Trustworthiness

The Industrial Internet Consortium's (IIC) second-quarter member meeting, held virtually from June 14th ~ 17th, was another success with:

- 178 attendees,
- 31 working sessions,
- three testbed sessions,
- five plenary sessions,
- seven industry track sessions,
- a two-hour smart manufacturing use case/proof of concept workshop and
- a joint half-day Smart Manufacturing Workshop with Global Industry Organizations with 63 attendees.

The meeting profiled two published papers. First, the *MILS Architectural Approach Supporting Trustworthiness of the IIoT Solutions* whitepaper, published back in March during our Q1 member meeting. This paper describes the details of the MILS architectural approach, which has emerged as a strategy for cost-effective construction of systems requiring dependability with high assurance.

The *Global Industry Standards for Industrial IoT* white paper published on 2021-06-02 provides an overview of how standards facilitate IIoT technological integration via a common language of interoperability, IT and OT convergence, compliance to avoid vendor lock-in, adherence to regulatory safety security and reporting and portability of employee skills.

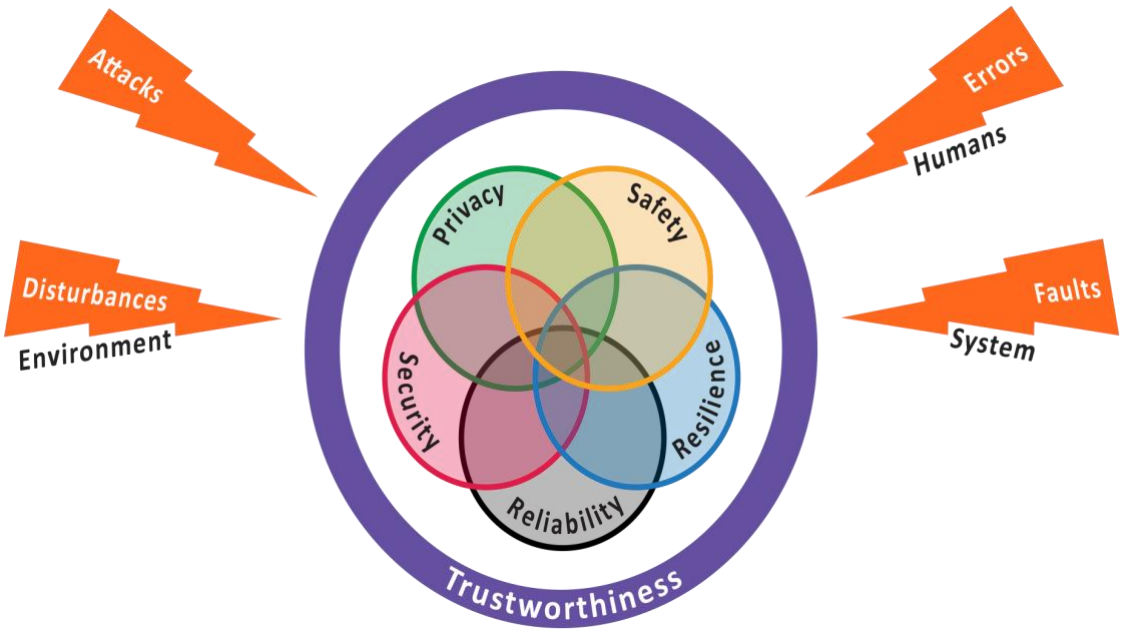
Finishing touches were put to another flagship document, the *IIoT Trustworthiness Framework Foundations*.

TRUSTWORTHINESS

The *Industrial Internet Reference Architecture* designated five *key system characteristics* to support a system's business purpose and to ensure that functions perform adequately without compromise. This was taken up in the *Industrial Internet Security Framework* technical report, leading to their combination into a single property: *trustworthiness*.

> *"Trustworthiness* is the degree of confidence one has that the system performs as expected. Characteristics include safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks."

Contemporaneously, the National Institute of Science and Technology (US) also introduced the term based on the same characteristics.



In addition to the trustworthiness characteristics, IIC also specified four groups of threats that endanger a trustworthy system: environmental disturbances, attacks, human errors and system faults. Threats can result in hazards that can lead to loss, which we wish to avoid.

Especially in industrial internet of things (IIoT) systems. This motivates further development of the concepts, especially as IIoT systems are connected to other systems that potentially were built with different trustworthiness requirements. Connected systems introduce risks to each other, so a single system cannot effectively be trusted until the other systems to which it is connected are also trusted.

The well-known “Jeep Hack” provides a vivid example of failures of trust in aggregated systems. This hack allowed near-total remote control of an ordinary consumer vehicle, a 2015 Jeep Cherokee. It illustrates how alignment of assumptions about the operational context is necessary across the different components from the supply chain. Specifically, the entertainment system, which was connected to the Jeep’s network via Bluetooth, was insecure, enabling the attack.

The early attacks were based on a hack to the diagnostic system that does not allow changes to be made above 5 mph (8 kph). The tire pressure monitoring system was the source of the information about the speed of the vehicle, and it was spoofed to tell the car that it was going slowly. This was possible because the protocol for the bus discarded duplicate messages. Once they knew how to get illegitimate message numbers onto the bus—before the actual tire pressure monitoring systems message—through a spoof attack, they could go at highway speeds.

This example shows how one untrustworthy system in an otherwise trustworthy solution can render all connected systems untrustworthy. It is essential that all systems connected to other systems be trustworthy. Otherwise, a failure of trust in one can bring down the others and result in a failure across all the connected systems.

As connecting systems, and particularly previously isolated control systems, to the internet and each other is key to the "industrial internet", getting trustworthiness right is a *sine qua non*.

This has been brought into sharp focus recently with the Colonial Pipeline ransomware attack. The Colonial pipeline delivers gasoline and jet fuel to the eastern United States. Although this attack did not affect the operational technology of the pipeline, which could have been environmentally disastrous, it did make billing the end customer impossible. There were also fears that, having been compromised, a further attack on the physical operation of the pipeline was possible. After paying a ransom, the system was restored within five days.

Another, less well-known attack took systems down for four weeks. This was another ransomware attack, this time on the Scripps Institute, a healthcare provider in the San Diego, California area. Patient records, including sensitive health information, were compromised. Appointments for surgery and tests had to be made "by hand", relying on paper records.

Trustworthiness is key. The Trustworthiness Foundation outlines several principles, as follows:

Principle 1: Trustworthiness characteristics must be considered holistically.

Principle 2: Understanding context is necessary for making Trustworthiness tradeoffs.

Principle 3: Organizational consistency over time enables reputation and trust.

Principle 4: Accountability is an essential underlying foundation of trustworthiness.

Principle 5: A culture of trustworthiness is essential to achieving trustworthiness.

Principle 6: Assurance based on evidence is essential to establish trustworthiness.

Principle 7: Software trustworthiness must be managed throughout the entire software lifecycle.

Principle 8: Implementing trustworthiness means implementing trustworthiness methods.

Principle 9: Maintaining change and audit records is necessary for trustworthiness.

Principle 10: A trustworthiness framework must enable timely business decisions.

Principle 11: Assurance requires a systems viewpoint with evidence of multiple factors.

Note, in particular, principle 8. The first challenge of implementing trustworthiness in system design is that none of the trustworthiness characteristics can be implemented separately and they cannot be simply combined: The characteristics may support or block each other; their combination results in new challenges.

The solution is to take the system design away from the trustworthiness characteristics to *methods* that are assigned to the system characteristics. A *trustworthiness method* is a component, tool, technology, software application, operational procedure or management directive that is assigned to at least one trustworthiness characteristic.

Examples of trustworthiness methods are:

- *Fire extinguisher*: a tool and a trustworthiness safety method.
- *CO_2 fire suppression system:* a tool and a trustworthiness resilience method (the purpose is to protect the system, not the environment or humans; CO_2 is dangerous to people).
- *Windmill restart:* operational procedure for airplanes during an engine flameout and a trustworthiness resilience method.
- *Encryption of all social security numbers on servers*: management directive and a trustworthiness privacy method.

The framework also provides ways to think about how the state of the system can be changed by applying the trustworthiness methods.

The trustworthiness framework:

- is flexible to include metrics as appropriate to the target context and audience,
- is stateful to allow accounting for both the history of the system and the current information about its trustworthiness,
- supports hierarchical decomposition to evaluate the effects of trustworthiness in different layers of the system and
- facilitates a simple visualization with relevant information.

The model also quantifies performance of the system in many operational areas, some of which may be unique to the system under consideration. A rating for each of these areas can be defined and used to track performance. These ratings can be aggregated and used as the basis for a single numerical value of trust: the *trust rating.*

Finally, note the importance of assurance, in principles 6 and 11, and throughout the system. Industrial systems are built from multiple components from multiple suppliers and any one of them may be untrustworthy. You need evidence that each of them is indeed trustworthy. A single component can bring down a complete system, and with it *your business*.

INDUSTRY PROGRAM

The Business Deployment Accelerator, the heart of our industry program, has several parts:

- IIC Testbeds are where the innovation and opportunities of the industrial internet–new technologies, new applications, new products, new services, new processes, new business can be initiated, thought through and rigorously tested to ascertain their usefulness and viability before coming to market. The OTA Go Kart Automotive and Over the Air Update (OTA) testbed was recently added to our testbed program so far comprising 27 approved IIC testbeds.
- IIC Test Drives are solutions that may be deployed as pilots to trial a technology. Test drives enable technology end users to learn about a technology in their facilities. Five test drives are approved; most recently the Valuable Asset Tracking for Healthcare test drive.

- IoT Challenges aim at solving real problems and validating solutions that address specific end-user-identified pain points. In these challenges, architects and solution providers compete to design industrial internet solutions that address high-profile real-world problems.

These three parts are simply formalized mechanisms to deliver digital transformation to industry. To do that, IIC members need to understand what changes technology end users wish to make. The IIC's Business Pain Point Collection initiative seeks to identify and understand business and industry pain points so our ecosystem may expedite business and industry guidance and solutions. We encourage everyone—members, liaison partners, non-member end users—to contribute to this collection. IIC will endeavor to identify digital transformation enablers that address the pain points so they may be deployed. Quickly.

Our Industry Leadership Councils (ILCs) are executive roundtables of innovative strategists representing organizations who meet regularly to set the vision for next-generation solutions in their respective industries. The Manufacturing ILC produced the first in a series of technical briefs aimed at help manufacturing leaders keep pace with rapid emergence of new technology. The ILC meets quarterly and includes representatives from major companies; additional end user companies are welcome. The general criteria for participation in an ILC are a director-level role or higher as well as actively implementing or using an IIoT solution in the corresponding field.

The IIC also seeks to form an Energy ILC, focused on utilities and distributed energy management. If you have recommendations for who might participate you may visit the ILC webpage above or contact either Howard Kradjel or Cheryl Rocheleau.

Our vertical task groups exist to understand business and technology needs within an industry. They connect industry needs to requirements, testbeds, and guidance that enable technology deployment and digital transformation. We have vertical groups for automotive, energy, healthcare, mining, and smart factory.

Our Special Interest Groups create customer-validated requirements for the development of holistic solutions for industry, initiate technical validation projects for these requirements, initiate new industry standards to help harmonize the technology landscape and provide an efficient platform for vendors suppliers and industry organizations to shape the future of IIoT solutions jointly. For more information please contact Stephen Mellor.

The Product Catalog encourages members to add products to the catalog, so that the public can shop for members' products. The Community Forum is an online venue for industry experts to exchange ideas, discuss IIoT problems and network as well as an IIoT beacon providing helpful, relevant content to technology users, vendors, integrators, technology experts, researchers, government entities and academicians. The Community Forum is a resource for follow-on conversations and webinars.

Other Group Activity

The IIC launched the Patterns Initiative on 2021-05-27 that aims to crowdsource, review, revise and publish a library of high-quality and well-reasoned patterns for use across industries.

The *Journal of Innovation* published its latest edition on *Applying Solutions at the Distributed Edge* on 2021-06-24. This edition addresses such topics as key criteria to move cloud workloads to the edge, heterogeneous computing at the edge and how to enable mission critical execution of distributing manufacturing processes on the edge.

A complete list of IIC publications can be found here.

Webinars

Visit our Webinars Webpage for access to one IIC-hosted and three liaison syndicated webinars this past quarter as well as a comprehensive list of past and future webinars.

New Members

Please welcome new members this quarter:

- GNARBOX
- prcvd.ai
- Prescient Devices, Inc.
- Sinergia Software
- Threatspan BV

IIC members gain experience they could never have as a non-member. Here are some key benefits of membership:

- ***Networking***—Make the connections; find the needed expertise.
- ***Information & News***—A fast pass to newsworthy industry developments.
- ***Competitive edge***—Stay ahead of the competition or take advantage of changes and developments that might otherwise have passed you by.
- ***Create a market***—Join a collective voice supporting a single mission; create the disruption in the market and develop the business opportunities.
- ***Establish a vision*** –Members work to define future architectures and innovate technologies for IIoT.
- ***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 your career, meet mentors and mentees, career prospects.
- ***Solve important problems—***and help your partners and customers.
- ***Events*** – Capitalize on opportunities for continuous exposure to industry