The quarterly members meeting held in Reston, Virginia, USA March 23 - 26, 2015 marked two notable milestones for the Industrial Internet Consortium. First, the Industrial Internet Consortium had its one-year anniversary. Having started on March 27, 2014 with just five members, one year later the Consortium had 153 member organizations headquartered in 23 countries, and is still growing.

The second milestone was the review of the Consortium's first technical deliverable, the *Industrial Internet Reference Architecture*. The draft was issued in two parts prior to the meeting. During working sessions in Reston, the document underwent intensive review by all concerned. Since the meeting, all the comments, issues, new text and objections were taken into account, and the final document was published on April 24, one hectic month later. The Industrial Internet Consortium is happy to report that the document passed unanimously. Most of this note describes, at a high level, the contents of that reference architecture and ends with a quick look at other deliverables.

STRUCTURE OF THE REFERENCE ARCHITECTURE

The Industrial Internet Reference Architecture (henceforth 'IIRA') is divided into three parts. The first is a set of "Key System Characteristics" to which a system must adhere, such as upholding privacy expectations, reliability, scalability, usability, maintainability, portability and composability.

The second part is a set of "viewpoints" that enables discussion from different perspectives, such as the business, system usage, functional components and implementation.

The third part is a set of concerns that span the system as a whole. These relate back to the key system characteristics.

KEY SYSTEM CHARACTERISTICS

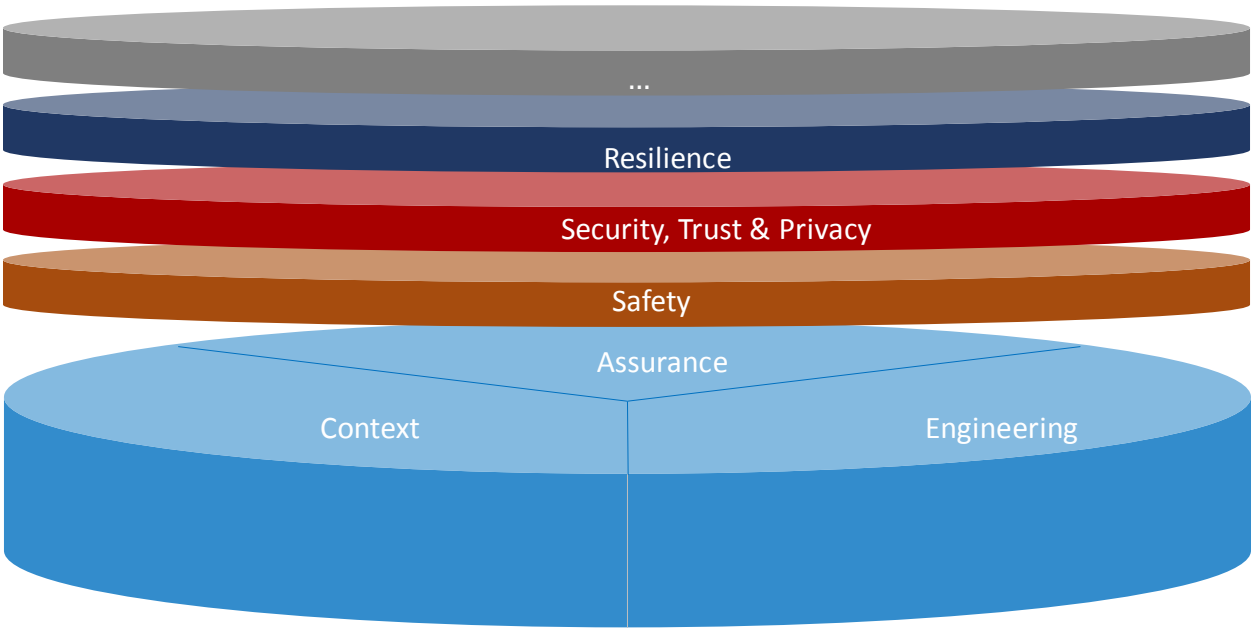
The key system characteristics of the Industrial Internet are addressed in three parts. First, there is a *context* into which the system must fit. Second, there is the actual *engineering* of the system, from conception through implementation. Third is the *assurance* that the system performs as it claims. This includes, obviously, testing and validation, but it also includes demonstrations of compliance and engineering processes.

On top of these are multiple key system characteristics, shown as layers. Of these, three are key to the discussion of Industrial Internet systems because of their criticality in ensuring the core functions, rather than the efficiency, of these functions, of the system:

Safety: the condition of the system operating without causing unacceptable risk of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.

Security: the condition of the system operating without allowing unintended or unauthorized access, change or destruction of the system or the data and information it encompasses.

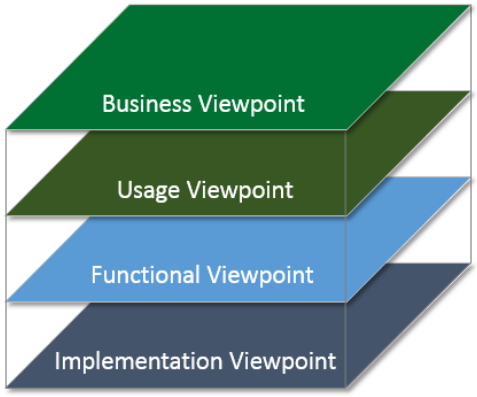
Resilience: the condition of the system being able to avoid, absorb and/or manage dynamic adversarial conditions while completing assigned mission(s), and to reconstitute operational capabilities after casualties.



VIEWPOINTS

Having multiple stakeholders involved, each representing unique concerns, calls for a framework to classify the concerns into appropriate categories so that they can be evaluated and addressed systematically across the full lifecycle of the system.

The members of the Industrial Internet Consortium have defined an architecture framework that describes the conventions, principles and practices, based on ISO/IEC/IEEE 42010:2011, that facilitates evaluation, and systematic and effective resolution of stakeholder concerns, and guides communication about the IIRA.

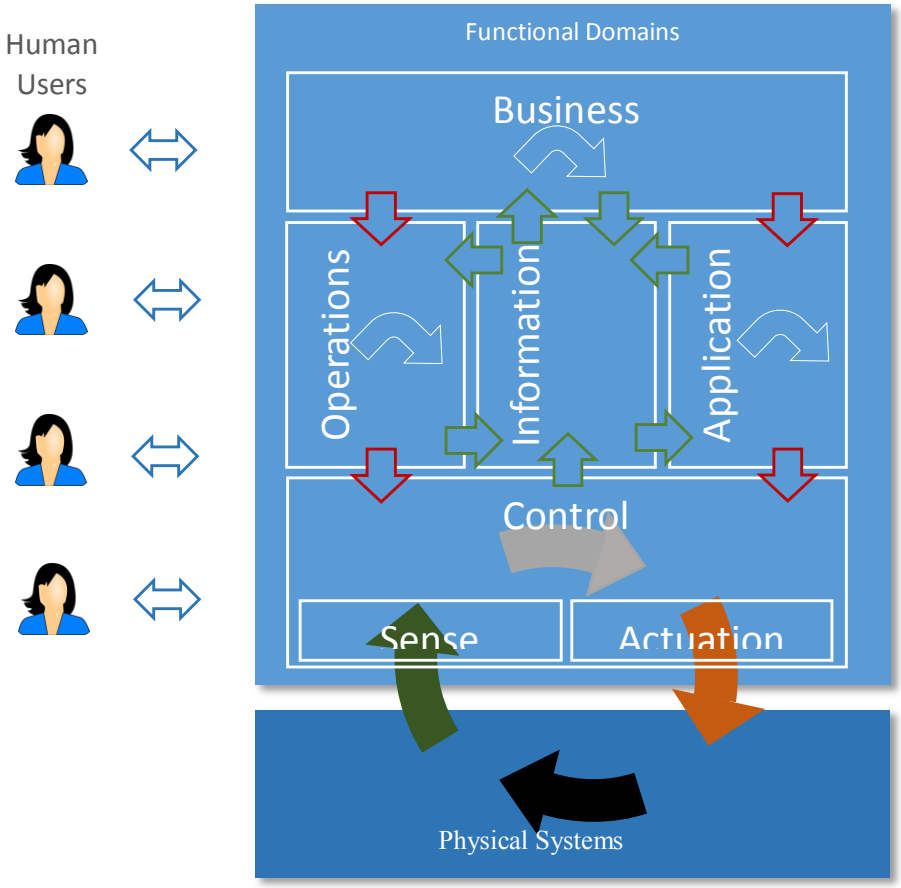


There are four main categories:

- The business viewpoint covers concerns related to the business (chiefly requirements)
- The usage viewpoint covers how the system is used by operators
- The functional viewpoint outlines the main functional blocks (about which, more below)
- The implementation viewpoint covers, unsurprisingly, implementation

The functional viewpoint contains the functional blocks that make up the system. An organization developing an Industrial Internet system may not use all the blocks, but should at least consider whether the functional blocks apply in their system.

The main functional blocks look like this:



Green Arrows: Data/Information Flows; Grey/White Arrows: Decision Flows; Red Arrows: Command/Request Flows

KEY SYSTEM CONCERNS

Key system concerns are common concerns that cannot be assigned to a particular viewpoint or functional domain, such as the key system characteristics described previously. Addressing these concerns requires consistent analysis across the viewpoints and concerted system behaviors among the functional domains and components, ensured by engineering processes and assurance programs.

For some of these concerns, key elements were summarized based on prevailing and matured technologies and practices most relevant to Industrial Internet Systems (IISs). In others, forward-looking ideas were introduced to bridge what is in place now and what is needed in the near future to support the kind of IISs the Consortium envisions. These topics are:

- Safety
- Security, Trust & Privacy
- Resilience
- Integrability, Interoperability and Composability
- Connectivity
- Analytics
- Intelligent and Resilient Control
- Dynamic Composability and Automatic Integration

Each topic is treated broadly, rather than deeply, and it is the intent of the IIC Members to elaborate on them as separate deliverables.

NEXT STEPS

Once approved by the Steering Committee, the Industrial Internet Consortium Technology Working Group can deliver the IIRA to member companies and established liaison partners. Although the document has been reviewed extensively, there will be necessary corrections, and a second version will be released.

The next step, however, is to build deliverables that identify existing standards and technologies, organize them, and then identify gaps between what the standards address and what is now needed for an Industrial Internet system. From those gaps, the Industrial Internet Consortium can write requirements for standards to fill those gaps and send them to expert organizations that can build such standards.

OTHER DELIVERABLES

Security and privacy, of course, are an integral part of the Industrial Internet Reference Architecture, but these are deep topics that will be considered separately. The Security Working Group is hard at work to produce a document that parallels the IIRA. This document is scheduled for review later this year.

The Vocabulary Task Group has produced a glossary of all the terms used in the IIRA.

The Use Case team is reviewing more use cases, and it has delivered a simplified use case template that helps to reveal architectural concerns.

The Safety and Data Management teams are presently defining their next deliverables.

On the Testbed front, the Industrial Internet Consortium Steering Committee has approved the sixth IIC testbed. Two of these testbeds have now been announced externally.

Track & Trace Testbed: The goal of this Smart Factory testbed is to manage handheld power tools in manufacturing and maintenance environments. This involves tracking and tracing the usage of these tools to ensure their proper use, prevent their misuse and collect data on their status. This testbed is led by Industrial Internet Consortium members Bosch, Tech Mahindra, Cisco, and National Instruments.

Communication and Control Testbed: This energy testbed re-architects the power grid system into a series of distributed microgrids that control smaller areas and support load, generation, and storage. Microgrids will operate independently from the main grid but will still interact with existing infrastructure. This testbed introduces the flexibility of real-time analytics and control to increase efficiencies in the legacy process of traditional power grids, ensuring that power is generated more accurately and reliably. This testbed is led by Industrial Internet Consortium members Real Time Innovations (RTI), National Instruments, and Cisco.

The Marketing Working Group delivered a series of Industrial Internet in Action case studies and Voices of the IIC videos in the first quarter, which helped to broaden external awareness of industry transformation that is happening today. In the next quarter, this group is focusing on the Industrial Internet in the Energy industry.

Information about these deliverables will be made available at www.iiconsortium.org and to the general Industrial Internet Consortium membership at its July meeting, to be held at GE Global Research headquarters in Niskayuna, New York.

Next year promises to have many more deliverables to report!

ABOUT THE INDUSTRIAL INTERNET CONSORTIUM

The Industrial Internet Consortium is an open membership organization with over 160 members from 23 countries, formed to accelerate the development, adoption, and widespread use of interconnected machines and devices, intelligent analytics, and people at work. 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. Visit www.iiconsortium.org.