Progress Report: 2016 Q2

The Industrial Internet Consortium (IIC) was announced just two years ago on 27th March 2014 in Reston, Virginia, USA. At that first meeting, all of the member company representatives could sit around a single dinner table and maintain a single conversation. With IIC approaching 250 members from 30 countries, when we met again in Reston last month, we could barely fit the working-group leads around a table, and certainly failed to maintain a single conversation!

When the IIC was founded, it had four working groups that met regularly: marketing, technology, security and testbeds. Testbeds enable innovation by testing out ideas, technology and business models. Testbeds distinguished IIC, then and now, and they are a strong “selling” point.

IIC is again leading the way with a new working group: *Business Strategy and Solutions Lifecycle*.

BUSINESS STRATEGY AND SOLUTIONS LIFECYCLE WORKING GROUP

The Business Strategy and Solutions Lifecycle Working Group was established nine months ago to provide guidance and best practices for all aspects of developing and operating an industrial internet solution: from defining a strategy and generating ideas, through business-case creation, project management, architecture design, technology selection, implementation, testing, rollout and monitoring through operations.

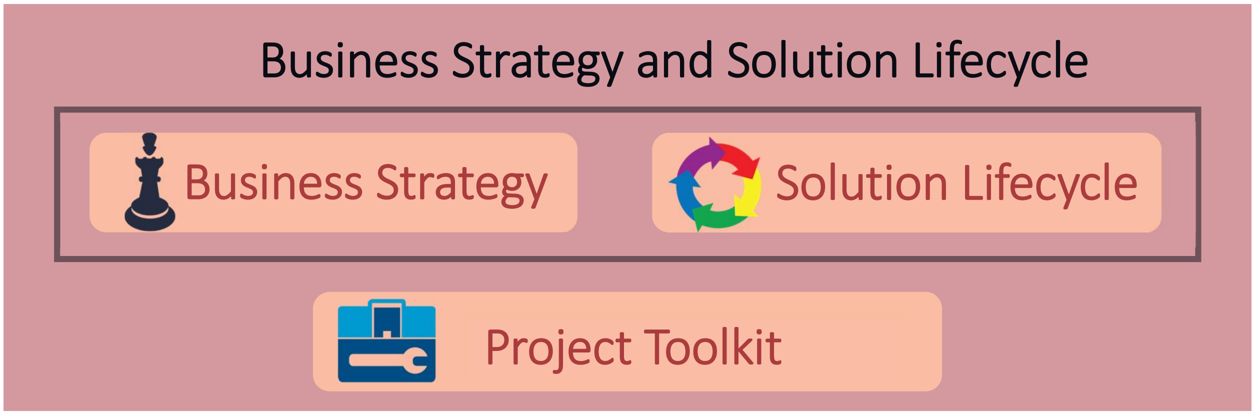
The goal is to help companies maximize the returns that are generated from Industrial Internet of Things (IIoT) concepts, manage project risks efficiently and establish a foundation for evaluating solutions and ensuring their compliance to business or regulatory requirements. Its activities fall under four major themes:

Business strategy: to identify and prioritize IIoT opportunities, analyze business requirements, prepare business cases and evaluate the viability of IIoT business models and generally support efficient downstream project activities and deployment.

System design: to formulate best practices for using and implementing the Industrial Internet Reference Architecture (IIRA) and its crosscutting concerns. This also includes:

Project Management: to define how to plan, develop and deploy an IIoT solution, organizational aspects, IT and operational technology (OT) collaboration, assets management and production line set-up across the entire lifecycle.

Metrics and measures: to assist the design and management of IIoT systems including defining system categories and profiles based on their capacities along different dimensions, contracts, testing, monitoring and evaluating systems for both functional aspects (performance, data flows) and key system characteristics such as safety, resilience, reliability, privacy and security.[1]



DELIVERABLES

The working group has defined four deliverables (so far).

Business Strategy for the IIoT Whitepaper: This document identifies and analyzes at a high level the key issues that an enterprise needs to address to exploit IIoT concepts fully for commercial (or other) gain. It is intended to be a reference for any enterprise planning to engage with IIoT concepts. Currently much of IIoT is characterized by uncertainty and flux. The adoption of IIoT concepts can be accelerated by 'de-risking' any decision to deploy IIoT technologies that a senior manager in any enterprise may take. Accordingly, the purpose of this document from an end-user and enterprise perspective is to provide a single-source compendium of the issues and challenges that should be considered before any IIoT initiative can be deployed. It is not intended to provide a detailed analysis of these issues and challenges, simply to highlight the existence of generic challenges (and opportunities) at a high level. The document is currently at a late draft stage, with a view to publication in the second quarter of 2016.

IIoT Solution Assessment Toolkit: This document is a toolkit to help IIoT project managers and solution architects manage their projects and testbeds more efficiently by re-using best practices from other IIC members. The toolkit provides a structured questionnaire that can be used after the initial business-modeling phase and before the solution design. The input includes data from the business model, known requirements and known constraints. The output supports typical project management tasks like cost estimation, risk management, creation of the project plan or work breakdown structure and architecture design, solution design and technology selection. It also enables comparison across projects, so that best practices and lessons learned can be readily

[1] Drawn from the working group's charter.

imported into a new project environment. The document is currently at a late draft stage, with a view to publication in the second quarter of 2016.

Reference Architecture Mapping Template: The template maps an IIC testbed—and more generally an IIoT system—to the IIRA. This mapping consists of showing how the target system can be described using IIRA concepts and terminology. It comprises tables that correspond to concepts developed by the IIRA. The template has three sections:

- general information on the target system,
- reference architecture viewpoints of the target system, and
- system characteristics and profiles detailing the overall properties of the target system.

Development work on the template is nearing completion, and once complete the template will become one of the first artefacts in the IIC library.

IIC Library: This is a collection of templates, patterns and metrics containing information gathered from testbeds and other projects that enterprises can use to get started. Initially the library will include elements such as the basic project management artefacts and frameworks that are needed to efficiently manage IIoT projects, as these are developed within the BSSL WG. As the work of the overall IIC progresses, the library will also act as the central repository for frameworks and other similar outputs developed by other IIC WGs. The library may also include case studies and similar analyses of 'real world' deployments where these can be informative to IIoT project managers on an ongoing basis.

Taken together, these deliverables cover the entire lifecycle of IIoT system development and will be a great help to Member companies in accelerating the development of their projects.

Back to Testbeds

Meanwhile, following on from the report last September, we have more than doubled the number of approved testbeds, from nine to nineteen. This explosion in the number of testbeds is due to two factors. First, there is a great deal of interest in them, demonstrating their value. Second, we have improved our internal processes so they can be approved more quickly.

Here is a sampling of two of these new testbeds.

Security Claims Evaluation Testbed: The primary objective of the Security Claims Evaluation Testbed is to provide an open and easily configurable security platform for evaluation of endpoint, gateway and other networked components' security capabilities. The testbed enables participants to connect their equipment to a system of other endpoints, gateways and so on. To evaluate the security capabilities of their equipment, interoperability to other devices, and to verify the critical areas of their architecture pattern are secured as outlined in the Industrial Internet Reference Architecture. The test bed will follow a staged approach with the first stage in a lab environment, the second stage in a micro-factory and the third stage as installed evaluation platforms across multiple geographies.

The technologies to be tested include: secure operation of end-to end system command and control during acquisition and processing and data analysis during standard functional modes of communication. Secure operation encompasses all functional elements—hardware, software and other system level components of the testbed.[2]

IIC Members Underwriters Laboratories (UL), Xilinx and Aicas sponsor this testbed.

Intelligent Urban Water Supply. This testbed seeks to:

- increase safety and quality of the water supply by employing system-wide water quality monitoring, supported by analytics, to raise water quality issues and identify sources of degradation,
- improve availability of the water supply by employing advanced asset-maintenance capabilities with real-time monitoring, fault detection and preventive maintenance to improve water supply asset reliability, and
- enhance efficiency of water supply operations by employing advanced analytics on water supply asset operational data to reduce asset energy consumption, detect water leakage and optimize system-wide water distribution during peak usage hours or under shortage in supply.[3]

IIC Members Water Process Group (WPG), Thingswise and the China Academy of Information and Communications Technology (CAICT) sponsor this testbed.

Security Working Group

The Security working group is nearing a milestone: it is has released a draft of the first half of the Industrial Internet Security Framework (IISF) Technical Report to IIC liaisons for comment. The second half is planned to be released in mid-May to give reviewers enough time to comment before the next IIC Quarterly Member Meeting in Tokyo in June. The document includes discussion of:

- Key System Characteristics Enabling Trustworthiness
- Distinguishing Aspects of Securing the Industrial Internet of Things
- Managing Risk
- Permeation of Trust in the IIoT System Lifecycle
- Protecting Endpoints
- Protecting Communications
- Security Monitoring and Analysis
- Security Configuration and Management
- Industrial Security Standards

[2] This description is taken directly from the proposal (prop.tb.011).

[3] This description is taken directly from the proposal (prop.tb.020).

- C2M2

And more! (No Ginsu knives though.)

OTHER WORK

The IIRA included discussion of key system characteristics, such as safety and security, and crosscutting concerns, such as connectivity. However, that discussion was high level and brief. Security, for example, deserves considerable elaboration; hence the IISF.

Accordingly, we are in the process of breaking the IIRA into several parts, so that common information ("What is the Industrial Internet?" for example) can be found in one place, and creating separate documents covering each of these topics and themes in more detail. The Security Framework is one of those.

We are hopeful that Connectivity will be next, followed by Safety. With these document structures, more work can take place in parallel, fleshing out each of these areas as needed by IIC members.

Things are coming together. ™