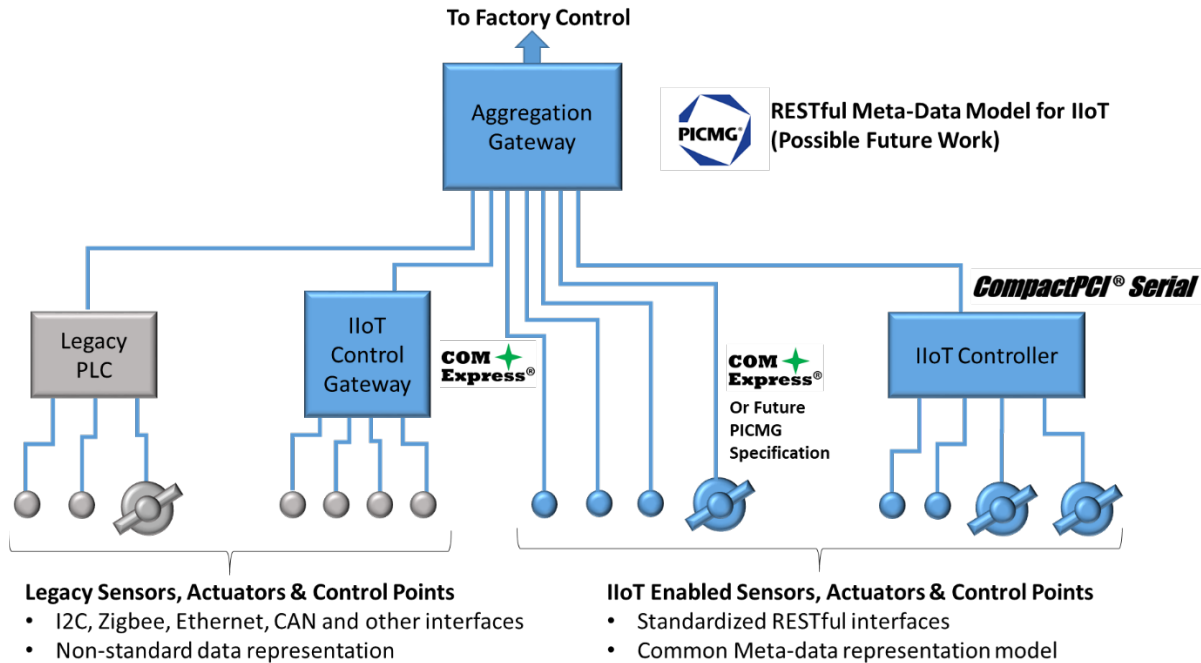


Figure 3- IIoT Components showing areas of PICMG contribution

## PICMG Contributions to IIoT

Because of the importance of industry standardization to IIoT rollout, and PICMG's long-standing support of the industrial computing marketplace, the opportunities for PICMG contributions are strong. In particular, COM Express is well suited for small gateway control and IIoT controller functions. CompactPCI Serial may also have a play in larger IIoT controllers and control gateways where scalability is required.

The COM Express® specification (PICMG, 2017) defines a family of Small Form Factor (SFF) and Computer On Module (COM) single board computers appropriate for a wide range of commercial applications. It is designed for the latest chip sets and serial signaling protocols, including PCI Express Gen 3, 10GbE, SATA, USB 3.0, and high resolution video interfaces. COM Express provides the highest performance of the many small form factor standards and products available. When used in conjunction with an I/O base-board, COM Express can easily interface to the wide array of legacy industrial control interfaces deployed today.

CompactPCI Serial® finds its origins in PICMG's first truly ruggedized industrial automation platform (PICMG, 2011). With multiple expansion slots based off of PCI Express, CompactPCI Serial is a high-performance, flexible platform that has been successfully deployed in a variety of industrial applications.

A third hardware form-factor (not yet developed) may also benefit I/O sensor vendors. This form factor would feature ruggedization, low power operation, moderate processing capabilities, and a postage-stamp size board outline. Such a form factor would allow today's sensor vendors to quickly migrate their existing products to fully IIoT compatible devices by leveraging off-the-shelf solutions from a variety of manufacturers.

As important as hardware is, the software meta-data model is key to the success of Industrial IoT and provides the best place for PICMG to contribute to the overall adoption of IIoT. While this effort is not directly aligned with the hardware platform management efforts of the past, PICMG has domain expertise in this area that is directly applicable. DMTF is the other industry standards organization that has been involved in this area with the development of the Redfish schema for datacenters. PICMG is currently exploring how to best work with DMTF in order to provide a solution for a unified data model for Industrial IoT.

PICMG is committed to accelerating the roll-out of Industrial IoT. Through standardization, these solutions significantly improve the ease in which IIoT installations can be deployed. If you or your company are interested in joining PICMG in this effort, please contact us using the information below.

Douglas Sandy  
CTO & Vice President of Technology  
[sandy@picmg.org](mailto:sandy@picmg.org)

Justin Moll  
Vice President of Marketing  
[justin@picmg.org](mailto:justin@picmg.org)

## About the Author

Doug Sandy is the Vice President of Technology for PICMG with over 24 years of industry experience in the embedded computing, industrial automation, telecommunications and cloud computing spaces. Doug has worked as Technical Fellow, Chief Technology Officer and Chief Architect for major corporations including Motorola, Emerson, and Artesyn Embedded Technologies. Sandy has focused much of his career advancing industry standards that provide multi-vendor interoperability and COTS solutions such as DeviceNet, ETSI NFV, and the PICMG families of specifications. He now enjoys training the next generation of engineers at Arizona State University's Polytechnic Campus where he is a full-time educator and program coordinator for software engineering capstone projects.

## About PICMG

PICMG is a nonprofit consortium of companies and organizations that collaboratively develop open standards for high performance telecommunications, military, industrial, and general purpose embedded computing applications.

There are over 150 member companies that specialize in a wide range of technical disciplines, including mechanical and thermal design, single board computer design, very high speed signaling design and analysis, networking expertise, backplane and packaging design, power management, High Availability software, and comprehensive system management.

Founded in 1994, PICMG's original mission was to extend the PCI standard to non-desktop applications. The formal name of the organization is the PCI Industrial Computer Manufacturers Group. It is now known as PICMG (pronounced "PICK-EM-GEE" or "PICK-MIG").



Equipment built to PICMG standards is used worldwide and anyone can build or use equipment without restriction (although certain technologies used for some military applications may be subject to U.S. export restrictions governed by ITAR rules).

Key standards families developed by PICMG include: CompactPCI®, AdvancedTCA®, MicroTCA®, AdvancedMC®, CompactPCI® Serial, COM Express®, SHB Express®, and HPM (Hardware Platform Management).

## References

DMTF. (2017). *redfish*. Retrieved from DMTF: <https://www.dmtf.org/standards/redfish>

Fielding, R. e. (1999, June). *IETF RFC 2616*. Retrieved from [www.ietf.org](http://www.ietf.org):  
<http://www.ietf.org/rfc/rfc2616.txt>

Morgan Stanley. (2017). *Automation World Industrial Automation Survey*.

Neil Gershenfeld, R. K. (2004). The Internet of Things. *Scientific American*.

PICMG. (2011, March). PICMG CPCI-S.0 CompactPCI Serial Base Specification Revision 1.0 .

PICMG. (2017, March). PICMG COM.0 COM Express Base Module Specification, Revision 3.0.