Enabling the Industrial Internet of Things

The world is being transformed as connected devices and equipment, embedded with sensors and software, communicate with one another and the cloud. The data generated by such intelligent technology can be analyzed to extract valuable information about the physical world, such as when an auto part is likely to fail, or how to make a wind turbine run more efficiently. Commonly referred to as the Internet of Things (IoT), this new reality is being driven by the falling cost of sensors, devices, compute and storage technology and the acceleration of cloud and Big Data analytics.

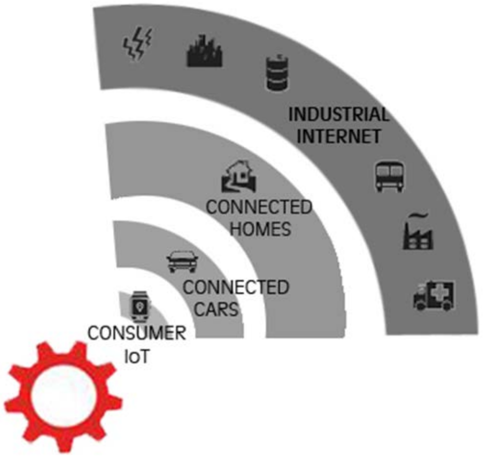
The IoT enables companies to harness and analyze real-world data in a way that wasn't possible before. "The Internet of Things will transform businesses and the way we live because it unleashes the capability to solve end user problems that businesses couldn't solve through traditional means," says David Formisano, Director of Internet of Things Strategy at Intel. "It attacks business problems such as how to save energy, time or money to be more efficient and compete more effectively in a global industry, or how to deliver new revenue-generating services that companies couldn't deliver before and their competition can't deliver today."

Industrial applications of the IoT: The last frontier

Much of the focus of the Internet of Things has been on consumer applications. This paper explores industrial applications of the IoT and their enormous potential to transform the business world. This emerging technology trend is referred to as the *Industrial Internet of Things (IIoT)*.

The IIoT connects devices and equipment in industrial environments, from security cameras and medical devices to farm and factory equipment. There are numerous potential applications, from improving patient care to minimizing unplanned factory downtime. "The Internet of Things will impact every industry on the planet, from consumer products to industrial manufacturing, says Rose Schooler," Vice President, Internet of Things Strategy at Intel. "It will serve as a catalyst to drive the next leap forward in productivity, giving industries the opportunity to innovate on both existing and new business models."

The economic potential is enormous. For instance, the McKinsey Global Institute projects that the IoT could make a global economic impact ranging from $2.7 to $6.2 trillion annually by 2025.[1] And GE estimates that, over the next two decades, the IIoT could add $10-15 trillion to global GDP.[2]



THE INTERNET OF THINGS LANDSCAPE

The security challenge

Companies have been slow to embrace the Industrial Internet, despite its vast potential, because of the risks involved. "The Industrial Internet addresses critical infrastructure in a way that we've never had to address it before," says Jeff Fedders, IoT Standards Chief Strategist at Intel. "Connecting the industrial landscape to the Internet has been almost prohibitive because of security concerns."

Industrial Internet applications expose networks that once were isolated to the risk of being attacked from unexpected sources inside and outside the firewall, whether intentional or not. Consider predictive

[1] "Disruptive Technologies: Advances that will transform life, business, and the global economy," McKinsey Global Institute, May 2013. http://www.mckinsey.com/insights/business_technology/disruptive_technologies

[2] "Industrial Internet: Pushing the Boundaries of Minds and Machines," GE Corp., Nov. 2012. http://www.ge.com/docs/chapters/Industrial_Internet.pdf

maintenance, an Industrial Internet application that enables companies to detect and address equipment problems before they occur. “Predictive maintenance is a powerful innovation that will improve the reliability of equipment and save costs, and perhaps lives,” says Sven Schrecker, Chief Architect of IoT Security Solutions at Intel. “But it requires access to some controls that traditionally have been ‘air gapped’ or separated from the outside world, so that analysts can pull off data points. Having that access is valuable, but it comes at a cost of potentially generating security issues.”

Predictive maintenance is just one example of how Industrial Internet applications create heightened security risk. Imagine the potential consequences of a security breach of a train, airplane, or dam or other critical infrastructure connected to the Internet, and the reason for companies’ reluctance to embrace this new technology trend becomes clear.

Industrial Internet: Potential performance gains in key sectors

The Industrial Internet presents opportunities across industries to generate major efficiency gains and cost reductions. Even a minor efficiency gain could produce major results. For instance, following is the estimated value of a 1% gain in efficiency over 15 years, for five global industry sectors:

- Aviation: $30 billion in fuel cost saving for commercial airlines
- Power: $66 billion fuel cost saving in gas powered fleets
- Healthcare: $63 billion in productivity improvement/reduction in system inefficiency
- Rail freight: $27 billion in cost savings due to reduction in system inefficiency
- Oil & gas: $90 billion reduction in capital expenses for exploration and development

Source: Peter C. Evans and Marco Annunziata, “Industrial Internet: Pushing the Boundaries (2012, Evans & Annuziata),” GE, November 2012. http://www.ge.com/docs/chapters/Industrial_Internet.pdf

The role of open standards

Open standards which are industry-led and open to participation by global stakeholders are essential to the advancement of the Industrial Internet. Voluntary global standards enable interoperability—the key to accelerating adoption, driving competition and innovation, and enabling cost-effective introduction of new technologies. “As we have seen in past technological revolutions—pc’s, data center, storage, and networking, to name a few—one of the key drivers that enabled rapid scale was the adoption of open standards-based platforms,” says Schooler. The support and adoption of IoT open standards is critical for the Industrial Internet of Things to scale rapidly across industries and the globe.”

Open standards will enable interoperability at all layers of the Industrial Internet architecture, from identity and security to hardware and software, making it possible for a broad range of companies throughout the supply chain to compete. “To enable healthy competition among suppliers, you need to ensure common interfaces and the ability to ‘plug and play,’ to create modular solutions,” says Fedders. Without open standards, there’s a possibility that the Industrial Internet could be dominated by a handful of vertical solutions controlled by relatively few companies.”

> *“As we have seen in past technological revolutions, one of the key drivers that enabled rapid scale was the adoption of open standards-based platforms. The adoption of IoT open standards is critical for the Industrial Internet of Things to scale rapidly across industries and the globe.”*
>
> \- Rose Schooler

Vice President, Internet of Things Strategy, Intel

IT and operations technology: A powerful combination

The Industrial Internet involves the merger of two worlds: information technology and operations technology. The implications of this marriage for industry are enormous, and fall into two categories:

New security and safety risks: Connecting the physical and virtual worlds creates new issues related to security and safety.

Security means ensuring that a system is protected from unintended or unauthorized access in order to prevent destructive operations. Industrial Internet applications increase security risks. For instance, the moment an actuator that opens the gate to a dam is connected to the Internet, there's the potential for a malicious actor to hack into the controls and release water downstream.

Safety is about minimizing the risk of physical damage or injury to people as a result of a business process. Safety is broader in scope than security; it addresses not just malicious threats but also natural factors (e.g., hurricanes, earthquakes, aging of equipment).

Industrial Internet applications can create new safety risks, even if the applications are secure. For instance, a secure self-driving car still poses a safety risk (e.g., of striking a pedestrian).

Threats to existing business models: In the merger of IT and operations technology, information can be the most valuable component. This makes the Industrial Internet a powerful force for disruption.

Uber illustrates the profound disruption that can result when the IT world moves into an operations technology environment—in this case, the taxi infrastructure. Uber's application of IT to the taxi industry upended the business model of the industry. The real value of Uber's business model lies in information sharing and connecting passengers to drivers, not in hard assets; anyone with a car potentially could be an Uber driver. Whenever information becomes the key component of a business solution that involves physical assets, we can expect to see more disruptions of traditional business models.

Advancing the Industrial Internet: Intel's role

Providing hardware and software tools

Intel is playing a key role in advancing the Industrial Internet. One important aspect of this role is the provision of hardware and software to support IoT applications. "The Industrial Internet requires key ingredients that are core to Intel's business," says Formisano. "It requires a massive amount of compute, from the data center through the network to connected devices. And it requires secure communication among devices. Intel has expertise in all of these areas."

In order to reach IoT scale and deployment velocity, Intel developed the Intel® IoT Platform, an end-to-end architecture based on horizontal and interoperable building blocks that functions as an IoT platform that can be deployed across industry sectors. Intel also offers hardware and software tools and support to developers, and a variety of venues in which to meet and collaborate, from online forums to IoT Roadshow events. "We have focused heavily on providing developers a comprehensive set of solutions that meet the needs of both the individual maker and the commercial developer," says Schooler.

To address the security concerns that have stalled adoption of Industrial Internet solutions, Intel provides hardware-assisted security integrated with software to provide world-class protection. This includes data protection and policy management to ensure that data can be trusted. Intel hardware and security software work together, making it easier to protect data and assets from theft, alteration, or tampering. These solutions are designed to automatically manage and monitor security threats to protect, detect, and correct against attacks.

Building an ecosystem

Hardware and software are essential, but advancing the Industrial Internet also requires an ecosystem of industry, government and academic partners working together. "It's challenging technically, so it requires industry-wide interoperability and cooperation," says Formisano. "And it's global challenge, so it needs an ecosystem that can scale."

Intel has a long legacy of enabling ecosystems that are founded around open standards. The company is now playing a key role in helping to build and scale a global ecosystem to advance the Industrial internet. "We have taken a leadership role in working with industry to drive key consortia and standards bodies in an effort to accelerate IoT deployments worldwide," says Schooler. We have also increased our focus on enabling our existing ecosystem and expanding it to include new partners to address the changing requirements of IoT and Industrial Internet solutions."

> *"The Industrial Internet is challenging technically, so it requires industry-wide interoperability and cooperation. And it's a global , so it needs an ecosystem that can scale."*
>
> - David Formisano
>   Director of Internet of Things Strategy, Intel

One initiative to expand the ecosystem was the creation of the Intel Internet of Things Solutions Alliance. This group of more than 400 member companies worldwide collaborates closely with Intel and each other to innovate using the latest IoT technologies, helping developers to be the first to market with solutions.

To further enable the ecosystem, Intel actively participates in a variety of industry alliances and standards bodies, and has co-founded two consortia to advance the IoT and its application to industry. The Open Interconnect Consortium (OIC) is defining the connectivity requirements and ensuring the interoperability of devices that will make up the IoT. The Industrial Internet Consortium^R (IIC), described below, is focused on advancing industrial applications of the IoT.

The Industrial Internet Consortium

The Industrial Internet Consortium was formed in March 2014 by AT&T, Cisco, GE, IBM and Intel to accelerate the growth of the Industrial Internet by addressing key obstacles to adoption, especially challenges related to interoperability and security. The consortium is a not-for-profit partnership of industry, government and academia. Members include small and large technology innovators, vertical market leaders, researchers, universities and governments. Membership is open to any public or private business, organization or entity with an interest in accelerating the Industrial Internet.

The IIC acts as a public-private community to advance innovation and best practices, providing insights and thought leadership. Member companies represent a wide range of capabilities, giving the consortium deep and broad expertise. “We have equipment vendors and manufacturers, system integrators, and owners and operators as well as cloud services, communications, edge, and hardware providers,” says Schrecker. “This enables us build a vision across specialties, and use the entire spectrum of capabilities across our membership to identify and address problem spaces and develop novel solutions.”

Key goals of the IIC

- Drive innovation by creating new industry use cases and testbeds for real-world applications
- Define and develop the reference architecture and frameworks required for interoperability
- Influence the global standards development process for Internet and industrial systems
- Facilitate open forums to share and exchange real-world ideas, practices, lessons and insights
- Build confidence around new and innovative approaches to security

Ensuring interoperability

The IIC is taking the lead in establishing interoperability across various industrial environments. “Our goal is to create an open, inclusive environment—to ensure that it’s possible to intermingle different vendors and services in a way that still provides the full set of service capability across the solution stack,” says Schrecker. “To do that, you need to marry the different layers--cloud services, communications, edge computing and hardware—to create stacks of capabilities that are integrated but which also allow you to plug different vendors into each layer.”

The IIC is focused on enabling interoperability across five vertical markets: energy and utilities, healthcare, manufacturing, the public sector and transportation. The consortium’s leaders are applying a top-down approach to achieve their goal—examining use cases, developing requirements, and building an architectural framework for the Industrial Internet.

Building global acceptance and momentum

While the IIC was founded by five US-based companies, from the start it was conceived and chartered as a global organization. The founders understood the need to leverage global standards to ensure interoperability of devices and equipment across countries and regions.

One early challenge was to create industry momentum and persuade key companies around the world to join the consortium. To demonstrate that the IIC is global in scope, the consortium’s leaders hired an experienced organization with global reach to manage the consortium and an executive director to work full-time on an outreach program. In addition, Intel contributed staff and engineering muscle, and assumed a leadership role on key committees that were focused on developing an architecture and security framework. “We immediately stepped up and chaired those positions,” says Fedders. “Intel is viewed by the IIC as a neutral player in the industry, so having Intel employees lead these committees alleviated the concerns of some members and prospects about the consortium’s neutrality. It reassured them that we wouldn’t favor one industry vertical over another. This helped in gaining buy-in and persuading companies to join.”

> *“Intel is viewed by the IIC as a neutral player in the industry, so having Intel employees lead key committees alleviated the concerns of some members and prospects about the consortium’s neutrality. This helped in gaining buy-in.”*
>
> - Jeff Fedders
>   IoT Standards Chief Strategist, Intel

Members of the IIC's Marketing Working Group also contributed to the brand building effort, traveling around the world to make presentations and engage in conversations with companies considering becoming members. As of October 2015, 225 companies, headquartered in 22 countries, had joined the IIC. With a solid foundation, and membership growing at a rate of three to five organizations weekly, the consortium has become a powerful collective voice for influencing the direction of the Industrial Internet of Things.

Integrating and advocating for open standards

The IIC is not a standards organization, but it is integrating existing open standards into its requirements, reference architecture and testbeds. “From the very beginning, we used existing standards to visualize and create a working model or reference architecture for the Industrial Internet,” says Fedders. “We're not out to create new standards, but through our working committees we're making what we think are the best choices among existing open standards.”

In addition to integrating open standards, the IIC is building relationships with other consortia and with key standards organizations and advocates for existing open standards and encourages the development of new standards required to support the evolving Industrial Internet. This includes standards related to data interoperability and analytics, device manageability, security, identity and privacy.

The IIoT in Action

Following are a few of the many case studies by IIC member companies that are harnessing the potential of the Industrial Internet of Things within their verticals. The IIC is focused on enabling interoperable solutions that cross verticals.

Communications The ***City of Nice, France*** installed a data connectivity platform and is now offering e-services such as smart parking guidance, traffic congestion management and information about city services. The city also introduced kiosks and smart phone apps as tools for citizens to interact.

The results? The city increased parking revenue 35% by reducing illegal parking; reduced congestion by 30%; and reduced air and noise pollution by 25% each. City leaders project future savings of as much as 80% in areas such as street lighting and waste management.

Energy *Envision Energy* sought to optimize the performance of its 20,000 wind turbines by enabling them to adjust rapidly to changing environmental factors (e.g., wind direction, temperature). The company also wanted to minimize turbine downtime through predictive maintenance. To achieve these goals, Envision installed an analytics platform to continously monitor 30 terabytes of real-time and historical data from the wind turbines, each with up to 150 sensors. The sensor data is used to alter the angle and speed of the turbine planes to optimize performance at any given time and to identify irregularities in performance, so the company can predict and address potential failures.

The analytics platform decreased downtime, and it increased productivity by an estimated 15% through performance optimization. The company projects that it will realize $150 million in annual savings as a result of the project.

Manufacturing When designing its new headquarters building, ***Del Papa Distributing*** wanted a single, secure network to ensure physical security, improve communications and collaboration among employees in different locations, and monitor inventory temperature. The company installed a solution that combines wired and wireless networks with video surveillance, physical access control, communications, teleconferencing and digital signs.

The new network prevents theft and provides better control over all entrances and restrictred areas. In addition, the system has boosted the daily shipping capacity in a 100,000 square foot facility by 6.4%, reduced travel time, and freed up reps for more customer interaction.

Transportation To boost capacity by increasing the speed and efficiency of its rail operations, ***Norfolk Southern Railroad*** installed a system that integrates railroad logistics with traffic control systems and develops an optimized traffic plan for the trains (including the optimal speed), considering factors such as train schedules, traffic-control systems and train movements relative to each other.

The system enabled more locomotives to run on the same track, at roughly 10% higher speeds. The solution is projected to reduce capital and expenses by up to $200 million annually. And by more precisely managing train schedules, the system also helps to optimize the use of railroad crews.

Overcoming obstacles to adoption

Through a variety of working groups, the IIC is tackling the biggest challenges facing the Industrial Internet, including interoperability, security, connectivity, and the development of viable business models. The working groups, comprised of representatives from IIC member companies and organizations, are coordinating and establishing the priorities and enabling technologies of the Industrial Internet in order to accelerate market adoption and lower the barriers to entry.

Three key working groups are focused on technology, security and testbeds.

Addressing technology requirements

The Technology Working Group is evaluating existing standards and identifying requirements for the Industrial Internet. The group coordinates the technical work required to build and enable the architecture, frameworks, standards and technologies for the Industrial Internet.

One of the key achievements of the Technology Working Group is the development of the Industrial Internet Reference Architecture (IIRA), released in June 2015. This document, which is based on open standards, provides a common language to describe the key system characteristics of Industrial Internet systems, including security, and the relationships between them. The IIRA will make it possible to create end-to-end solutions for the five verticals targeted by the consortium. “Think of the reference architecture as the blueprint for a building,” says Fedders. “The walls and rooms have been defined, and where interoperability is needed between rooms. We haven’t yet defined all the operations inside these rooms, and we haven’t done the plumbing and electrical, but the structure has been determined.”

The language in the IIRA helps developers to decide which elements they need for their systems, enabling faster delivery of implementations. The document helps to place existing and emerging standards into a common structure, making it easier to quickly identify gaps that need to be filled to ensure interoperability between components.

The IIRA can be downloaded free of charge from the IIC website.

Developing security solutions

One goal of the Security Working Group is to define a security framework to be applied to technology in general use in the industry. This is a complex challenge, in part because security must address the needs of a variety of players, including the equipment manufacturers and vendors that build products and equipment, systems integrators who implement and install the products and equipment, and the owners and operators who manage and monitor the products and equipment. Furthermore, security must encompass brownfield solutions for older equipment as well as greenfield solutions for new and emerging technology. The framework being developed by the Security Working Group addresses these challenges and more.

The IIC framework addresses the security risks around the marriage of IT and OT (operations technology), and it can be applied to existing and new technologies. It establishes best practices and can be used to identify security gaps in existing technologies. The document will help users to evaluate solutions and achieve improved security objectives for different classes of industrial activity, and to leverage novel technology to overcome existing and emerging security challenges.

The framework supplements information about security already in the IIRA, providing a richer level of detail regarding aspects of security most relevant to the Industrial Internet. This approach will ensure that security is not just bolted on to the architecture but rather is an integral component of it.

To strengthen security, the IIC security framework focuses on the interdependent system characteristics that must be considered in order to create a successful security design for an Industrial Internet system. The key characteristics are safety, reliability, resilience, privacy and security. These system characteristics are already being addressed in the industrial space, but typically each one is addressed in isolation. The IIC security framework describes how to consider the interactions among these characteristics when building systems, in order to choose the best security solutions.

Perhaps most importantly, the IIC security framework will enable users to assess the level of security of their systems during the design phase, so that needed changes can be made before implementation. This represents an improvement over the practice of assessing security only after systems are implemented.

In addition to developing a security framework for the Industrial Internet, the Security Working Group will provide guidance to the IIC's testbed teams for the implementation of more mature security solutions.

Testing to ensure that concepts work in the real world

Testbeds are a major focus of the IIC and its members. These platforms enable members to test potential Industrial Internet applications in a controlled environment that simulates real-world conditions. The IIC testbeds are where the innovation and opportunities of the Industrial Internet—new technologies, applications, products, services and processes—can be evaluated to determine their viability and usefulness before coming to market.

The Testbed Working Group is focused on accelerating the creation of testbeds. The group helps IIC members to define and gain approval for their testbeds; identify funding resources; and establish operational infrastructure.

> *"The testbeds are designed to demonstrate that a variety of use cases of the Industrial Internet will work in practice, not just in theory. I think that's a major differentiator between the IIC and other groups. We actually test our solutions to ensure they can be applied in the real world."*
>
> \- Sven Schrecker
> Chief Architect of IoT Security Solutions, Intel
> Co-chair, IIC Security Working Group

The IIC's testbeds leverage the IIRA and the key concepts espoused by the consortium (e.g., interoperability, scale, security). The use cases evaluated in the testbeds will help to determine the viability of business models.

The IIC is building a testbed-as-a-service (TaaS) operation and providing it to members as a proof of concept to demonstrate interoperability and security. Members can pay for the services they need instead of having to build a testbed infrastructure by themselves.

There are roughly 30 topics for which members can use the consortium's TaaS offering to test the viability of their business models. The topics focus on efficiency in five categories:

- Operations (e.g., production planning, inventory optimization)
- Maintenance (e.g., condition monitoring, predictive maintenance)
- Service (e.g., , materials management, supply chain analytics)
- Information (information modeling, machine-born data management and analytics)
- Energy (e.g., resource efficiency, safety performance).

The TaaS offering is attracting the interest of many organizations in joining the consortium, according to Fedders. "It's a way to monetize a large capital investment across many companies," he says. "Members can use our IoT framework, architecture platform, and investable assets to test their own business cases on top of it," says Fedders. The service will generate revenue to sustain the consortium while helping its members to develop new business ideas that leverage the Industrial Internet.

Testbed case study

Using predictive analytics to increase asset efficiency

One of the testbeds the IIC developed is being used to explore how predictive analytics can increase the efficiency of industrial assets. The project is a collaboration involving Infosys, PTC, GE and Intel.

The first phase of the project focused on predictive maintenance of a moving asset: aircraft landing gear. The project team collected real-time data from landing gear (sensor, geographic, event, time, and other system data) and focused on anomaly and fault detection, energy efficiency, asset utilization, system health, performance analytics, prognostics and holistic analytics. The data and analysis can be used to make better decisions about the operation, maintenance, overhaul and replacement of landing gear.

To generate their predictions, the team monitored a variety of parameters in flight (e.g., hydraulic pressure and electrical signals from weight-on-wheel switches) and on the ground (e.g., brake pressure and temperature and tire pressure.) They also tracked a range of diagnostics, from landing gear failing to retract/extend to binding of wheel bearings and brakes.

The key deliverable—a reference solution— was completed in August 2015 and demonstrated at the IoT Solutions World Congress in Barcelona in October. The solution is an end-to-end integration technology stack with a working prototype on an aircraft landing gear. Any IIC member can access this reference solution to test use cases involving other industrial assets.

The potential commercial benefits are significant. The ability to predict when maintenance is needed could reduce or eliminate unplanned downtime, ensure predictable delivery of service, reduce the cost of energy, labor and maintenance, enhance asset utilization and extend asset life—all of which will increase ROI.

The next phase of work

The publication of a reference architecture and development of testbeds were critical steps in advancing the Industrial Internet. Now the IIC is sharing the architecture, set of requirements, and use cases with other consortia and with global standards organizations.

"We want to share what we've developed with other organizations that share our goal of advancing the Industrial Internet," says Fedders. "The IIC has become recognized as a global sandbox where organizations can come to and apply our reference architecture to their space."

The next step is to integrate the security framework and ensure that it works cohesively with the reference architecture. The consortium's goal is to publish the security framework in the first half of 2016.

In parallel with finalizing the security framework, the consortium is building a data interoperability framework that will enable easy data exchange and analysis. This effort, which began early in 2015, will take roughly two years to complete and publish.

Many IIC members already have developed proprietary vertical solutions delivered over private networks. Fedders is hopeful that these companies will recognize the expanded opportunities that interoperability could deliver. "These companies have successful solutions, but they cannot fully monetize the rich data they collect because the data isn't stored in a standard format," he says. "They need interoperability if they're going to capitalize on more opportunities." Interoperability will also enable many companies to share costs rather than requiring each company to incur the expense of building its own solutions from the ground up.

The future of the Industrial Internet of Things

The IIC has made great strides since its founding in March 2014. By the end of 2015, the Industrial Internet Reference Architecture was contributing to the related IoT work of formal standards organizations such as the ISO/IEC JTC 1 Information technology standards organization and the Institute of Electrical and Electronics Engineers (IEEE). Through the development of a reference architecture, security framework and testbeds, the consortium has demonstrated that secure, interoperable IIoT solutions can be deployed in the real world.

The primary goal of the IIC over the next two years is to achieve scale. “It’s a huge challenge to build a globally interoperable ecosystem, because different regions and countries have different needs, security issues and regulations,” says Fedders. There are also logistical challenges of dealing with different regions, countries, languages and time zones.

To address those challenges, the IIC trying to grow the board and steering committee in a way which ensures that a broad range of viewpoints are represented. The consortium is also creating country teams, to consider alignment and synergies with related IoT initiatives supported by local governments and industries.

There are a number of regional efforts underway in which Intel participates. For instance, Intel is collaborating with local partners in China to ensure that IIoT solutions can work in that country, and is working with OEMs worldwide who have a pulse on different markets. “This is another way that we’re helping to scale the ecosystem globally,” says Formisano.

The future looks promising, as organizations around the world collaborate to advance the Industrial Internet. By offering key enabling technologies, supporting developers, and providing leadership through organizations such as the IIC, Intel is helping to build a strong interoperable global ecosystem to ensure that the Industrial Internet will realize its considerable potential.