IIC Quarterly Report:

February 2016

2015 was a busy year: publication of the Industrial Internet Reference Architecture in June, ongoing work on the Security Framework, creation of a new Working Group, Business Strategy and Solution Lifecycle and more. But how does all this fit together?

RAISON D'ETRE

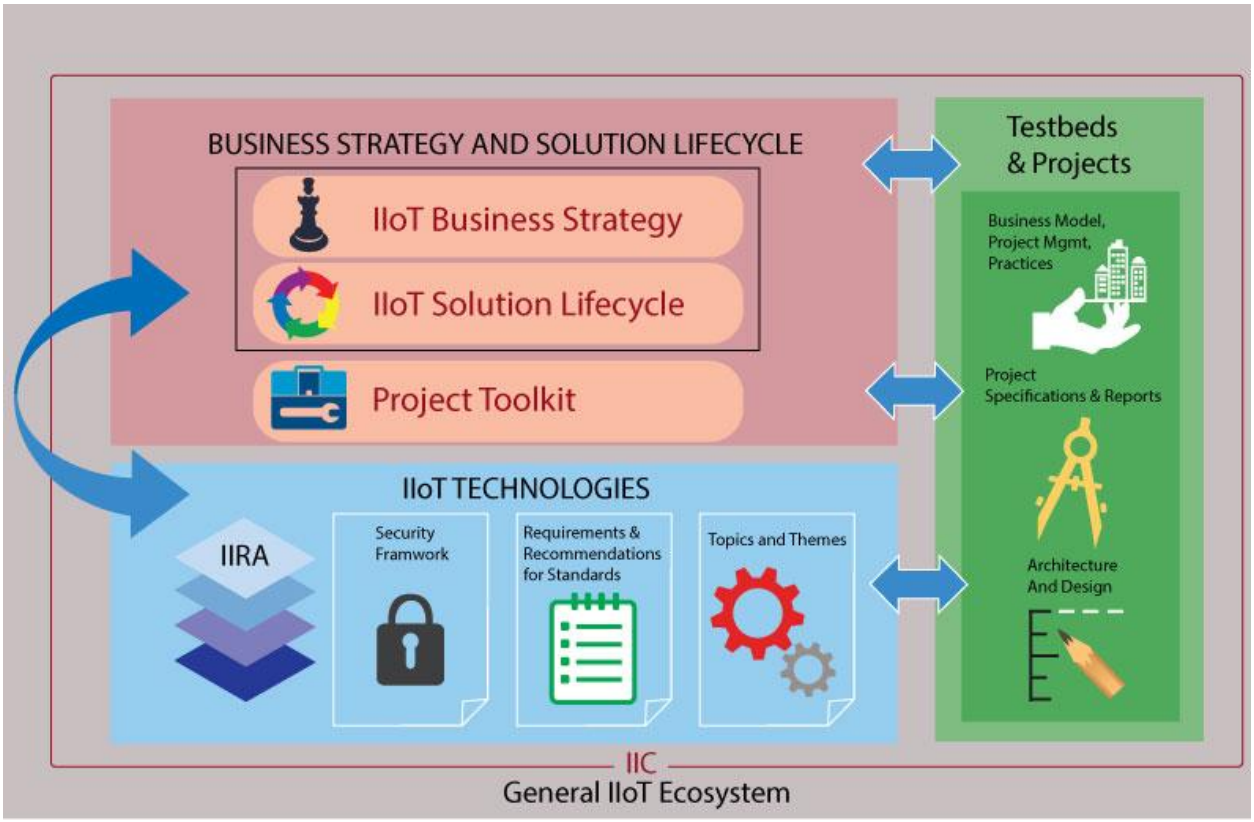
The Industrial Internet Consortium (IIC) exists "to accelerate growth of the industrial internet by coordinating ecosystem initiatives to connect and integrate objects with people, processes and data using common architectures, interoperability and open standards that lead to transformational business outcomes." This means that our primary goal is a business one (business strategies and solutions), but we need appropriate IIoT technology to shape those goals. We need also to test these new technologies and business models on real projects and testbeds, and bring these from the IIC ecosystem into the broader global ecosystem of industry, academia and government. These broad goals led to the formation of the several working groups in IIC, but it doesn't say what each of these groups should do exactly.

While much of the ink spilled today is about evolutionary improvements using modern IT technologies to address traditional operational technology (OT) concerns, the real business impact will be to expand our horizon of addressable concerns. Traditional OT has focused on process correctness and safety; traditional IT has focused on time to market and, as a recent concern, security. Both disciplines have developed in a world of relative scarcity, with perhaps hundreds of devices interconnected to perform specific tasks. The future, however, points toward billions of devices and tasks that change by the millisecond under autonomous control, and are so distributed they cannot be tracked by any individual. Our existing processes for ensuring safety, security and management break down when faced with such scale. Stimulating the redevelopment of our technologies for this new world is a focal point for the IIC.

To address those questions, we held a session entitled "Roadmap." It quickly became clear that we are not ready to place deliverables on a timeline. Rather, we needed to create a *statement of the technical activities* outlining the main components first, as depicted below.[1]

There are four main elements of this picture, each in a different color. They are: IIoT Technologies, Business Strategy and Solution Lifecycle, Testbeds and Projects, and surrounding all that, the IIoT Ecosystem.

[1] This diagram replaces the familiar three-stage arrow figure used in prior quarterly reports.



The foundation of the IIC's work is *IIoT Technologies* with the Industrial Internet Reference Architecture, published in June 2015 being the backbone. Without technologies the business goals cannot be met. The reference architecture comprises three parts: an overview, the architecture proper (based around the four viewpoints) and an analysis of key system concerns.

The technologies and other architectural constructs are put to use according to a *Business Strategy and Solution Lifecycle*. IIoT Business Strategy assists in developing the strategic context in which IIoT projects are identified and then everything we need to initiate, develop and operate an IIoT system.

Taken together, the IIoT Technologies and Business Strategy and Solution Lifecycle documents provide references. The reference architecture, for example, outlines the components that make up a typical IIoT system, and useful though this may be, these are just concepts and models. Similarly, Business Strategy and Solution Lifecycle guides project development, but it's not a real system. *Testbeds and Projects*, on the other hand, are the real thing. The references (on the left) guide us in building real systems (on the right); in turn real systems inform the references. The bidirectional arrows between them capture this relationship.

Similarly, IIoT technologies are useful only in so far as the business can make use of them and business strategy drives which technologies are needed. (The bidirectional arrow on the left.)

The *Ecosystems* comprise those businesses, academics and governments working within the IIC, the relationships fostered through their active participation and the transformational outcomes derived from member collaboration.

IIoT Technologies

The Industrial Internet Reference Architecture (IIRA) comprises three parts: an overview, the reference architecture proper and a set of key system concerns. We are presently revising this document in light of continuous evaluation of its applicability and to make each of these parts distinct. In so doing, we hope both to make the document more accessible and to seed a structure for documents that we produce in the future.

The backbone for the IIoT Technologies is the reference architecture, which can only be effective if it is secure. Much of the time at the La Jolla meeting was allocated to review and revision of the Security Framework. This document, presently over a hundred pages, deepens the security considerations in the IIRA, including a great deal of detail and references to existing standards in this area.

Security is only one, albeit an important one, of a number of *topics and themes* that need to be elaborated for a general IIoT architecture. These include safety, connectivity, resilience, interoperability, distributed data management, industrial analytics, dynamic and autonomous collaboration and more. Just as the Security Framework is a more detailed description on the topic of security than the summary provided in the IIRA, so we need detailed descriptions of each of these topics and themes. And just as the Security Framework is identifying existing standards, so will these other topics and themes.

But these standards are not yet adequate to the entire task. (If they were, we could shut up shop and go home.) We will analyze each of these topics and themes, write recommendations and requirements for standards, and present them to standards-development organizations. The IIC has already established liaisons with a number of organizations.

Taken together, the IIRA, the Security Framework, detailed topics and themes and requirements and recommendations for standards all inform real testbeds and projects, specifically their *Architecture and Design* (bottom right of the figure). And what we learn from building real testbeds and projects allows us to refine the references.

Business Strategy and Solution Lifecycle

This working group, established in the third quarter of 2015, extends the remit of IIC to cover the business side of IIoT projects. IIoT Business Strategy covers pretty much what it says on the tin. It begins even before project inception by developing the strategic context, identifying opportunities, prioritizing them, understanding technology and business requirements, preparing the business case, establishing partnerships and getting started.

The second part is the solution lifecycle—the actual delivery of the IIoT project. This covers planning and design of the architecture, building and testing the solution, operating and managing the solution, supporting new and existing customers, and finally decommissioning it.

These two elements inform and are influenced by actual business models, project management and practices on real testbeds and projects.

Third and last, this working group is creating a project toolkit covering templates and metrics for both business and technical aspects of IIoT projects.

Testbeds and Projects

Because we cannot possibly know everything, we have to experiment, guided by the concepts, models, methodologies and processes from both the IIoT Technologies and BSSL, with *testbeds*, scaled-down real-world systems that return technical and business results. The results from the testbeds feed back into all the prior work, particularly the project toolkit.

Testbeds and other projects provide the background for new business solutions grounded both in an understanding of the business value of the proposed product or service and their execution. These new products and services go to customers who, in turn, feed the ecosystem.

IIC Ecosystem

The IIC ecosystem is the collaborative environment created by the Consortium. By fostering collaboration around the globe throughout the year, the IIC enables the creation of the partnerships necessary to build consensus on the issues of industrial internet solutions. The ecosystem also publicly promotes the work of the members of the IIC, providing a broad platform to spread innovative ideas. It covers marketing and communications, and the publication of technical materials written by members. At the time of the La Jolla meeting, the IIC Marketing Working Group published the first edition of the Journal of Innovation, a concrete example of thought leadership.

We also work with groups that focus on specific vertical markets. For example, the Energy Task Group has 89 member representatives on its roster, producing case studies, and working with other organizations in the sector.

OTHER WORK

Meanwhile, the Technology Working Group has stood up several Task Groups. The *Innovation Task Group* "shall build a stage for those research communities, industrial forums and start-ups to present or demo the innovations to IIC members, where potential connection and collaboration could happen to accelerate the innovated technology and benefits for the members and the whole world," and they've managed a couple of presentations.

The *IT/OT Task Group* is also new. It recognizes that IT and OT realms differ fundamentally, in ways that complicate the development and growth of the IIoT. The goals of the IT/OT Task Group are to model and describe these challenges; and to make technology and management recommendations for addressing them.

The *Architecture Task Group* has reviewed the work of ISO JCT1 WG10, who are working on a reference architecture standard, and provided many comments from the members. They will be following up in detail over the coming months.

The *Liaison Task Group* exists to establish liaisons with standards development organizations and with other consortia of various kinds; it does not exist to carry out technical work. We are in the process of setting up a variety of contributing groups with whom to liaise, ISO JCT1 WG10, IEEE P2413, and other standards development organizations in the topic areas. When we have recommendations and requirements for standards, the Liaison Task Group is the conduit.

The *Vocabulary Task Group* has begun a careful read of the Security Framework looking for terms that require definition, providing drafts and reviewing them, so that the Security Framework can be as complete as possible when it is published for review to our liaisons.

The *Testbed Working Group* is still furiously working on testbeds. The latest to be approved in 2015 is the Industrial Digital Thread testbed.
