Progress Report: Industrial Internet Security Framework

The Industrial Internet Consortium (IIC) has always been international in scope and currently counts some 250 members from 30 countries. The latest meeting in Tokyo, Japan in early June. As usual, there were many meetings over the three days for the various working groups providing members with many ways to interact.

This note starts with the *Industrial Internet Security Framework* (IISF), which was released to our liaisons for review in two parts. The first part, released in late April, covered the background and the business viewpoint. The second part was released in late May. Member companies and our liaisons worked hard to provide comments for consideration at the meeting.

Industrial Internet Security Framework

The entire document is available for review by members, but for others, here is a flavor of the product of the Security Working Group, led by Sven Schrecker (Intel), Hamed Soroush (Real-Time Innovations Inc (RTI)) and Jesus Molina (Fujitsu).

The first part covers motivation, distinguishing aspects of Industrial Internet of Things (IIoT) systems, and the all-encompassing notion of *trustworthiness*. IIoT systems differ from information technology (IT) systems and operational technology (OT) systems, not only in the blending of the two technologies, but also their cultures. While 'security' to an IT specialist conjures up firewalls, viruses and worms, to an OT expert, working perhaps in a chemical plant manufacturing deuterium, it connotes clearances, barbed wire and armed guards. While these can be simply combined, they sometimes conflict. Perhaps the best person to fix an IT security problem is a pimply teenager with a criminal record for hacking. Try selling that to the FBI (US), MI6 (UK) or the Ministry of State Security (China)!

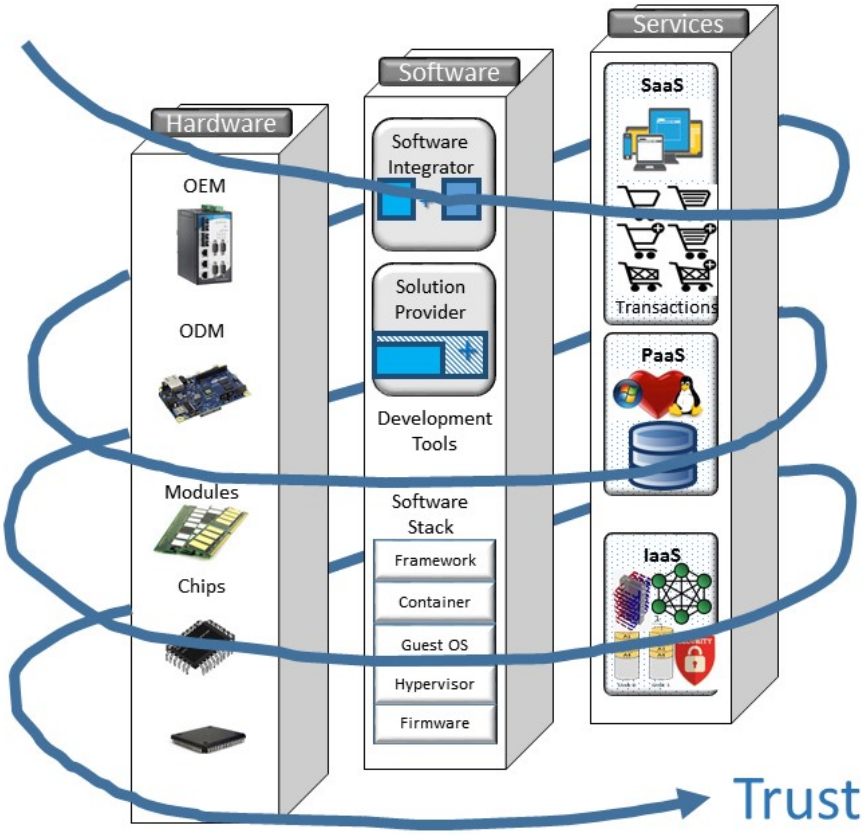
In general, trustworthiness entails the reconciliation of multiple key system characteristics, each of which has different importance to the different cultures and in different systems. These characteristics are:

- security,
- privacy,
- resilience,
- reliability and
- safety.

The IISF explains how these characteristics are interdependent and how to reconcile them into the overarching property trustworthiness.

Part II, the Business Viewpoint, describes risk, assessments, threats, metrics and performance indicators. All of these serve business management in protecting their organizations—and we, the public—from potential security breaches that could be disastrous. IT security problems that we read about in the press are serious, of course, but potential damage to the environment (and therefore to people) requires signal attention to trustworthiness from management, not just when the system is deployed but throughout its lifetime, all the way to decommissioning.

IIoT systems comprise components from many sources; they are not built entirely in-house. Trustworthiness permeates through all of these components from the owner/operator to component manufacturers and the system integrators in between.

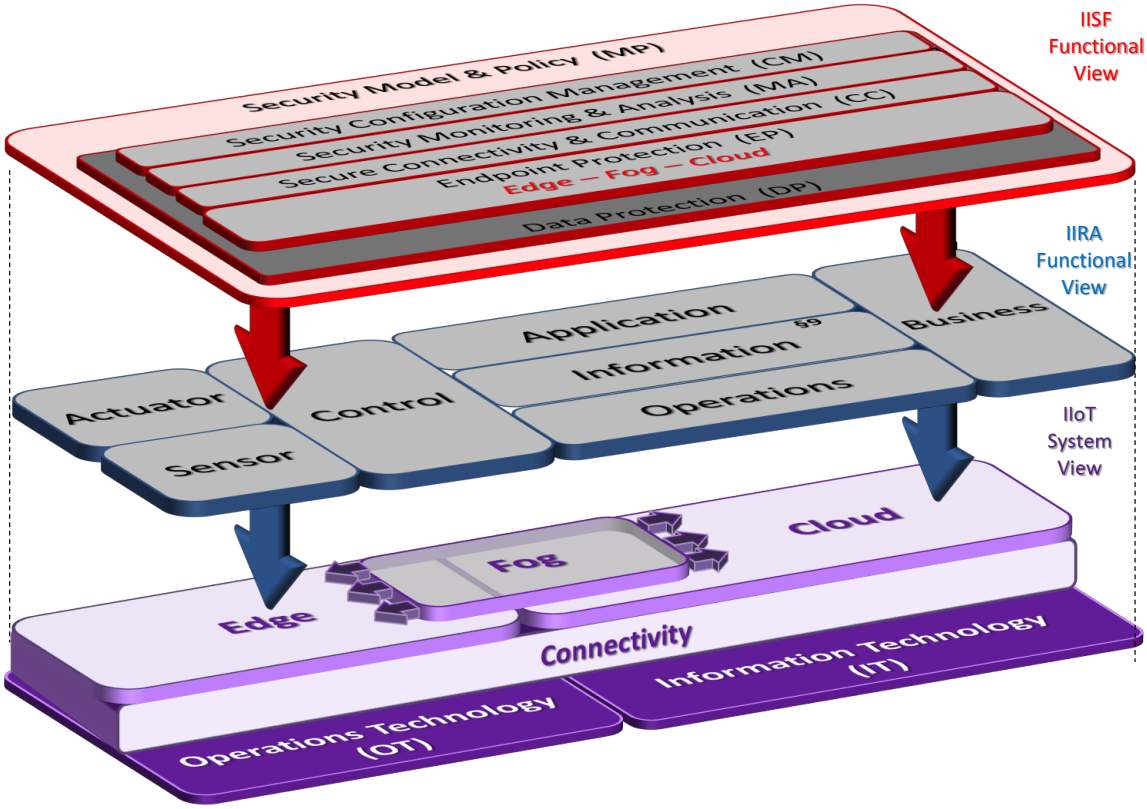


Each of these roles must guarantee trust to other roles, and those roles cannot take such assurances for granted. Assurance entails technology, of course, but it also includes documentation that captures precisely how that technology was deployed and how trustworthiness was rooted in the technology and the processes that created it.

All this is of Brobdingnagian importance to the public and the businesses that serve us, but what really gets the technologists going is the functional and implementation viewpoints that implement security. That security must not be bolted on to the architecture of the IIoT system;

it must be a fundamental part of it. However, security takes a different point of view from the architecture, thinking instead of protecting endpoints, communications, the fog and the cloud.

This is illustrated colorfully below.



The details cover a hundred or so pages, and they are still under review. (Two weeks is not enough to be thorough—which is a necessity in such systems). We hope the document will be released to the public by the time of our next quarterly meeting in Germany, in September.

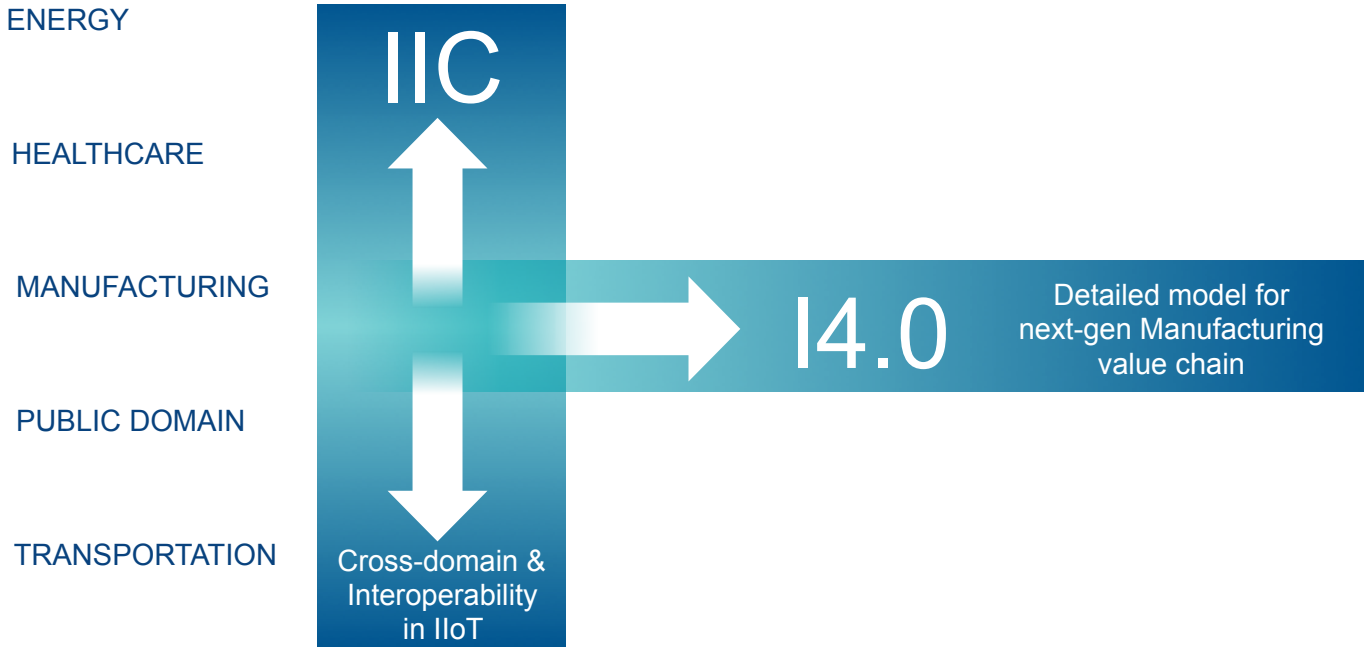
INDUSTRIE 4.0

IIC concerns itself above all with interoperability, especially across vertical market segments. Manufactured components exist in all those segments and Industrie 4.0 defines RAMI 4.0, a reference architecture for manufacturing. IIoT systems using the IIC's Industrial Internet Reference Architecture must therefore interoperate with those built based on RAMI. Both organizations recognize this and we have been working together for some months now. Our most recent meeting was in mid-May, where we identified six "joint task groups", one for security, another for alignment and a third to consider joint testbeds, for it is there that the rubber meets the code. Testbeds demonstrate conclusively what works together and what does not.

A fourth joint task group is defining ways to consolidate requirements from testbeds and our joint work. The goal is to provide requirements, from an IIoT perspective, to standards

development organizations. Obviously, it helps to work together, to reduce the effort and resolve differences in terminology and intent before the requirements are sent out.

We shall continue this work over the (Northern) summer and in Germany in September.



The Industrial Internet Interoperability Coalition

This spirit of cooperation continues with another subject discussed at length in Tokyo: the *Industrial Internet Interoperability Coalition (*I^{3}C). This proposed coalition is not a new organization, but a set of working relationships with IIC liaison organizations, and intends to orchestrate complex and partially competing protocols, open-source and standards on multiple levels, including device integration, gateway technologies, short-range wireless communication, long-range wireless communication, messaging, event processing, data management, analytics, cloud operations, and so on. Vertical and domain-specific standards also play an important role.

An integration of these standards and technologies to solve interoperability problems in a defined set of verticals, use cases and architecture patterns often applies in other parts of the IIoT landscape. I^{3}C provides a mechanism where multiple interoperability hotspots can be grouped into clusters that bring together a coalition of standardization organizations, open-source organizations, special interest groups and IIoT technology providers.

In addition to these activities and the work carried out with governmental initiatives, IoT Acceleration Consortium, Robot Revolution Initiative and the Industrial Value-Chain Initiative in Japan and Internet+ and China 2025 in China while we were in Asia, we continue to work with:

- Germany: Plattform Industrie 4.0
- France: Alliance Industrie du Futur

- European Commission: Alliance for Internet of Things Innovation
- United States: Cyber Physical Systems Public Working Group

OTHER WORK

Other groups were busy at work too. We spent more than a day on testbeds, including another testbed approved (to be announced shortly). The Security Working Group, of course, was hard at work reviewing comments from member companies and liaisons. The Vocabulary Task Group is busy reading the IISF to ensure all terms have a definition.

The Business Strategy and Solutions Lifecycle Working Group has several deliverables in train. The Industrial Internet Reference Architecture Alignment and Lifecycle Template, for example, comprises three tools that support three correlated objectives. First to assess how well a system description is aligned with the IIRA; second, to serve as an IIoT system design tool; and third to support uniform, common description of IIoT systems. These tools act as guideline for IIRA practitioners and make the IIRA more actionable or easily applicable.

Another is gamification of the *IIoT Solution Assessment* toolkit (a structured questionnaire to help you understand the risks of an IIoT project) and a paper on business strategy.

A third effort in this group is the Business Strategy for the IIoT, led by Jim Morrish of Machina Research. The purpose of this document is to identify and analyze the key issues that an enterprise needs to address to exploit Industrial IoT concepts for commercial (or other) gain.

We plan also to publish a document on Connectivity, fleshing out that portion of the Industrial Internet Reference Architecture. This effort is led by Dr. Rajive Joshi, Real-Time Innovations Inc. (RTI).

Yes, things are coming together!™
