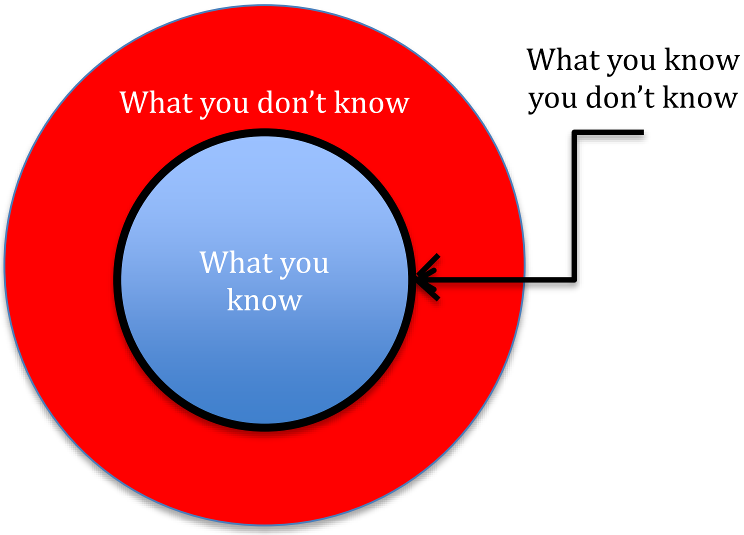
Trustworthiness

The Industrial Internet Consortium (IIC) held its 2017 fourth-quarter member meeting December 5th ~ 8th in Burlingame, CA, near San Francisco. It was especially busy and productive, with over 45 working or information sessions, 30 testbed sessions, IIC Connect and other activities. (IIC Connect is a series of twenty-minute meetings between members to help build—and use!—the ecosystem. There were almost fifty meetings this time.) We also held a World Tour event that showcased four testbeds, Smart Factory Web, TSN Testbed, FOVI and Smart Factory Machine Learning for Predictive Maintenance.

A common topic in the sessions was support for the Industrial Internet Interoperability Coalition (I3C) initiative. The I3C is an effort to open up the work of the IIC and make our content more digestible. Most of our groups are working to ensure relevant content is channeled to the I3C team for inclusion in the underlying content database to help it grow. The database links together the various elements so that we say things once and we can quickly follow threads of information that need to be considered. This is needed because a key feature of the industrial internet of things (IIoT) is the convergence of information technology (IT) and operational technology (OT), which means we need to bring different ideas and skills together and *help people understand what they don't know*.



By identifying what we don't know, and providing easy links to find out more, the IIC can help companies build trustworthy IIoT systems more quickly. The Industrial Internet Security Framework defines trustworthiness as "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 disruptions, human errors, system faults and attacks". The five elements are highly interlinked and must be understood by all parties, some of whom don't know they need to find out!

TRUSTWORTHINESS

Everyone talks about security, and we are all doing something about it, but security is only one part of making IIoT systems trustworthy. For a system to be trustworthy it needs to address all of security, privacy, resilience, reliability and safety, which are linked together and must be reconciled. For example, security would suggest that doors be securely locked, while safety would say it has to be as easy as possible to get out, and not waste valuable time looking for a key. Similarly, security would say that more layers of security are better than fewer, but again that would waste precious time while your power plant is trouble.

The focus of the Security Framework is security (hence the name), with some attention paid to privacy. It does not treat all the elements thoroughly. So to begin with, we kicked off a group to work on safety. (A little history: They began as a group under the Security Working Group (WG), but there were concerns that it would be seen as subordinate to it, so we moved the group to the Technology WG, but trustworthiness is more closely related to security, so we moved it back. The joys of trying to manage perceptions!)

The safety group, after all this juggling, has completed a short report on Key Safety Challenges for the Industrial Internet of Things. The report examines four:

- increased security risks due to increased attack surface,
- information technology (IT) and operational technology (OT) convergence,
- pervasive autonomy
- inadequate regulatory frameworks and evolving standards

These challenges require strong consideration. They will require more work on trustworthiness, including especially an understanding of the tradeoffs related to the aspects of it. The authors encouraged interested parties, including those working in both IT and OT, to collaborate to find solutions. (We have disbanded the Safety group now and created a new one: Trustworthiness.)

This call for collaboration between IT and OT is crucial. We need to know the safety challenges in *your* industry. Safety is quite a different matter in health care than it is in manufacturing. For this reason, we are establishing several focus areas. We spent a lot of time last year working with Plattform Industrie 4.0, holding a World Tour event series focused on manufacturing. The IIC Steering Committee has selected Energy as a focus area for the first half of this year. We shall examine trustworthiness in this domain, attend energy conferences, reach out to energy companies and the like. We are introducing our 2018 event series as a Global Event Series and will hold our first event as an Energy Forum, hosted by The MITRE Corporation, free and open to public, on February 9th in McLean Virginia, USA.

We will select another focus area for the second half of the year.

GROUP ACTIVITIES

Our groups continue to make progress on their activities and deliverables. Two highlights are:

The Marketing Working Group formed an *Automotive Task Group* that will provide direction to the IIC's activities in automotive. The group will collaborate with other groups to target areas such as analytics, distributed data interoperability and management, connectivity, and security.

The Security Working Group formed the *Automotive Security Task Group* that will engage with automotive and transportation verticals, focusing initially on trustworthiness.

LIAISONS

The Liaison Working Group continues to approve and pursue strategic technical relationships. New liaisons established this quarter include:

- MulteFire Alliance: An international association dedicated to building a global ecosystem in support of the common interests of members, developers and users in the application of Long Term Evolution (LTE) and next generation mobile cellular technology in configurations that use unlicensed and shared radio spectrum. MulteFire is an LTE-based technology that can be deployed standalone in unlicensed or shared spectrum, while ensuring fair sharing of spectrum with other users and technologies in the same bands.
- NEMA: The National Electrical Manufacturers Association (NEMA) represents nearly 350 electrical equipment and medical imaging manufacturers at the forefront of electrical safety, reliability, and resilience, as well as efficiency and energy security.
- Robot Revolution Initiative: The Robot Revolution Initiative (RRI) is an initiative of the Japanese Ministry of Trade and Industry that promotes manufacturing business revolution through IIoT and robot application expansion. RRI will serve as the center for wide-ranging stake holders who will clarify issues that they should work on by themselves, share progress status, and work together to specifically promote Japan's robot strategy.

TESTBEDS

Testbeds provide an environment for companies and multi-disciplinary stakeholders to team up and prove out complex systems and gain real-world experience. With 26 approved testbeds (and more in the pipeline), participants are generating best practices, recommendations and priorities for standards organizations. In our fourth-quarter meeting, there were seventeen testbed-update presentations, along with concept testbed introductions and testbed platform presentations.

The purpose, of course, is to generate "outcomes". Published in the sixth edition of the *Journal of Innovation*, is the article "The Outcomes, Insights, and Best Practices from IIC Testbeds: Intelligent Urban Water Supply Testbed" that describes insights specific to that testbed.

PUBLICATIONS

Publications released during the last quarter of 2017 include:

The joint white paper, Architecture Alignment and Interoperability, presents the mapping and alignment between the Industrial Internet Reference Architecture (IIRA) and the Reference Architecture Model for Industrie 4.0 (RAMI4.0). Published by the IIC and Plattform Industrie 4.0, it is the first substantial report on the joint effort between these two organizations since they started their collaboration.

The Key Safety Challenges for the IIoT white paper highlights four key challenges, explains why the current safety frameworks and approaches are inadequate and recommends how the greater IIoT community should address them.

JOURNAL OF INNOVATION

The sixth edition of the *Journal of Innovation* was published in November and includes articles ranging from artificial intelligence (AI) to the Intelligent Urban Water Supply Testbed including:

- How Democratized Artificial Intelligence Can Move Manufacturing to a New Evolution Pace
- Industrial Intelligence: AI's Implications on Security, Seamlessness and Services for the IIoT
- Outcomes, Insights, and Best Practices from IIC Testbeds: Intelligent Urban Water Supply Testbed
- Spotlight on the Industrial IoT Analytics Framework

INDIVIDUAL CONTRIBUTOR AWARD

The Steering Committee instituted an award program to recognize some of the great work you can see being carried out in the IIC. The award category for this quarter was the Individual Contributor Award. The award was given to Mr. Wael Diab (Huawei Technologies). Congratulations, Wael!

Wael was recognized by his peers for his leadership and contribution to the Liaison Working Group. His nomination cited the importance of the Group as the gateway for formal relationships with standards and open-source organizations, consortia, alliances, certification and testing bodies and government entities and agencies. The purpose of these relationships is to generate requirements for new standards from every part of the activities taking place within the Industrial Internet Consortium.

NEW MEMBERS

Please join me in welcoming the following new members to the IIC:

- Basler AG (Germany)
- Blockchain of Things, Inc. (USA)
- Blocks Wearables (United Kingdom)
- China Mobile Communications (China)
- Corlina (USA)
- IGS Group (Chile)
- Korea Industrie 4.0 Association (Korea)
- LISNR (USA)
- Machfu, Inc. (USA)
- OnBoard Security (USA)
- Saudi Telecom Company Solutions (Saudi Arabia)
- T-Systems International/Deutsche Telekom (Germany)
- WiseKey SA (France)

Come and join us!

IIC members gain experience they could never have as a non-member. They experience member meetings unlike any local meet-up groups. 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.
- ***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 Industrial Internet 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 by AT&T, Cisco, General Electric, IBM and Intel in March 2014, the Industrial Internet Consortium catalyzes and coordinates the priorities and enabling technologies of the Industrial Internet. The Industrial Internet Consortium is a program of the Object Management Group® (OMG®). Visit www.iiconsortium.org.