Headwinds

The Industry IoT Consortium's (IIC) first quarter of 2022 member meeting was held virtually, March 8th ~ 10th. We had planned to go to Germany, but winter surges of the coronavirus made that imprudent. After one (just one!) face-to-face meeting, we did not want this virtual meeting to be a continuation of the (bi-)weekly working sessions, so we asked members to look at what their group is doing to help technology users transform digitally. They then presented to the entire membership to help break down the silos than can arise from steady work on their topic. This meeting had:

- 56 member organizations,
- 79 member representatives,
- eight presentations from non-members,
- four working group plenary sessions,
- five group working sessions,
- one test drive presentation and
- one innovation panel.

The meeting profiled one published paper: Industry IoT Consortium Whitepaper Examines Impact of Distributed Ledger Technologies on Provider Networks. This is a deeply technical paper that examines how provider networks are affected by distributed ledger technology, and how innovative solutions can improve performance of a network.

Headwinds and Tailwinds

Five years ago, McKinsey & Company published a report on predicted adoption of the internet of things (IoT). In November 2021, they published a sequel: The Internet of Things: Catching Up to an Accelerating Opportunity. In this report, they looked at which sectors had adopted IoT faster than predicted and those that adopted it more slowly. Generally, adoption has been slower in hospitals, manufacturing and vehicles, while adoption has been faster than predicted in offices, home and farms. Clearly, the industrial verticals are adopting IoT more slowly than others. Why?

To find out, we invited one of the authors, Mark Collins, to keynote in Q1. There, he described current uptake in each industry and vertical sector, and the headwinds that inhibited adoption. What do these headwinds hold back? Value creation in plant-process optimization, equipment health monitoring, maintenance tracking, logistics, inventory and network optimization are just a few. Two areas stood out: security and interoperability, especially in industrial IoT (IIoT). Why?

For one thing, the consequences of a security breach in industrial IoT can be much more severe than in an office or home. Moreover, 'security' in IIoT has to cover far more than cybersecurity. It must include physical security, safety, privacy, resilience and reliability. We call these together *trustworthiness*, and that is much more than the sum of the parts. The various elements need to be reconciled in the face of differing vocabulary (what does 'security' mean to an IT person versus

the plant manager?) and emphasis (IT tends to emphasize cybersecurity while the plant manager is mortally concerned with safety, resilience and reliability). In short, the trustworthiness concerns in industrial IoT are both more significant and more difficult to address.

Interoperability also differs in consumer IoT versus industrial IoT. Most consumer IoT applications start from scratch with a life time of a few years, whereas the median age for industrial plants is 19 years. You may need to retrofit sensors. And while 5G is all the rage right now, some factories are lucky to be using 2G. Connecting multiple devices, possibly with ancient interface protocols, to the internet takes time and effort with careful planning of migration to new technologies while keeping the factory running. (See the II Connectivity Framework.)

Moreover, the range and variety of components in the home or office is less than in industrial systems. The age of these systems means that interoperability was, like security, an afterthought. Consumer IoT is often greenfield using vendors that are "walled gardens" that have no need (yet) for interoperability, so of course the headwinds are lighter. What, then, must we do?

For trustworthiness, the IIC has liaisons with multiple, global organizations and we are aligning our work with their standards. We are working to adopt security-by-design for all digital transformation projects in legacy systems. (It is a commonplace to observe that the internet was developed without security in mind.) 'DevSecOps' is an extension of 'DevOps', which combines software development with IT operations to shorten the systems development life cycle and provide continuous delivery with high software quality. DevSecOps lets developers add security (trustworthiness) to that process.

Developers in organizations undergoing digital transformation must communicate and align security strategy with value creation. This requires high-level contact with upper management, both to inform them of risks, and for alignment with value creation. Talking about the technical detail is not going to work. You need metrics that are understandable by non-technical people. And this feeds right into governance, where trustworthiness metrics and strategy are aligned at the board level. (See the II Trustworthiness Framework.)

The IIC defines interoperability as the ability of two or more systems to exchange information and mutually use the information that has been exchanged.[1] There are multiple levels of interoperability as shown in the figure on the next page.

We believe that the industry (and of course your mileage may vary) is somewhere around level three or four.

What does this mean for you? For vendors, interoperability is critical to selling into multiple verticals. Because of the shortage of IIoT talent, provisioning and installation must be facilitated. For customers, it means searching out and investing in IIoT talent, even as you recognize that

[1] This is taken from ISO/IEC 17788:2014.

Headwinds

Composability	Level 6: Conceptual Interoperability (**alignment of concepts relating to an abstraction of reality**; definition of concepts with engineering tools)
	Level 5 Dynamic Interoperability (coping with **system state changes**)
Interoperability	Level 4: Pragmatic Interoperability (known context and **use of information** exchanged)
	Level 3: Semantic Interoperability (ability to **interpret meaning of data** exchanged as information in a given context)
Integrability	Level 2: Syntactic Interoperability (common and **unambiguous data formats**)
	Level 1: Technical interoperability (ability to **exchange data as bits and bytes**)
	Level 0: No Interoperability

technology is not the driver—the outcome, the value proposition is what matters. In turn, this means that the operating models must change in response to the usage of the technology. There is no silver bullet!

For IIC, we have produced results from our testbeds and test drives, especially around the Time Sensitive Networking testbed. We need standards and open source to avoid pilot purgatory (a term coined by McKinsey). Training is needed in multiple areas to bridge the gap between IT and operational technology (OT). And we need thought leadership to mature the concepts and transfer the knowledge across verticals. (See the Guide to Global Industry Standards.)

Group Activity

The *Industry Working Group* engages industry leaders and technology users to understand their IIoT needs and facilitate digital transformation in their business. It has two initiatives:

- The Digital Transformation Enabler Initiative identifies sets of end-user-driven use cases and digital transformation technology enablers that it can support through development of guidelines, best practices, frameworks, test drives, testbeds and business pain points. The initiative focuses on specific application areas of interest to specific verticals and technology that can be applied to enable use cases in multiple verticals.
- The Business Deployment Acceleration Initiative identifies customer pain points, business challenges and collaborative co-innovation activities to solve them. The goal is to engage end users to understand business challenges and involve the IIC ecosystem to co-create a solution.

The group supports several vertical groups (below) that are identifying architecture patterns and reference architectures that support deployment of use cases for their respective industries.

The *Smart Factory group* is collaborating with Industrial Valuechain Initiative, an IIC liaison, on their Connected Industries Open Framework (CIOF), and with Purdue University and their Indiana Next Generation Manufacturing Competitiveness Center (IN-MaC) and Smart Factory lab. The

group plans the Global Industry Organizations Workshops. It seeks examples of maturity models deployed in factories.

The *Healthcare* group is focused on using IoT and IIoT solutions that provide safer and more efficient patient care. It promotes testbeds, facilitates collaboration with academia, industry and government. It develops patterns, promotes standards and whitepapers

It is working on identifying technologies and digital transformation enablers as well as defining terminology, outcomes and patterns. The group completed the Remote Patient Monitoring architecture pattern which was split into two patterns, a generic pattern and a specialization of the generic pattern to the remote patient monitoring. The current focus is on the Air Quality Monitoring architecture pattern

The *Energy* group identifies and establishes the technology, security and market criteria necessary to establish standards and specifications leading to wide-spread adoption of the industrial internet in this sector. It brings together business and technology experts in the energy sector from around the world to verify the feasibility of technology solutions and assess the viability of new business models emerging with the adoption of IIoT. It is working on Energy Reference Architecture Patterns.

The *Automotive and Industrial Over-The-Air* group promotes OTA updates and related technologies to end users in the automotive, intelligent transport systems and other IIoT industries. The AIOTA TG identifies and develops best practices, test drives, testbeds and use cases that guide the application of OTA, related communication and digital-transformation-enabling technologies in support of use cases.

The *Mining* group helps mining operators and mining equipment manufacturers optimize business operations and find new revenue streams. The objectives include global collaboration, engagement with global mining companies and organizations, research, whitepapers, case studies, mining reference architecture and development of mining test beds.

The *Business Deployment Accelerator* group addresses the pain points that IIoT users face in their businesses, and identifies the key technologies and digital transformation enablers to resolve them. These business deployment accelerators are used in go-to-market strategies and mapping of potential “customers” who will benefit from them. Testbeds and test drives are the vehicles to test solutions to resolve the pain points.

It is creating a pain-point repository for IIC members organized by business operational technologies and end-user-solutions and how to use them various. This will lead to a practical guide on how to support the go-to-market strategies and reach the customers.

The *Manufacturing Industry Leadership Council* meets quarterly. An attendee (who need not be a member) should be in a director-level role or higher and actively implementing or using an IIoT solution in manufacturing facilities. IIC seeks to add additional councils.

The group provides actionable guidance and best practices for all aspects of developing and operating an IIoT solution: business case creation, architectural design, technology selection, implementation, testing, roll out and operations.

The *Business Development Operations Group* is identifying tools for speedy and deep innovation (product, process and business model) process for user industries and identifying key issues for solving possible conflicts between the tool-driven innovation processes and organizational structure, incentives and funding system. The group is developing a framework to help solution operators undergoing digital transformation create their own innovation processes resolving problems integrating IT and OT.

The *Security Working Group* addresses the trustworthiness of the IIoT ecosystem, addressing safety, reliability, security, resilience, and privacy. Its objectives are to:

- promote IIoT business adoption of trustworthy technology, interoperability, best practices and models,
- guide practical implementation by working with IIC testbeds, providing public-facing technology demonstrations and thought leadership for the industry,
- apply the breadth of industry understanding through maturity models, use cases, case studies, norms and best practices and
- identify gaps and collaborate with external consortia, standards bodies and industry groups.

The group is working on a minor update to the *Industrial Internet Security Framework*, with representatives of ISA to review the mapping between 62443 and the security maturity model and with representatives of the Digital Twin Consortium to develop a Digital Twin SMM profile.

The *Trustworthiness* group explores aspects of trustworthiness relevant to IIoT and the IIC's vision of an IIoT ecosystem. Trustworthiness is the degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks.

Establishing confidence and being able to communicate that an IIoT system is trustworthy benefits many stakeholders. Assuring trustworthiness benefits the organization and customers by enabling the organization to deliver value while managing risks systematically. Additional value includes safety for employees and the community, privacy for individuals and the ability to communicate explicitly in a standardized manner about the grounds for claiming that an IIoT system, component or capability is trustworthy.

The *Technology Working Group* and its subgroups work with the vertical groups to maximize specific industry content in deliverables. They collaborate with other groups to maximize work on emerging technologies and digital transformation enablers.

The *Architecture* group is developing architecture patterns. It has a draft of the Industrial Internet Reference Architecture v2.0 (IIRA v2.0) that aligns better with ISO/IEC 42010 Architecture Framework and supports ISO SC41. Content includes architecture patterns and addresses system of systems (architecture pattern), heuristic computational intelligence, digital twin, blockchain, edge computing, physical senses, voice recognition, AI, machine learning and big data.

The *Connectivity* group is a resource for connectivity related issues and interfaces with IIC testbeds to promote connectivity innovations.

The *Digital Twin Interoperability* group provides a precise digital twin definition, elaborates on advanced use cases, conveys the role as the interoperability enabler among vendors and business value of digital twins.

The *Distributed Data Interoperability and Management* group will define the properties of a data service framework for the industrial internet. Its purpose is to provide a ubiquitous data-sharing integration framework for all architecture elements. The group is currently working on a report on information entity identification. They are researching future deliverables: community-sourced perspectives on information modeling, digital twin information models and exchange with testbeds and test drives.

The *Edge Computing* group is responsible for the creation, maintenance and adoption of a technical report addressing the implementation of edge computing. They have developed a technical brief template to present specific areas of edge to the group for addition to reports.

The *Industrial Internet Analytics* group is responsible for developing the Industrial IoT Artificial Intelligence Framework and defining and promoting best practices for realizable, comprehensive techniques and methods to derive information from data and where to deploy AI in IIoT.

The *Patterns* group gathers, creates and publishes architectural and design patterns for industry. It provides guidance and expert knowledge to support the selection of patterns.

Patterns are providing solutions for recurring problems and offer a possibility to present knowledge in a compact and simple way. This year, the IIC has described eleven patterns and made them available in the public repository. End products are posted on the Resource Hub Patterns Webpage. You can submit a pattern using the Pattern Template.

The *Vocabulary* group develops the Industrial Internet Vocabulary Technical Report to establish a common vocabulary for stakeholders to reference. A German version is due 2023.

The *Marketing and Innovation Working Group* concentrates its efforts on promoting the value of IIoT, supporting the IIC's industry programs, initiatives, groups and testbed results. It works directly with IIC members to promote their work and deliverables, thereby delivering brand awareness for the representative, the member company and the IIC.

IIC members gain experience they could never have as a non-member. Here are some key benefits of membership:

- ***Networking***—Make the connections; find the needed expertise.
- ***Information & News***—A fast pass to newsworthy industry developments.
- ***Competitive edge***—Stay ahead of the competition or take advantage of changes and developments that might otherwise have passed you by.
- ***Create a market***—Join a collective voice supporting a single mission; create the disruption in the market and develop the business opportunities.
- ***Establish a vision*** –Members work to define future architectures and innovate technologies for IIoT.
- ***Success***—Members are building businesses and dedicating their professional lives to IIoT. They want to be successful, and they want others to succeed.
- ***Professional development***—Grow your career, meet mentors and mentees, career prospects.
- ***Solve important problems—***and help your partners and customers.
- ***Events*** – Capitalize on opportunities for continuous exposure to industry developments.

The group has accumulated a substantial collection of IIoT technology and business presentations and corresponding videos (44 sets in total, and is working to make this valuable asset accessible to a wider audience.

Webinars and Publications

Visit our Webinars Webpage for access to IIC-hosted and liaison-syndicated webinars as well as a comprehensive list of past and future webinars.

A complete list of IIC publications can be found here.

New Members

Please welcome new members this quarter:

- iBebot Limited ,
- Purplenow Technologies,
- Labforge Inc.,
- MobilFlex,
- YellowDotPink and
- iiDevice Nevada Technology Labs Inc.

The Industry IoT Consortium is the world's leading membership program transforming business and society by accelerating the Industrial Internet of Things. Our mission is to deliver a trustworthy Industrial Internet of Things in which the world's systems and devices are securely connected and controlled to deliver transformational outcomes. Founded March 2014, the Industry IoT Consortium catalyzes and coordinates the priorities and enabling technologies of the Industrial Internet. The Industry IoT Consortium is a program of the Object Management Group® (OMG®). Visit www.iiconsortium.org.