Industrial Networking Enabling IIoT Communication

An Industrial Internet Consortium White Paper

IIC:WHT:IN23:V1.0:PB:20180829

David Zhe Lou, Huawei Technologies

Jan Holler, Ericsson

Cliff Whitehead, Rockwell Automation

Sari Germanos, B&R

Michael Hilgner, TE Connectivity

Wei Qiu, Huawei Technologies

The internet has redefined a number of consumer-oriented businesses such as media, travel, retail and finance. It is now redefining industries like energy, manufacturing, transportation and healthcare. This new wave is the Industrial Internet of Things (IIoT): an internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes. [1]

The foundation of IIoT is how the industrial assets (the things, machines, sites and environments) can be connected to business professionals and processes. By 2023, one forecast calls for 20 billion connected devices [2] instrumented with sensors, actuators and embedded computing capabilities. The network is the important infrastructure that supports different application requirements and different deployment situations in the vast range of industry sectors and associated industry-specific applications affected by IIoT.[3]

Industrial networking is a collection of technologies at the Internet Protocol (IP) layer and below that enable the transformation of industries. There are many choices in technologies, both existing and emerging. What are the networking needs, what applications to support on the industrial network, and what is the deployment situation and conditions? These are key questions to answer when defining a strategy for technology selection and reaching a concrete deployment solution.

ENABLING IIOT COMMUNICATION

Industrial networking is different from networking for the enterprise or networking for consumers. First there is the convergence of Information Technology (IT) [4] and Operational Technology (OT). Important networking considerations include whether to use wired or wireless, how to support mobility (e.g. vehicles, equipment, robots and workers) and how to reconfigure components. Other factors include the lifecycle of the deployments, physical environmental conditions such as those found in mining and agriculture and electromagnetic conditions where interference from machines and equipment can be a problem. Then we have power. Will it be available? Or will devices need to run on local power such as batteries?

Second there are the technical requirements. They include network latency and jitter, throughput needs, reliability and availability. The requirements can vary from being relaxed to highly

[1] Industrial Internet Consortium *Industrial Internet Vocabulary, Version* 1.0, May 7, 2015.

[2] Ericsson Mobility Report, *https://www.ericsson.com/en/mobility-report*, June 2018.

[3] The Internet of Things: Mapping the Value Beyond the Hype, McKinsey Global Institute June 2015.

[4] Information Technology (IT) and Information and Communication Technology (ICT) are often used interchangeably. Here, we use “IT” to accentuate the industrial trend of IT/OT convergence.

demanding. The network must meet the end-to-end performance requirements for applications deployed both at the edge and in the cloud. Service Level Agreements (SLAs) must suit the industrial application's requirements, which are very different for utility smart metering, agriculture monitoring sensors or the remote operation of a mining drill rig requiring stereoscopic high-quality video feeds and haptic feedback for control.

This white paper sets the stage for a forthcoming publication, the Industrial Internet Networking Framework (IINF), which will complement the Industrial Internet Connectivity Framework[5] by detailing requirements assessing available technologies and providing best practices for how to achieve appropriate IIoT networking solutions.

It introduces a few typical industrial scenarios followed by their impact on networking. The scenarios show that there is no universal or preferred networking technology for IIoT systems and that diverse requirements must be considered when selecting an appropriate solution.

The derived networking requirements lead to the diversity of design considerations, which provides introductory guidance to IIoT solution architects and industrial networking engineers to help them make the right choices.

We then briefly introduce an upcoming publication, the IINF, that is intended to be used to select the appropriate solution.

Future IIoT Scenarios and Their Dependence on Networking

Productivity and profitability depend on keeping the operation running. For example, to maintain the highest level of production in manufacturing, machine maintenance needs to take place during scheduled downtime. This is best when machines can predict when and where faults are about to happen so they can be serviced then. This collected data needs to be communicated across industrial networks for analysis and can also be used for machine learning and for conducting business intelligence.

Inventory control systems also use industrial networks to maintain efficiency and increase inventory throughput. Machine interoperability and network interoperability standards create environments that easily allow industrial operations to be commissioned, managed and integrated into business processes.

Industrial networks improve productivity and performance by communicating essential operational data. For example, condition monitoring and energy monitoring collect data from every piece of equipment in the operation that can be used to create profiles for every piece of equipment, such as power usage across an equipment cycle and vibration profiles during normal operation. This data is often transmitted to the cloud for analysis and, when compared to

[5] The Industrial Internet of Things Volume G5: Connectivity Framework, *www.iiconsortium.org/IICF*

previous profiles, can contribute to predictive decisions about when to service the equipment, thus pre-empting equipment failure during production.

There are many more emerging scenarios that affect these layers and that need to be supported. We offer several examples here. They are not intended to be comprehensive.

Scenario #1: Elastic Virtual Industrial Control

Traditional industrial processes comprise distributed subsystems controlled by discrete industrial controllers, typically a Programmable Logic Controller (PLC). Future production systems will need to meet fast-growing market demands by providing agile and flexible production processes that achieve competitive production costs through deployment of scalable automation systems. However, the addition of each new PLC brings with it additional costs and maintenance, and because each PLC offers constrained control resources, the hardware PLC function is not elastic. “PLC-as-a-service” at the edge or within a cloud could meet the scalable automation requirements of business.

A deterministic network is imperative for many industrial communication applications, so a challenge facing “PLC-as-a-service” or “control-as-a-service” is how to ensure deterministic communication from the edge or cloud to the field devices. Emerging standards for time-sensitive networking (TSN) and deterministic Ethernet help address these timing requirements.

The network can be divided into four parts as shown in Figure 1.

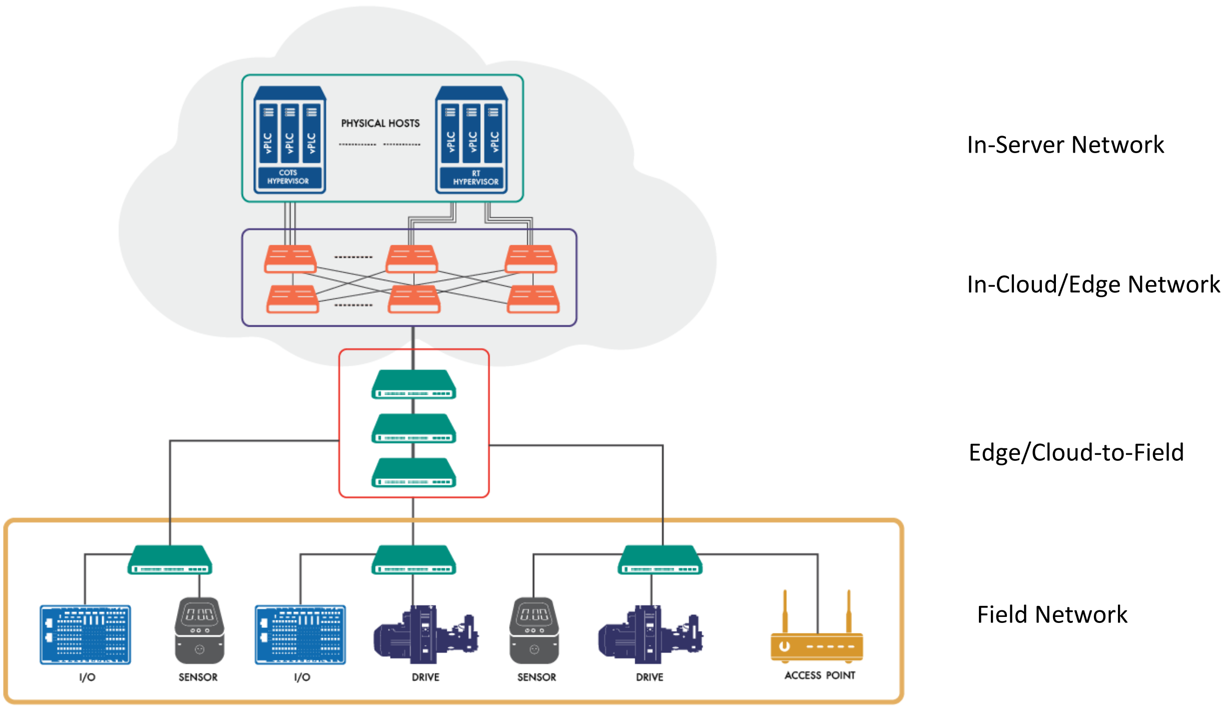

Figure 1: Network Architecture for Edge or Cloud PLC

In-server network denotes the internal data bus of the server. A hypervisor is required to guarantee deterministic performance for each virtualized PLC.

In-edge/cloud network should guarantee the required latency and jitter between layers and lossless networks.

Edge/cloud-to-field network is typically across the WAN and should guarantee the quality of service from layer 3 and above. Deterministic IP or deterministic networking technologies should be applied here to support industrial communication.

Field network refers to an in-plant network. Typically edge nodes will be deployed in the plant to realize the most time-critical (<1ms) control functions.

SCENARIO #2: PROCESS IMPROVEMENT FOR PRODUCTION

Manufacturing and processing operations undergo improvement or optimization programs throughout the lifecycle of the products being made. The trend is for process improvements to be performed more frequently and in some cases nearly continuously. To achieve more frequent process improvement, more and more IIoT sensors are being added to the operations.

For example, the United States Food and Drug Administration has provided guidance for manufacturers to adopt a risk-based approach to meeting product quality and regulatory requirements through the use of Process Analytic Technology (PAT).[6] A core tenet of PAT is continuous inline monitoring of the process that transforms the raw materials into end products. This monitoring technique requires more instruments and sensors for the process and the new sensors will require industrial networks to communicate with the control systems.

Because most industrial operations have been in place for a long time, new sensors need to be retrofitted onto existing infrastructure and machinery, which can be done efficiently with wireless communication technologies. Wireless mesh networks using technologies such as IEEE 802.15.4 and Bluetooth LE mesh will provide the edge connectivity to the new sensors. Wired sensors will continue to be relevant and may migrate from dedicated fieldbus technologies to variants of industrial Ethernet including single-pair Ethernet networks.

SCENARIO #3: THE REMOTELY OPERATED MINE

The mining industry has shown great interest in wireless solutions and has been working with wireless remote control and electrification of vehicles for over two decades. There are strong drivers for increased efficiency and improved safety using fewer people with a high degree of

[6] "Guidance for Industry: PAT: A Framework for Innovative Pharmaceutical Development, Manufacturing, and Quality Assurance", U.S. Department of Health and Human Services, Food and Drug Administration, Center for Drug Evaluation and Research (CDER), Center for Veterinary Medicine (CVM), Office of Regulatory Affairs (ORA), Pharmaceutical CGMPs (September 2004)

automation and remotely controlled machinery and vehicles. In some cases, the mines are at such depths that having personnel at the front is not realistic, practical or even legal. Another strong driver for the mines is to run an operation that is as environmentally neutral as possible.

The communication solution for remotely controlled machines is based on unlicensed spectrum and in some cases proprietary technology. For some applications, these solutions are sufficient, but miners request more standardized and integrated solutions because adding a machine often requires adding network infrastructure. Network coverage where mobile vehicles and equipment operate must also be contiguous to ensure seamless handoff of communication from one coverage area to the next, but still be cost-efficient, which requires the appropriate network planning.

A remotely operated machine or highly mobile vehicle may need six to eight high-resolution cameras for simultaneous video feedback, combined with light detection and ranging (LIDAR) information, haptic feedback and general machine telemetry and instrumentation. A large number of sensors gives a distributed view of the ore body and mine environment and the data must be analyzed in near-real-time. In the future, a number of such machines must coexist with other mine services to accommodate sensors for presence, air quality, seismic sensing, etc. All must be delivered in real-time and meet ultra-high reliability requirements.

High availability and reliability of the communication network is top priority to enable closed-loop automation. Remote control feedback could require as much as 100Mbps per machine in the uplink from vehicle or machine up to the network. The margins due to real-time and availability would be substantial, so 10Mbps on average, per machine, would not suffice. End-to-end latency for a well-working remote control could likely be tolerated at around 200ms, but today's cameras have capturing and coding delays using a large portion of that budget. Potentially, less compression could be used, but at the cost of higher bandwidth needs. Availability requirements, with a closed automation-loop, could be in the order of 0.99999, which corresponds to an annual outage of slightly over five minutes.

SCENARIO #4: IN-VEHICLE CONNECTIVITY

Automobiles deploy sensors and actuators that require effective and resilient communication in potentially harsh environments. Many of the sensors and actuators in these applications also have constrained resources (processing capability, memory, power and size) that place restrictions on the networking elements of device connectivity. While wireless networks are able to satisfy the needs of many devices in these applications, wired networks will continue to play a significant role. The single-pair Ethernet (SPE) work in IEEE is an attractive solution for automotive in-vehicle use.

In-vehicle automation applications require the high performance of Ethernet, high reliability and resiliency in challenging environmental conditions and low weight to help auto makers achieve their goals for fuel efficiency. In 2011, the One-Pair Ethernet (OPEN) Alliance special interest group was founded to “drive wide scale adoption of Ethernet-based automotive connectivity”.[7]

SCENARIO #5: SMART GRID APPLICATIONS

Utilities currently use multiple communication solutions to manage and operate their business. Communication solutions employed by a typical utility in the United States include:

- *Land Mobile Radio* (LMR) for field crew communication,
- *Wi-Fi/cellular/satellite* for Mobile Workforce computers,
- *PowerLine carriers* or *RF-mesh/Wi-Fi/cellular* for Metering (AMI),
- *RF-mesh/microwave/cellular/satellite* for Distribution Automation and Transmission Automation and
- *Microwave/fiber/leased T1s* for Substation Automation, Power Plants, Corporate Headquarters and field offices.

Since the beginning of electrification, stakeholders’ roles in the electric grid were fixed and power flowed in one direction. Distributed energy resources, plug-in electric vehicles, battery storage and smart connected appliances are now disrupting that pattern. Production, storage and consumption involve large numbers of distributed devices with power flowing in different directions. To use these technologies, coordination between the different elements of the networks is required, which drives the need for advanced wide-area networking solutions such as low-latency wireless networks on licensed spectrum with priority access. *Figure* 2 shows key stakeholders in the Smart Grid and the diversity of communication paths.

[7] http://www.opensig.org/download/datasets/1375/Broadcom_NXP_Freescale.pdf

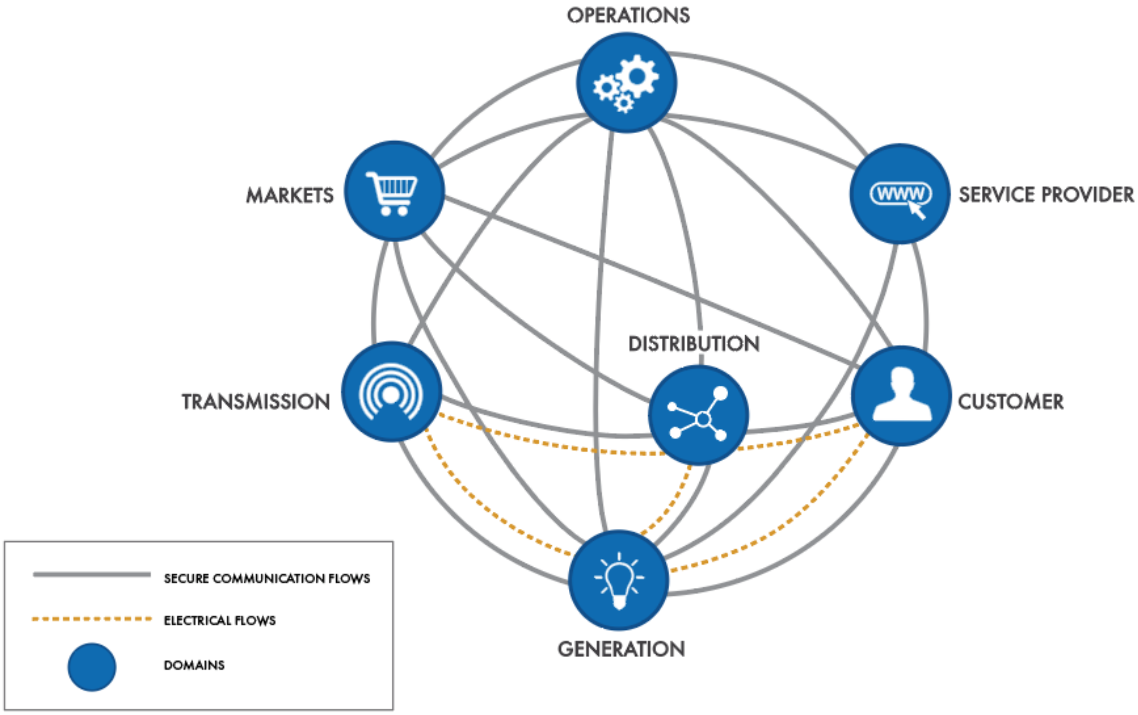

Figure 2: Key Smart Grid Stakeholders

The communication needs of each actor vary significantly, resulting in the need for multiple networking layer technologies to meet the requirements. The evolution towards a true Smart Grid will require edge intelligence and distributed control. The historical load information will be combined with probabilistic forecasting for automated intelligent analysis. This information needs to be communicated to all stakeholders in real time.

Scenario #6: Smart Logistics

Logistics is the process of optimizing the flow and storage of things between endpoints, such as producers and consumers, by reducing resource usage like transportation fuel and storage space, optimizing stock levels and minimizing unnecessary waste of product. Optimization is also about timely delivery, so a capability to "track and trace" things by requiring identification and positioning using, for example, RFID tags combined with detected network presence. We can then monitor the things throughout the logistics process end-to-end. Products can be perishable (e.g., food), fragile (e.g., fine art) or need to be secured against tampering (e.g., pharmaceuticals). This means that different types of goods need appropriate monitoring (e.g., temperature, humidity, vibration, shock and tampering) and logging (e.g., who, when and where) across the logistics flow. The handling must be individually adapted according to the need of each product, whether performed manually or by machines.

Logistics is global and multimodal involving different means of transportation, mainly shipping, road, rail and air through many distribution points at ports, airports and hubs. To ensure the appropriate tracking, monitoring and handling of goods, the logistics flow must be connected end-to-end. At the highest level, this requires using diverse wide-area networking capabilities such as cellular networks and satellite connectivity together during long haul transportation, and cellular connectivity and Wi-Fi in combination for logistics hubs.

As goods can be monitored individually, connectivity will be tiered to address the context of the item being monitored. For example, ships can contain tens of thousands of containers, each being monitored individually, and each carrying separate pallets of different goods and each pallet containing many individual items. Monitoring will take place at the different levels of containers, pallets and individual items, and networking will require different technologies at each of these different tiers. In this example, networking gateways provide local short-range connectivity inside the container for the goods and the necessary wide-area connectivity for the container. As containers are moved from ships to trucks or rails, necessary mobility support is required. Containers can have dual networking interfaces as well (e.g., Wi-Fi and cellular), thus requiring multi-access mobility. As goods are redistributed at ports and logistics hubs, automatic, authenticated and authorized network reconfiguration is required across the tiers. Connectivity still can be intermittent across the tiers so robust networking as well as local application processing closer to the edge is required to ensure the appropriate operations like aggregation of data, monitoring for improper handling and raising alarms.

Environmental conditions across the logistics flow are generally harsh, with extreme temperatures, humidity and even corrosive materials. Items must be monitored over long periods so the cost and energy consumption of sensor devices and networking are key considerations. We also require the right choice of radio technology, possibly including mesh network solutions, to handle, for example, the significant number of steel containers on a ship, each requiring a connection.

INDUSTRIAL NETWORKING REQUIREMENTS AND DESIGN CONSIDERATIONS

The scenarios described above show that IIoT applications could become more diverse, flexible, intelligent and efficient by taking advantage of novel networking technologies. The future of networking will require continuous improvement of reliability, security, deterministic transmission and management capabilities. To fulfill those requirements, various design considerations for IIoT networking need to be evaluated and they are summarized below.

Network architecture: Each vertical has different scenarios and network requirements. Some require reliable low latency communication, while others demand low power consumption or long-range wireless communication. Yet these different sectors must be able to communicate so a common network architecture with ubiquitous connectivity that connects sensor to cloud, interoperates among vendors and spans industries is essential. The network infrastructure, protocols and technologies applied to the industrial internet should be transparent to industrial applications and services to avoid frequent variation across various scenarios and verticals.

End-to-end and vertical integration: A traditional hierarchical approach of several levels (sensor, device, control and enterprise) often has each level using different network infrastructures and technologies. Gateways are required to bridge these networks. An end-to-end solution can flatten the hierarchy and support the convergence of IT, OT and the internet without the need for technology conversion such as interface type, switching and routing.

Flexibility: Mass customization in manufacturing has caused a dramatic shift in assembly plants. Modern assembly lines and logistics need to be flexible and agile to manage the required product variability without introducing waste or compromising quality. To support flexible manufacturing, the network should be able to self (re)configure dynamically.

Determinism: Many industrial scenarios require deterministic communication. Factory automation (e.g., motion control) demands deterministic ultralow latency transmission in the order of sub-milliseconds. For those scenarios, time-sensitive protocols and technologies with low jitter should be used to ensure applications' integrity and predictable system performance.

Technology lifecycle management: Network technology evolution has consistently followed a cycle similar to Moore's Law with frequent turnover of products and increases in performance. In contrast, OT systems comprise systems with longer life cycles, on average 19 years. This difference in development speed leads to slow adoption of new network technologies into existing OT deployments. Manufacturing subsystems should therefore be decoupled from the network devices while keeping a consistent interface between them.

Backwards compatibility and future-proof: New networking technologies should be interoperable with legacy networks to protect past investment and ease future developments.

Communication stack in end devices: To guarantee reliable, secure and deterministic industrial communication, sophisticated network methods, functions and protocols are required. Since many end devices are limited in resources and power, those limitations must be taken into account when designing the communication stack and physical layer hardware for them.

Trustworthiness: Trustworthiness[8] of an IIoT deployment requires security, safety, reliability, resilience and privacy. The industrial network should provide means and measures to enable and support trustworthiness from the network perspective.

Openness and standard: The infrastructure, protocols and technologies used in the industrial networking system should be open and standardized to allow for maximum interoperability and to promote wide cooperation among industrial partners.

[8] The Industrial Internet of Things, Volume G4: Security Framework, *www.iiconsortium.org/IISF*

Licensed and unlicensed spectrum: Due to reliability, coverage and regulatory tradeoffs, the effect of using licensed or unlicensed spectrum must be considered when designing industrial application with wireless communication.

Power consumption: The communication design should consider power consumption.

Coverage: Coverage includes the area to be covered, the number of communication endpoints that need to be supported and bandwidth requirements. Range and reach should include planning for required distances, line of sight and radio propagation properties in the targeted environment.

Mobility: Different levels of mobility include whether support is needed on a global, regional or local level. Local can imply even at the site or sub-site level. Characteristics of mobility include how frequently mobility occurs, how fast the mobile object is moving and requirements on needed bandwidth and latency while mobile.

STANDARD AND TECHNOLOGIES LANDSCAPE

INDUSTRIAL INTERNET NETWORKING COMMUNICATION STACK MODEL

The hourglass model of the internet protocol stack as shown in Figure 3 is well known. The hourglass waist is at the (inter)networking layer where the IP resides. The Industrial Internet Connectivity Framework enriched this model in the layers above the Networking Layer. In both models, the lowest layer is the physical layer, which defines the physical and technical properties of the transmission medium and regulates the relationship between the network hardware and the physical transmission medium. Above it is the link layer, which is responsible for the interaction of multiple network components to ensure a reliable and deterministic transmission between network nodes. Above the link layer is the network layer that provides the functional and procedural means to enable the transfer of data sequences of variable lengths (data packets) from a transmitter to a receiver over one or more networks.

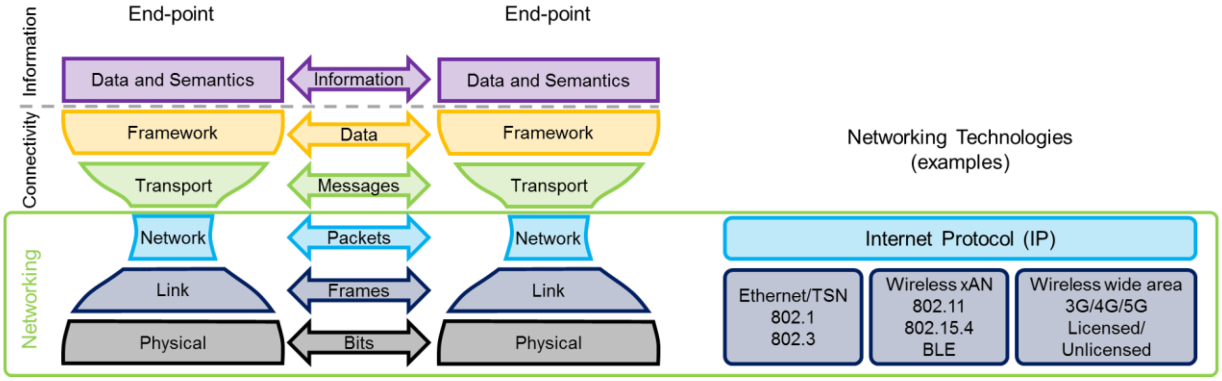

Figure 3: Networking in the Industrial Internet Communication Stack

Networking technologies are plentiful. Whether they are open standards, general or specific to an industry, their features and capabilities evolve continuously. They can be both wired and wireless, where the latter can operate in both licensed and unlicensed spectrum. Prominent examples include standards from the IEEE family of networking protocols, like 802.3 Ethernet, 802.1 Time Sensitive Networking (TSN), and different versions of 802.11 and 802.15.4. There is Bluetooth Low-Energy (BLE), and an evolving set of cellular technologies developed by 3GPP, including 3G, 4G LTE with NB-IoT and Cat-M1 targeting low cost massive sensor deployments. The emerging 5G standards with New Radio (NR) are targeting new capabilities such as vehicle-to-everything and Ultra Reliable Low Latency Communication for industrial use cases. And there are industrial communication buses standardized by IEC, such as PROFINET and Modbus®.

Figure 4 provides an overview of prominent industrial networking standards, technologies and Standards Development Organizations (SDOs) for the network, link and physical layers. It is not an exhaustive list of relevant standards.

Industrial networking standards can be technology standards, system and product standards or application-specific standards.

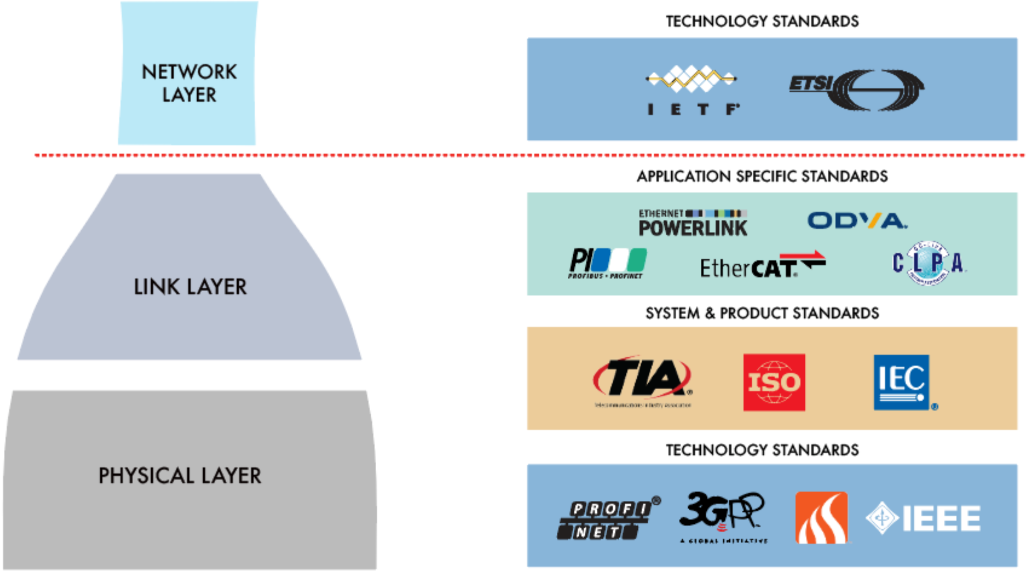

Figure 4: Standards and Technologies

For the network layer, the standards are predominantly technology based. The well-known internet protocol suites, IPv4 and IPv6, are defined by the Internet Engineering Task Force (IETF). Besides, there are also some ongoing research and innovation initiatives (from EU FP7, ETSI NGP, e.g.) aiming to promote innovation on the network layer.

Traditional industrial Ethernet link layer technologies that are considered application-specific standards include PROFINET (defined in PROFIBUS and PROFINET International (PI)), EtherNet/IP (defined in ODVA), POWERLINK (defined in Ethernet POWERLINK Standard Group), EtherCAT (defined in EtherCAT Technology Group) and CC-Link IE (defined in CC-Link Partner Association [CLPA]). Standard Ethernet, which is defined in IEEE 802.1/802.3, is the first choice on which to build the converged industrial network due to its broad acceptance and the Time-Sensitive Networking (TSN) technologies that are based on it.

In the wired network, the physical layer technologies are defined in different levels of detail by different standards development organizations. For example, IEEE 802.3, ISO/IEC JTC 1/SC 25/WG 3 and TIA TR-42, PROFIBUS and PROFINET International (PI), ODVA, CLPA and others define cabling requirements.

The wireless network can be divided into licensed network and unlicensed network. The IEEE and the MulteFire Alliance develop technologies based on unlicensed spectrum while the 3rd Generation Partnership Project (3GPP) focuses on licensed spectrum.

IEEE and other standards organizations such as Bluetooth Special Interest Group (Bluetooth SIG) develop and define standards for various wireless networks. IEEE 802.11 is a family of specifications for wireless local area networks (WLANs). IEEE 802.15 focuses on the Personal Area Networks (PAN) that are used to connect end devices such as PCs, cell phones, consumer electronics and industrial instruments. The Bluetooth SIG oversees the development of Bluetooth new technologies and standards, one example of which is the recently released specification of mesh networking operating on Low Energy (LE) devices.

The MulteFire Alliance is an independent, diverse and international member-driven consortium defining and promoting MulteFire, an LTE-based technology for small cells operating standalone in unlicensed and shared spectrum. Many IoT technologies are currently being discussed in MulteFire.

The 3rd Generation Partnership Project (3GPP) Standardization covers licensed cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities. 3GPP standards are structured as *releases*. Different generation technologies such as 2G, 3G, 4G and 5G can refer to the functionality in different releases. In 3GPP Release 13, enhanced machine-type communication (eMTC) and narrowband Internet of Things (NB-IoT) technologies are targeted to provide solutions for IIoT communication of lower complexity and power, deeper coverage, and higher device density. In contrast, the first 5G New Radio (NR) release delivers enhanced mobile broadband (eMBB) and ultra-reliable, low-latency communication (URLLC), which can address high-performance IIoT use cases.

In addition, there are many emerging network technologies currently being discussed or developed in the industry. Technologies such as Network Slicing (part of 5G), Software Defined Networking (SDN), Network Function Virtualization (NFV) and Low Power Wide Area Network (LPWAN) may provide better or different support for industrial applications.

Industrial Internet Networking Framework (IINF) Overview

IIoT connects industrial machines and devices to enterprise information systems and business processes to achieve higher productivity. With tighter integration of automation and information, IIoT concepts will evolve from intelligent products and intelligent services to cloud-based control services, which demand network support with novel technologies and protocols. Industrial networking and IIoT are complementary. Evolution of IIoT demands novel network infrastructure and advanced networking technologies enable a deeper industrial revolution, as shown in Figure 5. For example, intelligent production demands a converged network infrastructure with open standardized technologies to break the hierarchical and isolated automation pyramid. Cloud-based control services require an IP-based deterministic large-area network with flexible network configuration to support reliable and secure industrial communication from the cloud to the field.

Meanwhile, the underlying network technology is also improving to support IIoT concepts. From fieldbus to industrial Ethernet, from proprietary technologies to open standards, the evolution of network technologies improves productivity and increases the interoperability of communication.

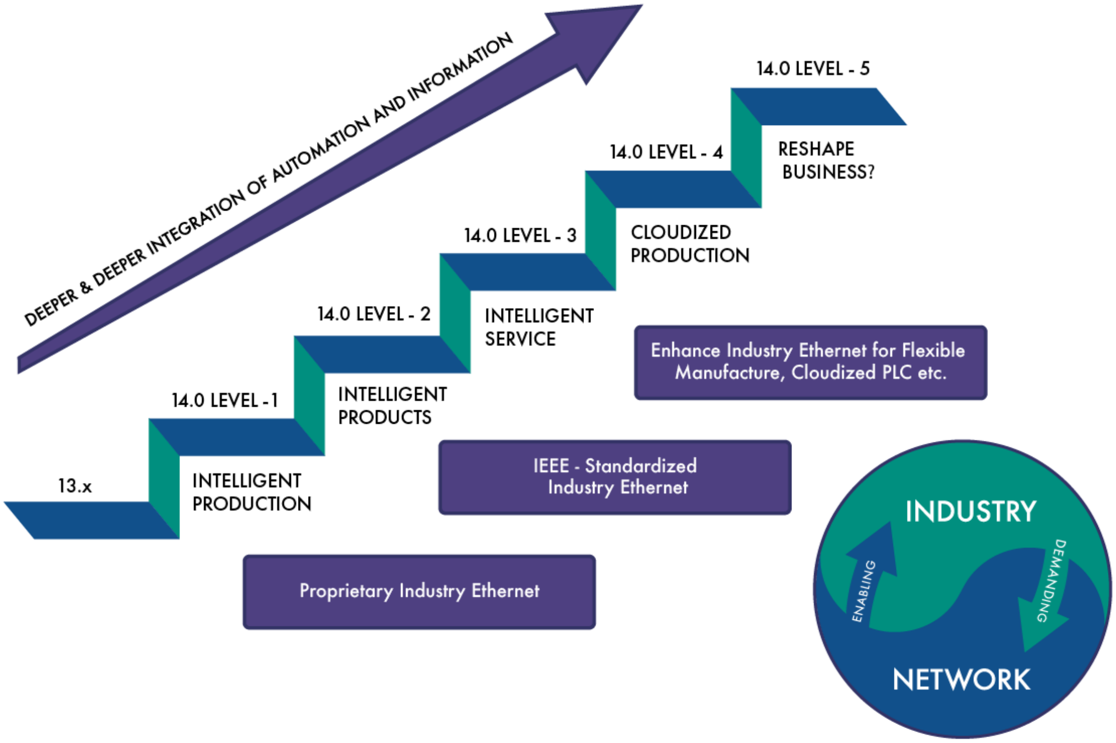

Figure 5: The Yin-Yang Model of Industrial Networking and IIoT

A TOOLBOX OF METHODS AND GUIDANCE

One of the key objectives of the IINF is to create a *conceptual toolbox* that provides guidance and recommendations for suitable network infrastructure and technologies for various industrial scenarios. The toolbox as shown in *Figure 6*6 comprises three conceptual steps: a network requirements analysis, network architecture creation and technology mapping. The first step involves analyzing industrial scenarios and deriving network requirements, which will be used in the next step. The second step aims at providing tools for creating a network architecture for the input scenario by applying design considerations onto the derived requirements. By consolidating various industrial network architectures, another goal is to develop industrial networking reference model(s) or blueprints for various verticals. The third step is the mapping of existing technologies onto the network architecture to output a recommended instantiation of the network architecture and relevant technologies. The last step will also identify technology gaps, which can be input to SDOs.

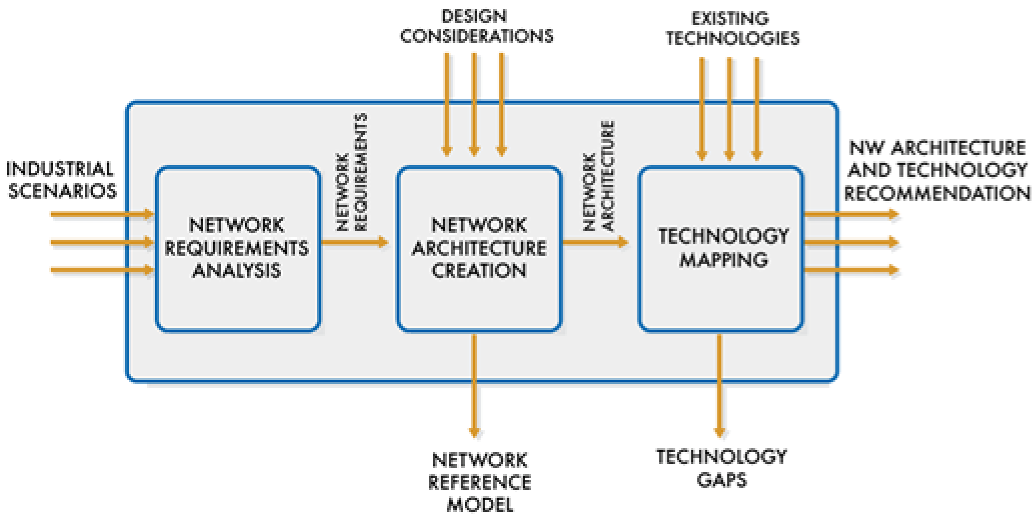

Figure 6: Toolbox of Methods and Guidance

CONCLUSION

This white paper sets the stage for a forthcoming publication, the Industrial Internet Networking Framework, which will complement the Industrial Internet Connectivity Framework by detailing requirements and best available technologies for the lower three layers of the Industrial Internet Communication Stack.

Because there is no universal or preferred networking technology for IIoT, we introduced the concept of the toolbox and methodology which will be elaborated in the forthcoming Industrial Internet Consortium (IIC) publication of an Industrial Internet Networking Framework.

The IINF will include requirements and solutions overviews as well as tools to support the process of deriving requirements from usage scenarios and selecting the appropriate technology. The IIC encourages all members and stakeholders to engage in the development and publication of the IINF.

AUTHORS AND LEGAL NOTICE

This document is a work product of the Industrial Internet Consortium Networking Task Group, co-chaired by David Zhe Lou (Huawei Technologies), Sari Germanos (B&R Automation) and Jan Holler (Ericsson).

Authors: The following persons contributed substantial written content to this document: David Zhe Lou (Huawei Technologies), Jan Holler (Ericsson), Clifford Whitehead (Rockwell Automation), Sari Germanos (B&R Automation), Michael Hilgner (TE Connectivity), and Wei Qiu (Huawei Technologies).

Technical Editor: Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Authors into an integrated document.