ISA InTech Cyber-IIoT article

Convergence and Commercial Momentum Drive the Industrial Internet of Things (IIoT) Evolution

Ms. Marissa Morales-Rodriguez, Oak Ridge National Laboratory, Director-Elect of ISA Test & Measurement Division

Dr. Sterling Rooke, X8 LLC, Director-Elect of ISA Communication Division

Dr. Peter Fuhr, Oak Ridge National Laboratory, Director of ISA Test & Measurement Division

Dr. Penny Chen, Yokogawa, Director of ISA Communication Division

Introduction:

Industrial instrumentation and sensors are purpose-built for applications. Rugged and proven for field applications in harsh environments such as oil platforms or 5,000 feet below ground in a copper mine, these instruments require reliability and performance. Before the turn of the millennium, industrial technology—and information technology in particular—drove these systems and often exceeded the abilities of consumer products. ~~In recent years, this trend has changed.~~ However, ~~A~~as we stand today, commercial Internet of Things (IoT) technology has advanced rapidly, with industrial control systems lagging in intelligence and features.

Experienced owner-operators of industrial facilities recognize the buzz surrounding the Industrial Internet of Things (IIoT) but often shun the notion of consumer-grade devices being installed and integrated into an operational control system. During the International Society of Automation (ISA) Process Control and Safety Forum (PCS) in Houston, Texas, in November 2016, ISA's Communication Division convened a panel to focus on IIoT. Experienced industrial and control engineers on the panel expressed concerns and reservations with IIoT. Whereas some acknowledged an interest in the topic, others did not recognize it as an inevitable part of the industrial controls landscape. Granted, IIoT is still mostly a vision in the instrumentation and automation landscape; however, its place on stage is coming into view. During the opening session of PCS 2016, ISA President Jim Keaveney rhetorically asked the audience if IoT had peaked and also wondered if "cyber" would be the next area for innovation. This paper will explore the nexus of "domestic" IoT and how product evolution will drive its development toward that of IIoT.

Government to promote IIoT evolution?

On September 1, 2016, the National Telecommunications and Information Administration within the US Department of Commerce (DOC) conducted an IoT workshop. Discussions included how IoT and IIoT were set to converge around common threads. An important area of convergence will occur around onboard components and subsystems with software as a runner-up because of cost and the innate drive to be first to market. However, as the recent Samsung Note 7

battery failure and subsequent recall has shown, releasing a product with flaws that are later discovered in the field by your customers is a bad idea. Despite this, the hype surrounding IoT is truly at its peak relative to other emerging technologies.

President Trump has targeted infrastructure as a key agenda item in his administration. This proposed infrastructure buildout combined with growth in US industrial capacity would benefit from incorporation of IIoT sensors and systems. At the Consumer Electronics Show (CES) in January 2017 in Las Vegas, many companies demonstrated attempts to deploy IIoT in industrial facilities—many with woefully inadequate performance and cybersecurity. The rush to develop and deploy will no doubt result in increased consumer IoT being used for IIoT (again, as on display at CES 2017). The net result of these market and need forces is that they will accelerate the IoT and IIoT convergence.

At the DOC IoT workshop, participants spent a significant amount of time discussing the important role government can play in setting IoT standards. IoT experts at the workshop made it clear that with assistance from the federal government - specifically the Departments of Energy and Commerce and their national laboratories- guidelines for cybersecure and robust IoT could be developed. With help from the government and organizations such as ISA, industry will have a clearer path to develop industry-centric IIoT rather than rush to field consumer IoT devices. The question is that, even with this framework, will simple cost and a discount of risk dominate so that IIoT essentially becomes IoT wrapped in a harder shell? The authors of this paper propose that this is what will occur.

However, we must take heed when it comes to cybersecurity and realize that with commercial IoT, an industrial target could be attacked in a manner similar to an attack on a commercial target—but with very different consequences. The solution? Although we should accept that IoT and IIoT will converge, there must be clear distinctions in cyberarchitecture and associated protections. This goes for implementation as well as regulations and guidelines proposed by both governments and industrial organizations like ISA.

Industrial Internet of Things (IIoT)

Could seemingly trivial items such as Amazon Echo/Alexa be worthy of consideration for industrial automation and applications? Many stalwarts of the status quo voice concerns about safety standards and dangers of this technology in the industrial setting. Although these are valid concerns, a more important concern is that commercial IoT standards or best practices do not always apply to IIoT concerns.

IIoT is a specialized IoT implemented in ruggedized packages suitable for industrial applications environments. In fact, legacy industrial control devices such as Programmable Logic Controllers (PLCs) will be compatible—for the time being—with IIoT running alongside. IIoT benefits from data flowing through standard based and common networks. From a networking standpoint, the IIoT systems will break the ongoing practice of using proprietary networks and bring into place a common standard based networking technology. The convergence of the IT technology and OT operation knowledge for industrial automation environments is well underway. Soon IIoT will approach the network edge for almost every industrial application. IIoT installations can include hundreds or even thousands of sensors across a large facility. To handle all of this

information, one approach is for IIoT to leverage the cloud in a manner similar to the Alexa example with IoT.

In the book *Internet of Things with Python*, the author, Gaston Hillar, illustrates how sensor readings from IoT devices compound into a situation that must be managed (Hillar 2016).

A typical industrial practice involves acquiring one measurement per second from each IoT device. The number of measurements – from just one device - is:

- 60 measurements for all the variables per minute
- 3,600 (60 × 60) measurements per hour
- 86,400 (3,600 × 24) measurements per day
- 31,536,000 (86,400 × 365) measurements per year (assuming a non-leap year)

Consider the situation where an industrial facility has 3,000 IIoT devices running the same code, thereby generating 94,608,000,000 (31,356,300 × 3,000) measurements per year[1]. In addition, it is envisioned that a data ingestion engine may analyze and acquire information from other data sources, such as tweets about weather-related issues in the locations in which the sensors are capturing data. The net result is huge volumes of both structured and unstructured data to analyze computationally to reveal patterns and associations.

From a convergence standpoint, many of these big data repositories and data manipulation centers will be the same for both IoT and IIoT. The key differences are cost and technical capability, and these commercial repositories are quite capable of servicing IIoT data at a low cost. Comingling of data between a home toaster oven (IoT) and the IIoT data from a cement kiln, for example, is not the real worry. The greater concern is a denial of service attack on the large provider. If we consider Amazon and its AWS discussed earlier in this paper and similar technologies, we can appreciate how an attack on a *commercial* business such as Amazon could disrupt critical processes supported by IIoT in a factory.

What constitutes IoT and the technology levels associated with IoT use in, for example, the electric grid? Figure 1 illustrates the situation.

[1] Each IioT device is generating one reading per second.

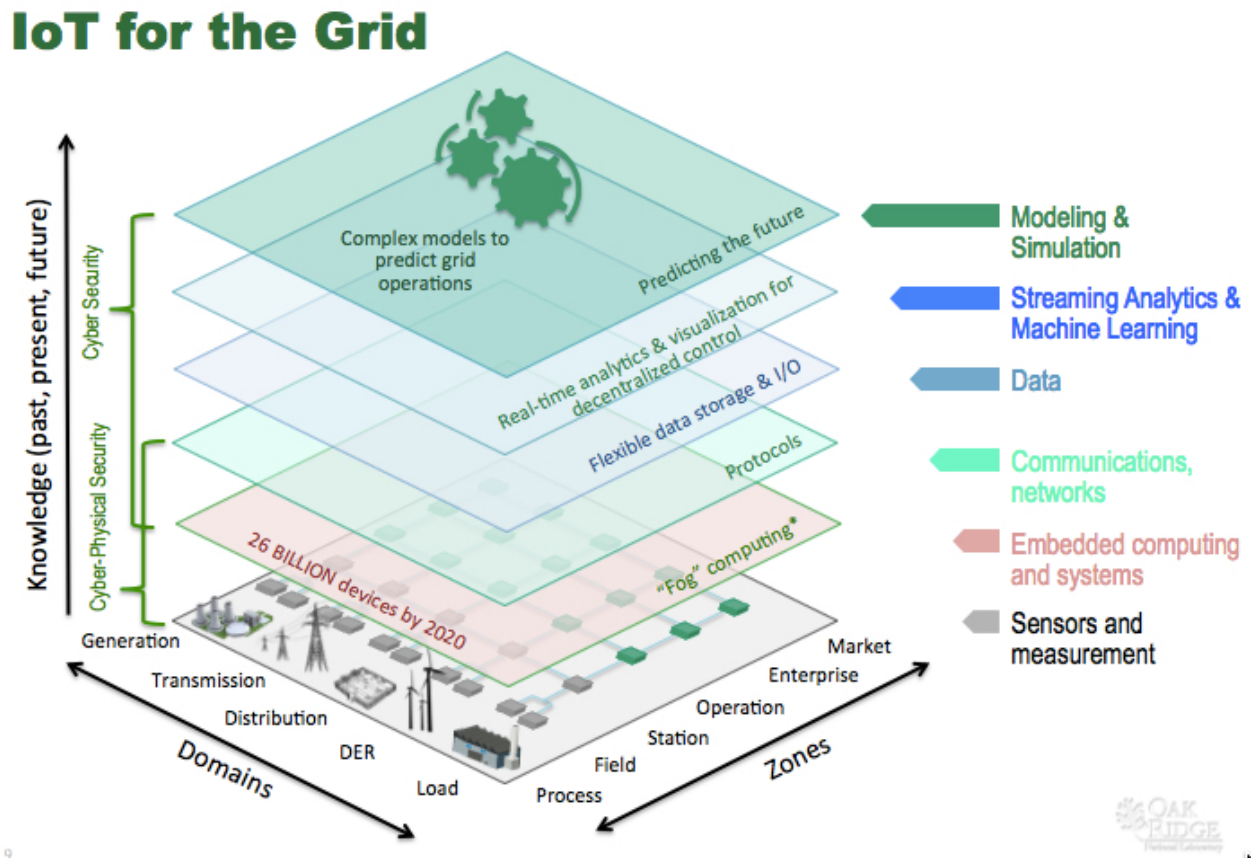


Figure 1. IoT for the electric grid.

Intersecting Technologies

With the introduction and promulgation of IoT devices in an industrial setting, a wide range of questions and problems arise, including the following examples:

1. How do wireless IoT devices all share the frequency spectrum? Such issues of spectrum congestion – such as numerous devices sharing the same frequency spectrum – are lumped into the general category of the "spectrum crunch". One example of the correct answer can be for the IoT device to incorporate levels of spectrum sensing (in essence acting as a spectrum analyzer for the frequencies of "interest") while having spectrum mobility (being able to change operating frequencies easily and quickly). The spectrum subsystem elements for such an adaptable IoT device are shown in Figure 2.

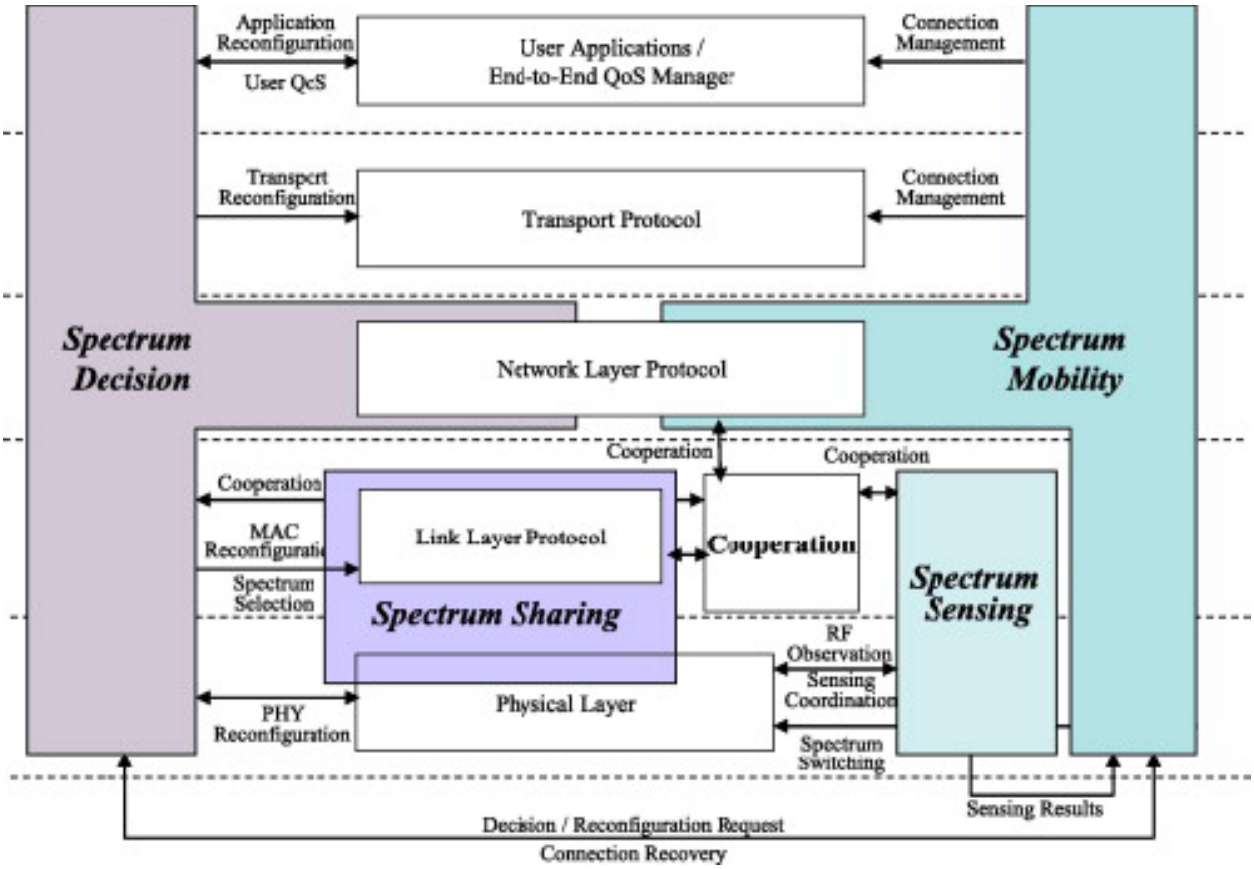


Figure 2. Spectrum sensing, sharing, decision, and mobility functional components of an IoT device for dense deployments in industrial settings.

2. Process control systems speak a wide range of protocols, as shown in Figure 3. Should an IIoT device or system speak one/all of these protocols? Or is having a logical system element perform protocol translation sufficient?

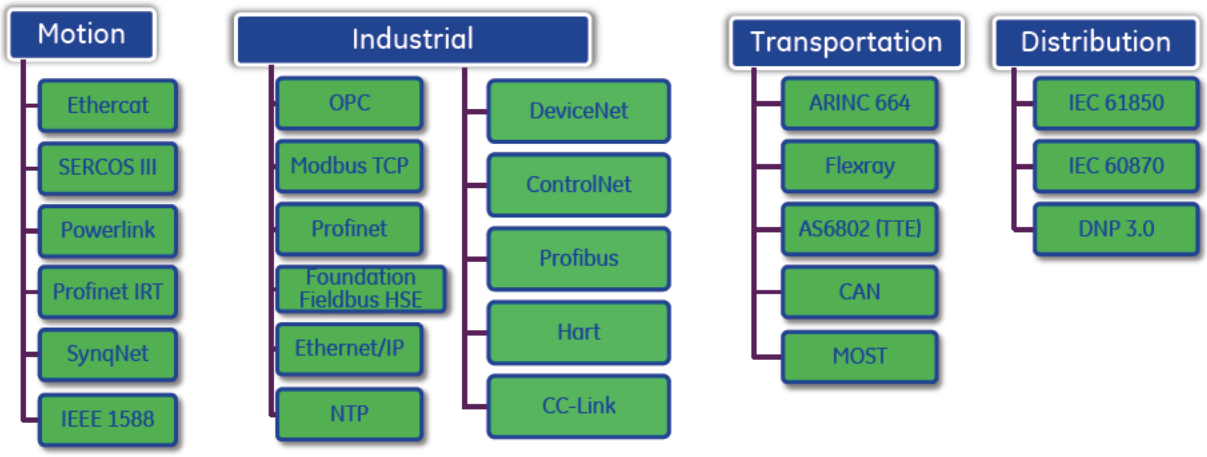


Figure 3. A few of the protocols used in industrial settings are shown.

3. "IP addressable to the edge," such as most IoT device and system designs, causes the logical element and subsystem design—which is foundational to the vast majority of today's industrial networks (see Figure 4)—to be incorrect. IP-to-the-edge can provide wonderful integration into IT-centric networks, thereby allowing IT security applications to have entire network visibility. A "flat architecture" provided by IP-to-the-edge allows for an everything-to-everything level of connectivity. It also allows users to partition a variety of working zones based on its operational or business needs. Authors believe the constraints should be set by applications and business needs not by technology incompatibility. This should be one basic concept of IIoT.

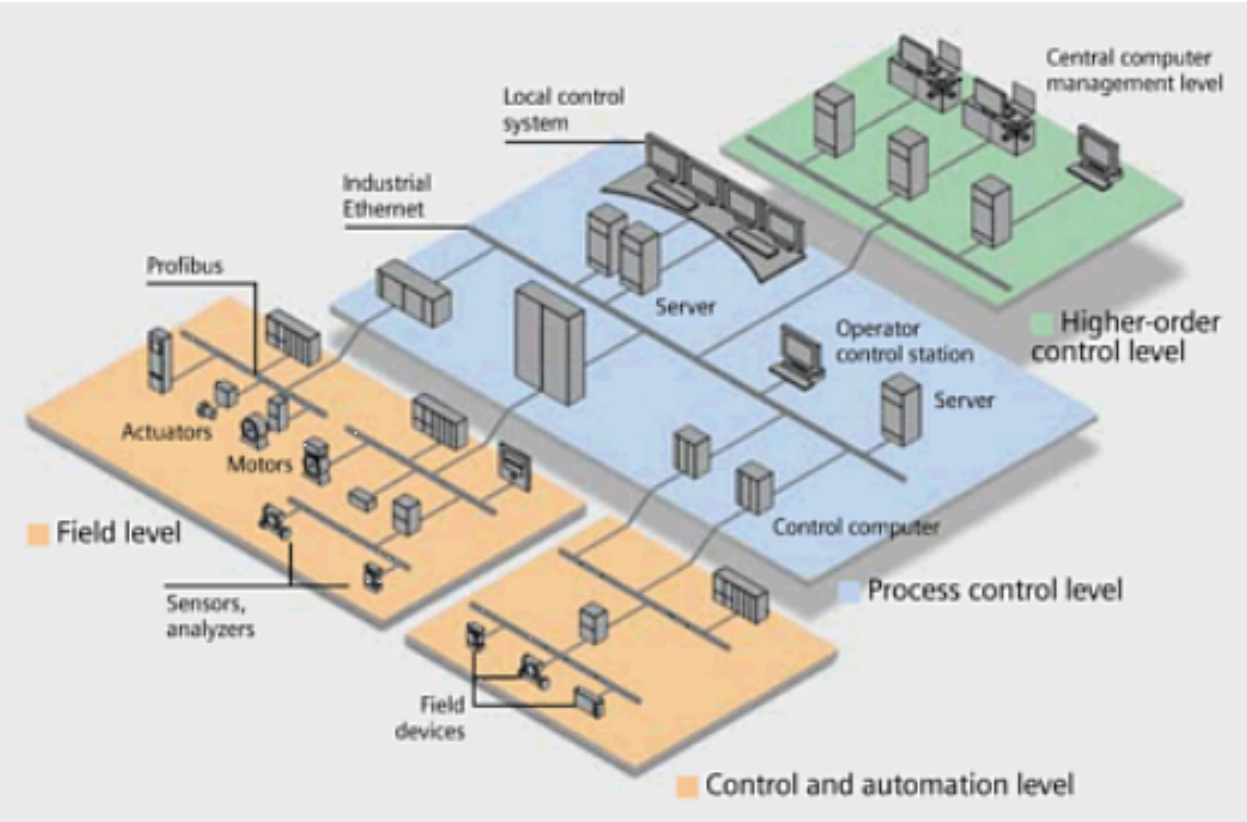


Figure 4. Control and automation system architectures as shown here rely on separation of functionality and components. ISA Instrumentation standards such as SP88, SP95, and SP99 rely on such separations.

4. Sensing technology has also advanced by IoT movement. The IoT edge devices may have varying levels of complexity and functionality with various vendors leaning toward sophisticated (and relatively energy-consumption-intensive operation), whereas others promote the advancing technology of passive wireless sensor tags (with no batteries, extreme low cost, and intrinsically safe operation; see Figure 5). The ISA Communication Division has collaborated with the National Aeronautics and Space

Administration, the US Department of Energy, and other organizations in the past 6 years to conduct passive wireless sensor tag workshops and promote new types of low-cost wireless sensing technologies for IIoT.

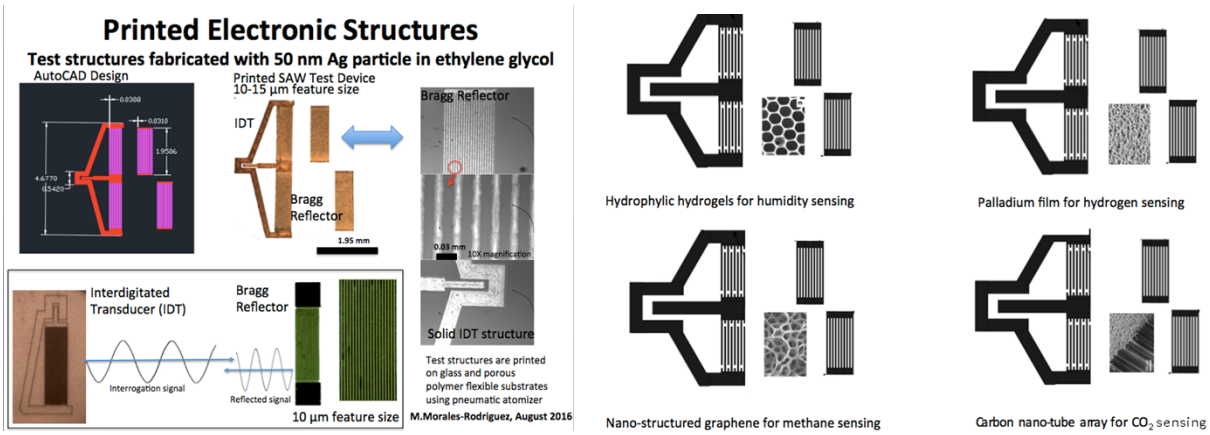


Figure 5. Passive wireless sensors for industrial use may measure chemicals and physical parameters.

5. In essence, the question distills to the following: What does the industrial network have to look like for IIoT devices to be used? Several great standardization activities have been initiated in IEEE and the Internet Engineering Task Force (IETF), such as the IEEE 802.~~3~~ 1 Time Sensitive Network and the IETF Deterministic Network. Those technologies are created to address the need of IIoT, which allow a single network to share its resources and to be deterministic to reserve network bandwidth for time-critical applications. An initial set of functionality and performance "answers" for IoT devices in a factory automation setting is provided in Figure 6.

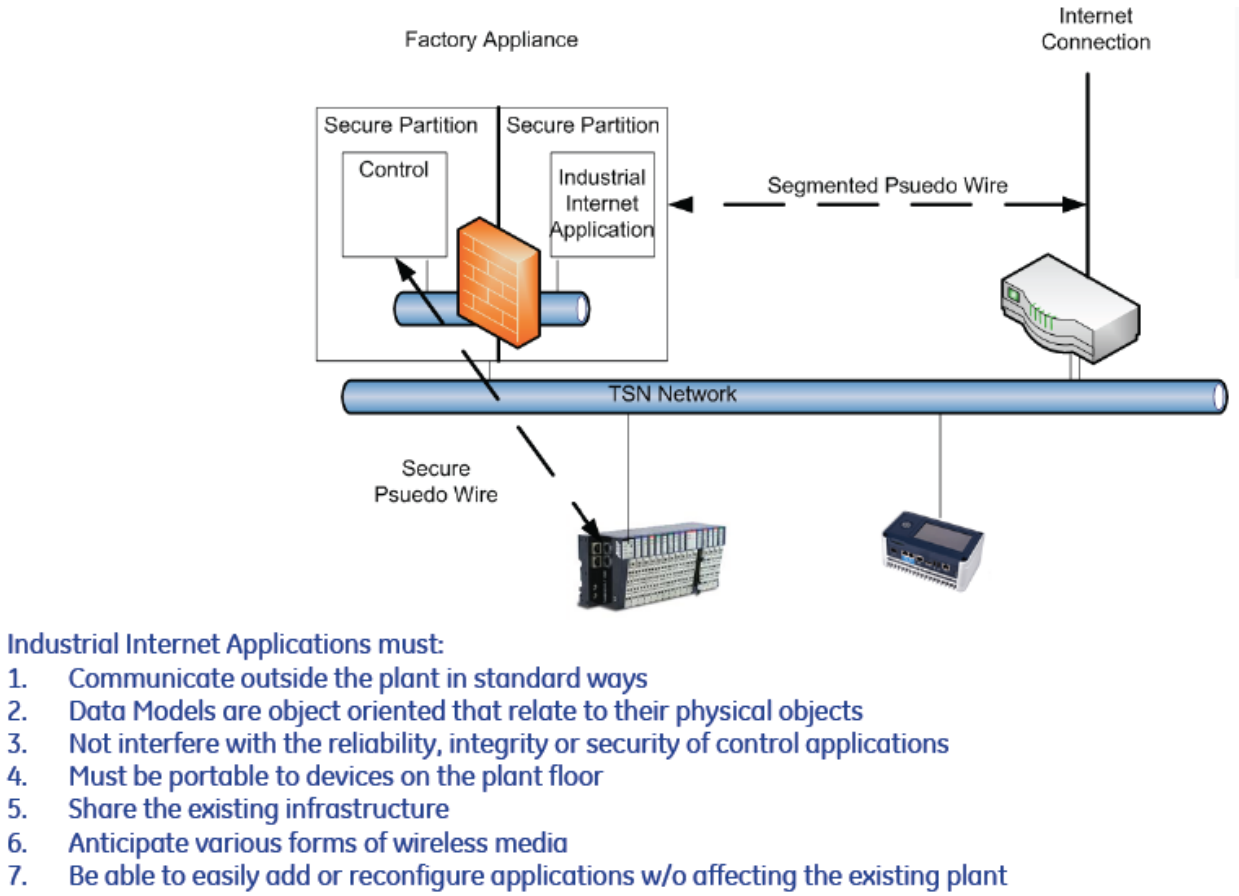


Figure 6. An industrial internet ready time sensitive network architecture.

Data of "things"

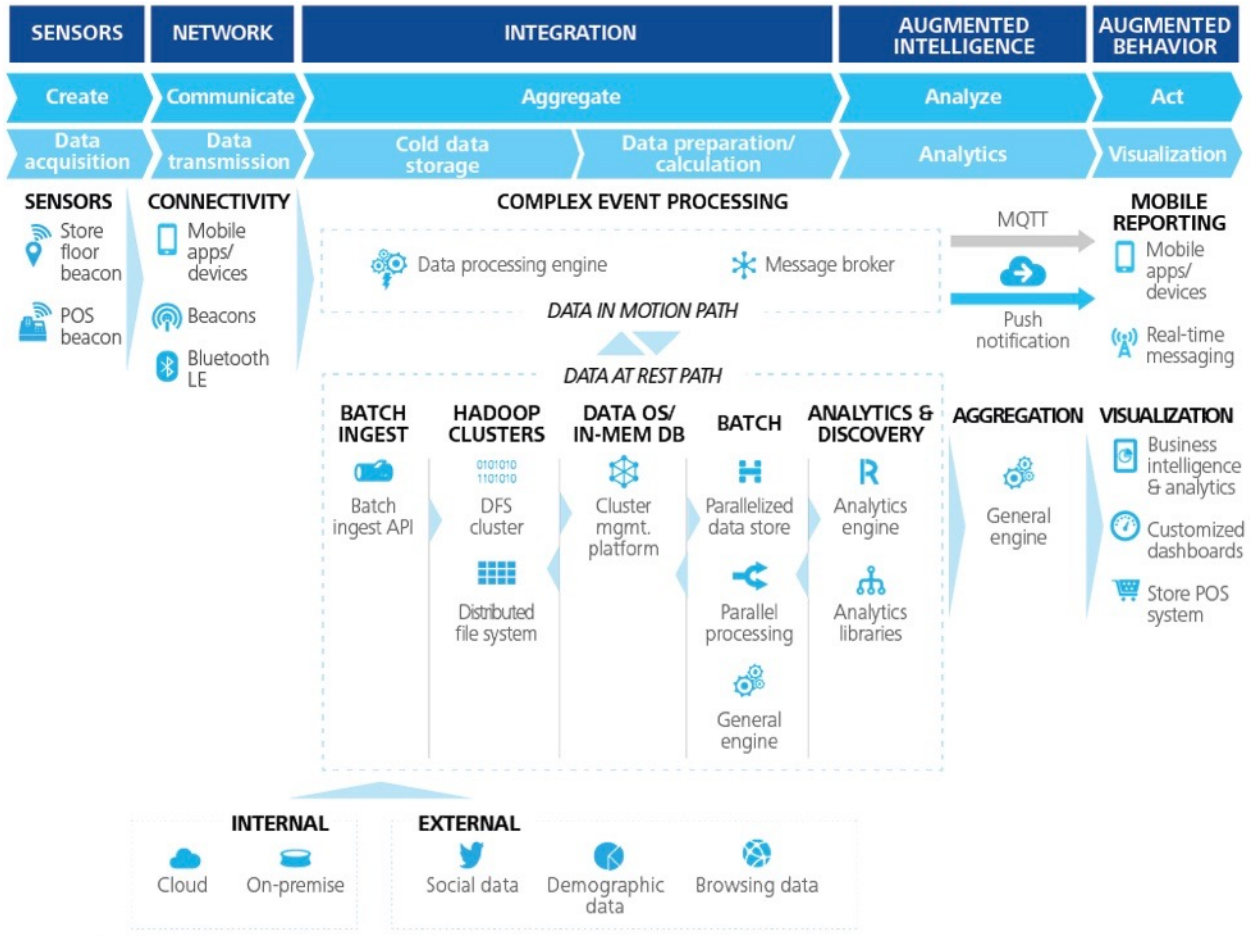
In the preceding section, we introduced the data footprint of IIoT with some simple calculations.[2] In this section, we delve deeper into why IIoT will simply ride alongside or leverage data technology from commercial IoT. Does this affect security in the industrial (IIoT) space? Even if a company does not use the same data storage systems such as AWS or other commercial IoT, its software could have many of the same security flaws. For custom applications such as a factory IIoT system, only small portions of original code are introduced; the rest of the software leverages preexisting objects and modules born in the commercial IoT sector. Thus, is this wave of data really all the same ocean from a storage and software standpoint? In other words, because of modular programming and reuse, are commercial IoT flaws present in often-unpatched IIoT systems?[3]

---

[2] For a description of safety critical system standards with system architectures, review the "Kenexis Fire and Gas Systems Engineering Handbook." The book calls out architectures and standards for process control equipment (like IIoT), including ISA84, IEC 61511, and IEC 61508.

[3] Once a vulnerability in the commercial space (IoT) is known to the hacker community, hackers can easily develop exploits and payloads that leverage the same vulnerability in unpatched IIoT systems.

Integration of IoT devices into a SCADA/DCS/ICS control system world will lead to required changes to the decades old ISA95 Purdue Model or the related ISA88 factory automation network architecture. Such statements simply follow the facts that IP-addressable devices—such as most, but not all, IoT devices and systems—integrated into network-centric architectures logically lead to a change in the deployment fabric. An illustrative architecture is presented in Figure 7. What is most noteworthy of such an IoT architecture—data fabric—is that it follows an IT-centric network architecture, thereby allowing for standard IT cybersecurity tools to be suggested for use.



Source: Deloitte's IoT Reference Architecture.

Graphic: Deloitte University Press | DUPress.com

Figure 7. A example of multifunction IoT architecture.

The network architecture shown in Figure 11 is not being promoted by the authors as a possible replacement for current SCADA/DCS/ICS architectures. It is provided simply as an illustration of an ~~intergrated~~integrated and collaborative II~~i~~oT architecture.

The Industrial Internet Consortium—like many similar groups—has developed a conceptual architecture that presents one "view" of IIoT, shown in Figure 8.

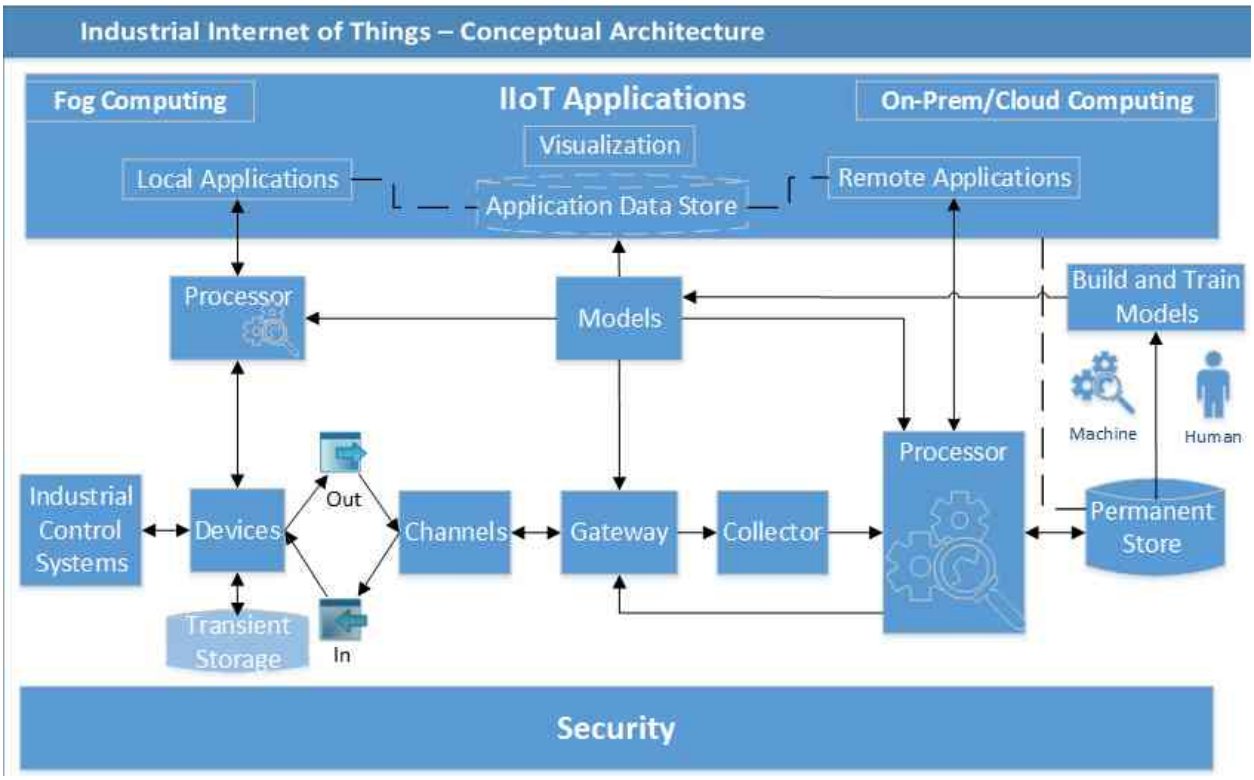


Figure 8. An example of ~~C~~conceptual IIoT architecture. (Source: http://www.infosysblogs.com/bigdata/2016/07/industrial_internet_of_things_.html)

Again, where do standards come into play? Maciej Kranz states "The IoT World Forum has been working on a common model to drive interoperability across all IoT components: devices and controllers, networks, edge computing, data storage, applications, and analytics. The IoT World Forum Reference Model organizes these components into layers and provides a graphical representation of IoT and all that it entails." Kranz concludes with this bold statement: "The IoT World Forum Reference Model opens the door to an 'Open IoT' system, with guaranteed interoperability."[4] The reference model is presented in Figure 9 (Kranz 2015).

[4] Readers who are knowledgeable and/or participated in the ISA SP95 and SP100 development processes can attest to the difficulty of achieving simply stated goals such as "guaranteed interoperability."

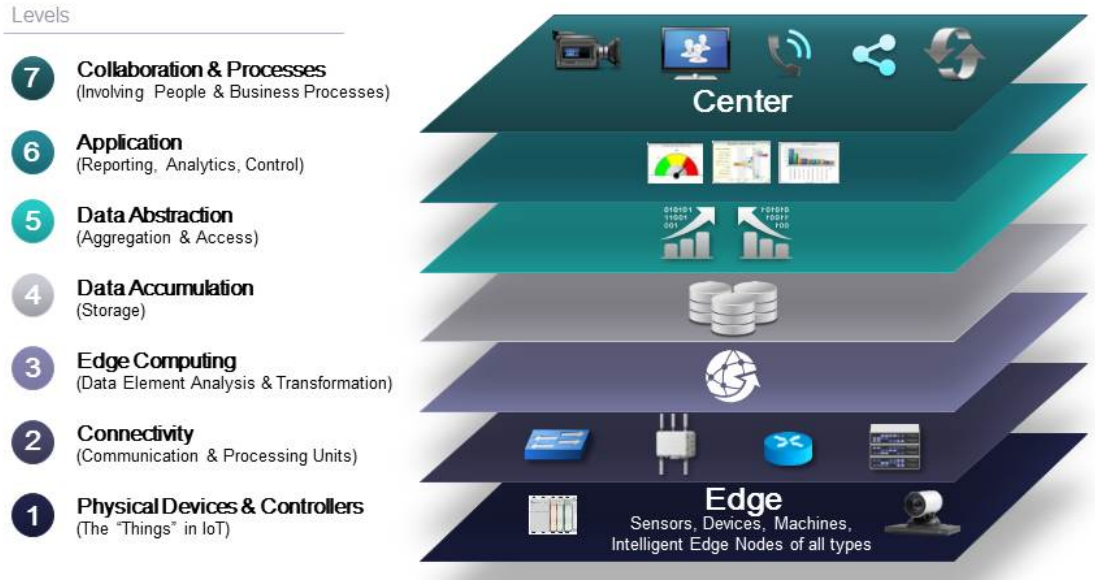


Figure 9. A example of ~~C~~conceptual IIoT architecture. (Source: IoT World Forum Architecture Committee, 2015, http://www.infosysblogs.com/bigdata/2016/07/industrial_internet_of_things_.html)

Cybersecurity, IoT, and the Attack Surface

The introduction of IoT devices, in particular IP-addressable devices, into an industrial setting most assuredly increases the number of elements/devices that may be vulnerable to cyberattack. The situation was illustrated in the December 2016 distributed denial of service (DDOS) cyberattack attributed to IoT devices first being infected with malware, then being coordinated in the DDOS attack on major Internet routers.

Does this warrant avoidance of IoT device use in an industrial setting? As directors and directors-elect of two of ISA's technical divisions, the authors of this paper answer that question with a resounding "No." However, such cybersecurity instances do illustrate the need for a change from the decades-old defense-in-depth SP99 model. In a future article, we will present a bold design for a cybersecure network architecture appropriate for 2017 and beyond.

Conclusions

Lower costs, enhanced features, and higher cyber risks—these are what we can expect as IoT and IIoT converge. Standards and guidelines can help carve an orderly path forward. A path for IoT in industry will be needed because infrastructure initiatives will likely invite rapid IIoT deployment.

ISA's Communications Division and Test & Measurement Division currently have a joint working group focused on IIoT with the associated examination of functional and operational security if/when IoT devices are deployed into a control system. Although the term "cyber" is often

overused, it truly applies in the world of IIoT; however, new sensor and control capabilities bring enhanced attack surfaces in the world of cyber.

In follow-on papers in this series, the authors will discuss cyber implications for our overall critical infrastructure and drones for remote inspection to uphold cyber assurance.

References

"Where the Smart Is." *The Economist*, http://www.economist.com/news/business/21700380-connected-homes-will-take-longer-materialise-expected-where-smart, June 11, 2016.

Hillar, Gaston C. *Internet of Things with Python*. Packt Publishing Ltd, 2016.

Kranz, Maciej. "IoT Meets Standards, Driving Interoperability and Adoption," http://blogs.cisco.com/digital/iot-meets-standards-driving-interoperability-and-adoption, July 21, 2015.

Puri, Ketan. "Industrial Internet of Things (IIoT)—Conceptual Architecture," http://www.infosysblogs.com/bigdata/2016/07/industrial_internet_of_things_.html, July 13, 2016.

Rossman, John. *The Amazon Way on IoT: 10 Principles for Every Leader from the World's Leading Internet of Things Strategies*. Clyde Hill Publishing, 2016.

Sexton, D., "Deterministic Ethernet for Industrial Internet of Things," ISA Communication Division Symposium, Washington DC, May 2014.

Smith, Sean. *The Internet of Risky Things*. O'Reilly Media, 2017.

Note: An expanded version of this paper is available on the ISA Communication Division and ISA Test and Measurement Division websites.