Why We Build Testbeds: First Results

Everyone knows that factories, even factories that make manufacturing tools, use tools from many vendors. But who knows whether the tools will interoperate? And report their positions correctly and precisely? Or whether standards meet the needs of new applications and provide the capabilities needed for the tools to perform as expected? No one. Until now.

The Industrial Internet Consortium (IIC) is beginning to answer these questions, and others that arise in industrial operations from smart factories to smart grids, as a result of its testbed program. Testbeds provide platforms to think through innovations and test new applications, processes, products, services and business models to ascertain their usefulness and viability before taking them to market. They uncover the technologies, techniques and opportunities essential to solving these and other important problems that benefit businesses and society.

The goal of the IIC is to accelerate the adoption of the industrial internet and so transform the global economy. The Industrial Internet of Things (IIoT) ecosystem must be similarly comprehensive, with guidance on interoperability, security, connectivity, business models, standards, architectures and patterns that must all be firmly rooted in reality. This is why the testbed program is the primary focus of the IIC and its members. The outcomes from testbeds are the cornerstones of a feedback loop from concept to reality and back to guidance for further innovation. This is why, although member companies sponsor and own their testbeds, they also agree to share certain deliverables and progress reports with IIC members and the greater ecosystem.

This report, delivered as we reflect on our astounding growth from two to twenty-six testbeds, describes some specific results from several testbeds and draws some tentative conclusions across multiple testbeds in the program.

Testbed Initiation

A systematic, yet flexible, proposal and execution process governs testbeds. It begins with an innovative idea and a proposal to identify testbed concepts, goals, value, potential partners and commercial viability. Each proposal must include at least:

A business case: Testbeds should target applications with potential to deliver a practical path to substantial economic impact on a global scale. The goal is to ensure the testbed is of interest to a significant section of the IIC community, either by its ability to address current business issues, or by its ability to generate future revenues.

Relevance to IIoT frameworks: The testbed should have some relationship to IIoT frameworks. The goal is for the testbed to help us understand what works and what doesn't, so we can correct the frameworks and extend them to help members develop IIoT systems more rapidly.

A security review: Each testbed is reviewed to "ensure security is considered in every testbed". The purpose is to build security in to a *secure* industrial internet, and not bolt it on afterwards.

Deliverables: The proposal should identify tangible deliverables. The goal is to feed what is learned back to the sponsoring companies and the IIC. Results include technologies, best practices requirements for standards the testbed itself, which can then be taken into production to generate value and further innovations.

Each proposal is reviewed carefully to ensure it meets these criteria. Once the criteria are met, security understood, and the testbed proposal reviewed, it is put forward for approval.

TESTBEDS

The testbed program currently comprises twenty-six approved testbeds. Some of these testbeds were approved only last month and will take some time to implement, but some are fully deployed and have produced tangible results. Others are in between.

To communicate the results from fully deployed testbeds, we have conducted a series of interviews and published them in the IIC Journal of Innovation (JoI). Testbeds are in multiple industries and each is trying to achieve unique results in different ways. Consequently, the results obtained so far are wide ranging (or, to use the technical term, "all over the place"). We summarize these publicized testbeds below, and recommend you read the JoI testbed articles to gain context of each testbed and so understand the results more completely.

We present "results snippets" from testbeds that are underway in sidebars.

Track and Trace Testbed

The Track and Trace Testbed was the first testbed approved by the IIC. The testbed focuses on optimizing several key performance indicators for industrial use cases. The initial focus was on tracing process tools. The testbed team deployed specialized sensors that provided information about the location of tools and assets in use. The testbed team expanded from process tools to logistics equipment, specifically to forklifts. The expansion resulted in the deployment of two

use cases: the *Tracing Process Tools Use Case* deployed by Bosch in its industrial tools sector, and the *Tracking Forklift Use Case* deployed in Traunreut, in Bavaria.

Results: The team identified standardization opportunities in localization-technology interfaces, tightening-tool interfaces, enterprise-system interfaces, data models, data communications and device management. One goal of the testbed team was to identify reusable interfaces that would open the testbed to solution components from different vendors. The team created a layered model to depict the standards stack and correlation of tools and assets being tracked with corresponding enterprise systems, but no established standards were evident that satisfied the interfaces described in the model.

The IIC maintains active liaison relationships with standards-development organizations such as the Object Management Group (OMG), a natural liaison since the IIC is a program of the OMG. The purpose of these relationships is to pass standards recommendations to those bodies and reduce duplication of effort to ensure that new standards and technologies necessary to enable the industrial internet are brought to market more rapidly. We can identify and work with the standardization bodies that can create standards to satisfy these interfaces.

Time-Sensitive Networking Testbed

Time-Sensitive Networking (TSN) enhances Ethernet to bring more deterministic capabilities to the network, including time synchronization, sending scheduled traffic flows, and central, automated system configuration. This testbed applies TSN technology in a manufacturing system with a wide range of automation and control vendors to display its capabilities and value.

There are two fixed TSN Testbed locations; one is hosted at the National Instruments (NI) headquarters in their Industrial IoT Lab in Austin, Texas, USA and the second at the Bosch Rexroth development site for IoT-related control and communication solutions in Erbach, Germany.

The Manufacturing Quality Management Testbed

The Manufacturing Quality Management (MQM) Testbed is a joint effort by Huawei, Haier, CAICT, and China Telecom to establish a repeatable process, with manufacturing quality as the measure, to retrofit outdated factories applying modern sensory networks and analytic technologies. The initial success was shown through the welding section of the air conditioner production line in Haier's factory. Prior to the process, the quality control was based on the noise detection by an experienced examiner.

Results snippets:

- In March, the optimized noise detection analytic engine was proven to help reduce the false detection rate by 45%.
- In June, the analytic engine for noise detection was integrated into the production line, the accuracy of pass/fail detection was dramatically improved.
- The testbed is based on IIC's reference architecture with a deep learning analytic engine to carry on the noise detection task.
- The team is working with other IIC members to provide software means to model the process graphically and to show the whole scheme can be represented in a systematic fashion.

Results: By vetting technical standards and the interoperability required in smart manufacturing, the testbed team has advanced its goal of achieving real-time control and synchronization of high-performance machines over a single, standard Ethernet network, supporting multi-vendor interoperability and integration. The TSN testbed has deployed early-phase usage of enhancements to Ethernet standards and is influencing standards IEEE 802.1 and IEEE 802. This will improve those standards and make the use of TSN more prevalent in industries where it can improve efficiency, such as in manufacturing and energy. Multiple technical issues have been raised, and then passed on to Avnu, an organization developing interoperability and certification ecosystems for applications meeting precise timing and low latency requirements using open standards. Through Avnu, the work is channeled back into IEEE. Many IIC members participate in both organizations, easing the information flow.

Communication and Control for Microgrid Applications Testbed

A microgrid comprises local power generation and consumption that can be physically isolated from the rest of the power grid. A microgrid is typically deployed for a large campus (for example, college and corporate campuses, large hospitals, large factory sites and residential communities) and operated by the owners of these properties, commercial operators or utilities. Local power generation is often from renewable energy sources, such as wind and solar, and as such is highly variable. Clouds, for example, can reduce the solar generation level very quickly. Rapid monitoring, coordination and control are required to manage loads, storage and local and remote power generation enabling the microgrid to deliver power seamlessly.

The Communication and Control for Microgrid Applications Testbed simulates a smart grid microcosm demonstrating many technologies and protocols: Data Distribution Service (DDS), Open Field Message Bus (OFMB) and how they can be combined and deployed in the field. The testbed proves the viability of a real-time and securely distributed control architecture for real world microgrid applications, and offers access to new technologies, such as TSN, for testing.

Results: The Industrial Internet Reference Architecture (IIRA) informs the construction of IIoT systems including testbeds. During conception, the business viewpoint helps to sharpen the business purpose of the system; at implementation time, “patterns” help developers to get started. This testbed applied an IIRA pattern (the three-tier architecture pattern), by implementing a variation (a layered databus architecture pattern) and ended with a different pattern (a three-tier architecture that allows for federating multiple data buses on top of one another into multiple tiers). This gibberish has meaning and value for systems developers. It is

quicker to start with a pattern and then modify it than it is to start with the proverbial "blank sheet". Our library of patterns, with advice on when to use which one, accelerates project development. We have added this new pattern, and will add others as testbeds discover, apply and test them.

In addition, the Microgrid testbed is contributing to the power industry standard (Open FMB) and it is using the OpenFMB standard in the testbed. The IIC has a liaison with Smart Grid Interoperability Platform (SGIP), and the SGIP are using the Industrial Internet Security Framework (IISF) to shape the security model in the OpenFMB standard.

INFINITE Testbed

INFINITE (INternational Future INdustrial Internet TEstbed) is an innovation platform designed to accelerate the development of industrial internet products and services. INFINITE uses software-defined networking to create virtual domains so that multiple virtual domains can run securely on a single physical network. This makes it ideal for mission critical systems.

Results: The team has identified business benefits, new business models and organizational transformations aiding IIoT adoption in the following use cases:

Bluelight enabled intelligent route planning for ambulances to improve response times, leading to better pre-hospital emergency care experiences and outcomes for patients. The insights from this use case will drive improvements in resilience and flexibility for ambulance services.

First responder improves the safety and effectiveness of first responders when involved in an emergency situation, especially those in harsh environments. Data is analyzed to monitor worker health and enable a fast response to ensure their safety.

SPARKS detects anomalies or fraudulent behavior within the power grid. Machine-learning algorithms detect anomalies in the power grid. They can also be applied to monitoring other types of Operational Technology (OT)—the physical plant that makes up the industrial base.

The Condition Monitoring and Predictive Maintenance (CM/PM) Testbed

In today's increasingly competitive global economy, production and operations efficiency can often be the difference between generating a profit or a loss. National Instruments' online real-time asset monitoring systems combined with IBM's advanced machine learning and analytics can provide the necessary insight into the health of critical assets, resulting in increased production, reduced downtime, and higher production output.

Leveraging advanced sensors that go beyond vibration (Motor Current Signature Analysis and Thermography), it automatically predicts equipment failure and notifies a person or system so that pro-active steps can be taken to avoid equipment damage and unscheduled downtime.

The CM/PM Testbed deployed a real-world installation of the proposed solution at NI headquarters in Austin, Texas. It demonstrates how to make older assets smart, collecting asset health data from four pump/motor skids used to pump chilled water for an HVAC system and helping maintenance and reliability engineers to be more effective and efficient in their roles.

The *flood event advisory service* applies data analytics in a flood zone. This use case is not fully deployed but the testbed team anticipates greater efficiencies through the automation of manual processes and improved accuracy of flood prediction events leading to a better-informed public.

General Results

Security

The security review poses the same questions to each testbed. This regularity—derived from the IISF—allows us to formalize data collection on security-design choices in each testbed and match them to requirements derived from use cases and verticals. In the security review, each testbed describes its:

- architecture and how it relates to the IIRA,
- threat model (STRIDE IoT[1] has been the preferred tool),
- security use cases,
- constraints derived from other characteristics that affect security decisions (e.g. privacy, reliability, resiliency and safety) and
- security design choices.

As the security review questionnaire focuses on security design choices (e.g. identity or implementation of root-of-trust), early results across multiple testbeds suggest that initial designs do not adequately implement edge security protections or describe how to protect the edge-to-cloud link. So far, mitigation techniques generally reside in a networked device (gateway or firewall). The questionnaire needs to evolve to understand the mitigation techniques implemented by testbeds because security claims for these devices, such as providing identity and protection for edge devices, are often not substantiated.

It is unclear at this stage whether this is a general problem ("we don't have a collection of patterns to secure the edge") or a prioritization problem ("it's only a testbed—we'll worry about that later").

The cloud system usually bears the responsibility for the whole of network security, including Information Technology (IT) and OT. While the IT network-security threats are well understood,

[1] STRIDE IoT is a security analysis tool based on the STRIDE threat classification model developed by Microsoft, more information at https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-architecture.

initial results suggest the OT, or edge, security controls require additional evaluation without a strong dependence on IT-centric security solutions. Additional security controls are needed to create adequate security profiles for each testbed. To investigate that, we expect future questionnaires to evaluate, in detail, security controls and their orchestration at the edge.

Standards

TSN is an enhancement of Ethernet. There are multiple technical findings coming from the TSN Testbed that will affect standards IEEE 802.1 and IEEE 802.3. The IIC is gathering these together and working with those certification and standards-development organizations, such as Avnu and IEEE.

The Track and Trace Testbed team faces the challenge of finding a standards-based solution to multi-vendor device interoperability. One of the partners has an internal data model used to address the immediate problem, but a standard will speed adoption. The Track and Trace team are exploring options with the OMG, which has a Manufacturing Technology and Industrial Systems Domain Taskforce that could develop a standard to meet this need. An open-source implementation from, say, the Eclipse Foundation would bring it to market more quickly.

Beyond such standards, there is value to be gained from understanding (and standardizing) common operations from wildly different devices, such as the movement of robot arms and autonomous vehicles. They both observe acceleration profiles governing their acceleration and movement; one in three dimensions, the other in two. Standards across vertical domains will foster further innovation, enabling what the World Economic Forum calls the autonomous, pull economy.

Best Practices

The Business Strategy and Innovation Framework proposes centers of excellence to accumulate data and spread knowledge about internal projects. At this early stage of the industrial internet, it is best practice to collect data to see what it can teach us. The security review process, for example,

The Smart Factory Web Testbed

The Smart Factory Web (SFW) Testbed aims to network a web of smart factories to improve order fulfillment by aligning capacity across production sites with flexible adaptation of production capabilities and sharing of resources, assets and inventory. The usage scenario ‘Order-driven adaptive production’ is being specified and implemented for several constellations of networked and collaborating factories. The four model factories of Korea Electronics Technology Institute (KETI) and Fraunhofer IOSB are the initial baseline in the Smart Factory Web and allow for extensive experimentation.

Results snippets:

- Factories and their assets can be registered and searched for in the SFW portal.
- A central theme is Plug & Work, a method using the IEC standards OPC UA and AutomationML to insert (“plug”) assets into a factory and for the factory to automatically recognize and (re-)commence operations (“work”).
- AutomationML is applied with data communication over OPC UA to achieve semantic interoperability and is applied to exchange information between engineering tools, to model assets, to describe the capabilities of assets and to describe the information model of an asset.

provides a consistent mechanism for collecting information, supports transparent reasoning about the security profile, and enables the data collection that led to the security observations above that will change how we build security into IIoT systems. (Of course, it also involved security experts who raised critical questions concerning the design considerations and controls necessary to deliver the desired level of security in the testbed!)

The lesson we learned from this data collection is that having a structure for data collection—even if we're not sure that the data we collect is the right data—informs the next round of projects. The security data may be directly useful, or it may not. If not, we can change it. It would be helpful to share that knowledge throughout the IIoT ecosystem and even standardize the data collected, once we know more.

Further data collection (about architectural patterns, standards in use, or connectivity, for example) might reveal further observations, such as new architectural patterns, or enable the creation of concerted standards'-requirements efforts or new approaches to connectivity.

We can see several areas where we need to collect further information:

- functionality of the security of network devices,
- cloud security controls,
- data management,
- analytics,
- connectivity choices and
- security use cases

We have begun work on the latter two. We won't get results unless we collect the data!

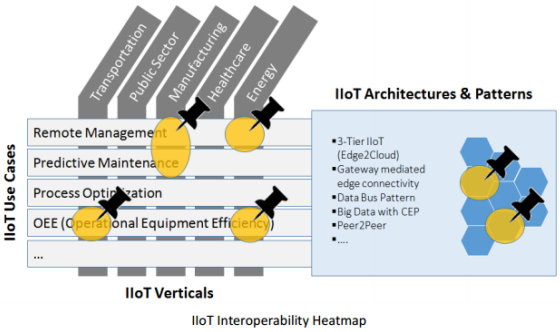
The Industrial Internet Interoperability Coalition

The IIC testbed program is producing testbeds that are influencing industries through the deployment of innovative solutions, validating and influencing standards, creating and extending ecosystems and leveraging liaison relationships.

IIC membership aids in ecosystem development and testbed partnering as evidenced by the reported results of growth in team participation and involvement of partners satisfying critical needs in testbed capabilities. But this is not enough. We need to go global.

No single organization can address all the industrial internet's challenges. This is why the IIC is launching the *Industrial Internet Interoperability Coalition* (I^3C). The goal of I^3C is to identify interoperability hotspots that require special attention and identify the use cases, architectures and patterns associated with those hotspots. I^3C will bring partners together to address clusters of interoperability hotspots with an integrative, holistic perspective, using our results and frameworks.

The I[3]C portal will allow other organizations to access testbed results, use cases, architecture patterns and best practices, and contribute to them. We plan to display participants (i.e., standards bodies, individual contacts) and invite participation in the challenge of addressing interoperability hotspots.



IIoT Interoperability Heatmap

The IIC will develop the I[3]C results further, looking for hotspots, needs, patterns and so on, and it will progressively update its frameworks for use by the ecosystem. As our testbeds continue to mature, so will our testbed results collection, expanding in width, breadth and structure as the feedback loop between our testbed program, standards-development organizations and I[3]C evolves.

There is also room for improving testbed results reporting. In the current set of results the careful reader will observe inconsistencies with how results are reported and in what categories. Gaining consensus around a common model of result categorization, with agreement about consistent usage, will aid in understanding and analyzing results and with drawing inferences from across testbeds, and will feed into I[3]C and the IIoT ecosystem.

Similarly, with standards reporting, there is little information about the specifics of what aspect of an existing standard is being affected, and in what way, or about what action is being taken to create a new standard. One might conclude that the information is not provided because the topic is too detailed and complex to be described succinctly. It may be useful to record the standards needs and involvement from across testbeds to help assure that the needs are being fulfilled in the most effective way. We must work to prevent silos of information.

The disciplined approach taken to testbed formation, security evaluation and execution helps to assure that testbeds have an opportunity to thrive and achieve their goals. Improvements in data collection, organizing results, and presenting results, use cases, architectures and patterns via the I[3]C portal will further the impact of testbeds and their results. The IIC and its members are leading the way. The question is, who will be left behind?

CONTRIBUTORS

In addition to the results described here, each testbed team forms an ecosystem. No one company can own the platform (because there are so many) and no one company can supply all of the components needed. It is that realization that led to the formation of OMG's IIC program in March 2014. To avoid having the credits roll for another ten pages (and probably miss a key contributor), we have chosen to list only the people directly involved in writing up the results.

Testbed results and descriptions have been referenced from IIC JoI articles and in some instances have been included verbatim. Our thanks to the authors of those papers.

Testbed Proposal Process: Brett Murphy, RTI; Jacques Durand, Fujitsu; Mike Mossbarger, ENT Foundation; Joseph Fontaine, IIC.

Track and Trace Testbed: Bosch, Cisco, SAP SE and TechMahindra. *Interviewees*: Michael Dietz (SAP SE), Andreas Mueller (Robert Bosch GmbH) Dirk Slama (Bosch Software Innovations); Interviewer, Joseph Fontaine, IIC.

TSN Testbed: Analog Devices, Belden and Hirschmann, Bosch Rexroth, B&R Industrial Automation, Cisco, Intel, Hilscher, Kalycito, KUKA, NI, Renesas Electronics, Schneider Electric, SICK AG, TTTech and Xilinx. Contributors: Paul Didier (Cisco Systems Inc) and Joseph Fontaine (IIC).

INFINITE Testbed: Asavie, Cork Institute of Technology, and DELL Technologies. Contributors: Donagh Buckley (Dell EMC Research Europe), Joseph Fontaine (IIC) and John O'Sullivan (Cork Institute of Technology (CIT).

Microgrid Testbed: Cisco, NI and RTI. *Interviewee*: Brett Burger (NI), Interviewer: Joseph Fontaine (IIC).

MQM Testbed: Huawei, Haier, CAICT, and China Telecom. MQM Contributors: Mitch Tseng (Huawei).

SFW Testbed: Fraunhofer IOSB, Korea Electronics Technology Institute (KETI) Contributor: Kym Watson (Fraunhofer IOSB).

Condition Monitoring and Predictive Maintenance (CM/PM) Testbed: IBM, National Instruments, SparkCognition. Contributors: Roberto Piacentini (NI), Sky Matthews (IBM).

Security Data Collection: Jesus Molina (Waterfall Security Solutions LTD).

The Industrial Internet Consortium is the world's leading organization 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.

IIC members gain experience they never could 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 and find the sought-after expertise.
- Information & News—A fast pass to newsworthy industry developments.
- Competitive edge—Stay ahead of the competition by taking advantage of industry changes and developments that might otherwise have passed you by.
- Create a market—Join a collective voice supporting the single mission of creating disruption in the market and developing 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 careers and meet mentors, mentees and career prospects.
- Solve important problems—while assisting partners and customers.
- Events – Capitalize on opportunities for continuous exposure to industry developments.