The Safe, Secure and Reliable Industrial Internet: A Standards Story

March 2017
Industrial Internet Consortium (IIC)

Mission
To be a global, member supported, organization that promotes the accelerated growth of the Industrial Internet of Things (IIoT) by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data using common architectures, interoperability and open standards to deliver transformational business and societal outcomes across industries and public infrastructure.

Launched in March 2014 – now over 270 members

The IIC is an open, neutral “sandbox” where industry, academia and government meet to collaborate, innovate and enable.
Collaboration within the Industrial Internet Consortium

IIC Working Groups have individual charters, inter-related outcomes both within the Working Groups and with external organizations.
Definition: The Industrial Internet of Things (IIoT)

"An Industrial Internet of Things (IIoT) system connects and integrates control systems with enterprise systems, business processes, and analytics. An IIoT system enables significant advances in optimizing decision-making, operations, and collaborations among a large number of increasingly autonomous control systems. Insights gained through the IIoT technologies will provide new business outcomes and will likely disrupt many existing business practices.

IIoT technology is useful for all industry and infrastructure, from manufacturing to utilities, healthcare, financial services, and telecommunications. Because of the nature of the assets connected to the Industrial Internet, IIoT systems must be designed to be secure, reliable and resilient to insure safety, business innovation, and public trust."
The IIC Addresses Ecosystems
The IIC Addresses All Kinds of Networks and Connectivity
The IIC Addresses IIoT Systems in Numerous Sectors & Verticals

<table>
<thead>
<tr>
<th>agriculture</th>
<th>building</th>
<th>consumer &amp; home</th>
<th>defense/aerospace</th>
<th>energy</th>
<th>healthcare</th>
<th>manufacturing</th>
<th>public sector</th>
<th>public security &amp; safety</th>
<th>transportation</th>
</tr>
</thead>
<tbody>
<tr>
<td>farming</td>
<td>building/ construction</td>
<td>consumer products</td>
<td>defense</td>
<td>energy</td>
<td>connected medical devices</td>
<td>factory</td>
<td>education</td>
<td>public safety</td>
<td>mobility</td>
</tr>
<tr>
<td>ranching</td>
<td>smart home</td>
<td>home products</td>
<td>military</td>
<td>utilities</td>
<td>hospitals</td>
<td>industrial automation</td>
<td>environment</td>
<td>public security</td>
<td>transportation</td>
</tr>
<tr>
<td>fishing</td>
<td>office</td>
<td>cooking (commercial)</td>
<td>aerospace</td>
<td>mining</td>
<td>medical offices</td>
<td>smart products</td>
<td>water</td>
<td>surveillance</td>
<td>public transportation</td>
</tr>
<tr>
<td>weather</td>
<td>building security</td>
<td>entertainment</td>
<td>oil and gas</td>
<td>pharmacies</td>
<td>transportation</td>
<td>disaster prevention</td>
<td>vehicle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>building</td>
<td>maintenance</td>
<td>phone &amp; network services</td>
<td>smart grid</td>
<td>medical therapy</td>
<td>waste management</td>
<td>civil administration</td>
<td>law enforcement/ police</td>
<td>traffic infrastructure</td>
<td>logistics</td>
</tr>
<tr>
<td>sporting events</td>
<td>home healthcare</td>
<td>disease diagnosis</td>
<td>continuous patient monitoring</td>
<td>clinical trials</td>
<td>emergency and crisis response</td>
<td>military</td>
<td>freight management pipelines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>travel</td>
<td>tourism</td>
<td>continuous patient monitoring</td>
<td>clinical trials</td>
<td>assisted care</td>
<td>dentistry</td>
<td>shipping</td>
<td>aeronautics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Collaboration within the Industrial Internet Consortium

IIC Working Groups have individual charters, inter-related outcomes both within the Working Groups and with external organizations.
Viewpoints – Chapter 6 – Functional Viewpoint

Human Users

Functional Domains

Business

Operations

Information

Application

Control

Sense

Actuation

Physical Systems

© 2017 IIC. All rights reserved, used with permission.

Approved for Public Release; Distribution Unlimited. Case Number 16-4794
Relevant Business, Usage, Functional, & Implementation Standards

OMG Business Process Model and Notation (BPMN) Standard
OMG Unified Modeling Language (UML) Standard
OMG System Modeling Language (SysML) Standard
Knowledge Discovery Metamodel (KDM) - ISO/IEC 19506 & OMG KDM
OMG Unified Architecture Framework Standard
OMG Unified Component Model for Standard
OMG Interaction Flow Modelling Language (IFML)
OMG Data-Distribution Service for Real-Time Systems (DDS) Standard
Collaboration within the Industrial Internet Consortium

IIC Working Groups have individual charters, inter-related outcomes both within the Working Groups and with external organizations.
The IIC is *not* a standards organization. It evaluates and organizes existing standards to:

- Advocate for open standard technologies
- Influence the global standards development

The Technology Working Group is currently:

- Evaluating existing standards
- Identifying requirements for the Industrial Internet
CONVERGENCE OF INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY

Information Technology (IT)

Operational Technology (OT)

IloT

IloT System

© 2017 MITRE. All rights reserved, all other material used with permission.
Need Secure, Safe, Reliable, and Resilient Behavior that Upholds Privacy Expectations

Cyber Risk is Expanding into Physical Risk

- Loss of information or service
- Loss of reliability or safety
- Loss of life or property

“Back office” → Production
Key System Characteristics Enabling Trustworthiness

- ISO Assurance Case Standard
- OMG Structured Assurance Case Metamodel Standard
- Open Group Dependability through Assurance Standard

© 2017 MITRE. All rights reserved, all other material used with permission.
CONVERGENCE OF IT AND OT TRUSTWORTHINESS

Information Technology (IT)

IIoT

Operational Technology (OT)
TRUSTWORTHY SYSTEMS
The Key System Characteristics of Trustworthiness as a Quality Measure

- Industrial IoT Quality is a continuum of system characteristics
  - OT Safety (IEC 62443*) meets IT Security (ISO 27000*)
  - Privacy (GDPR*), Resilience (ISO*, IEC*), Reliability (NIS*) are quality features in both OT and IT
  - Determine and ensure quality measures per vertical, e.g. audit, certification

* Examples
Composition of a Trustworthiness Quality Measure

**Resilience**
- EU: NIS
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog NIS

**Reliability**
- EU: NIS
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog NIS

**Security**
- EU: GDPR
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog GDPR

**Privacy**
- EU: GDPR
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog GDPR

**Safety**
- EU: IEC 61508/62626
- UK: … (after Brexit)
- US: IEC 61508
- CN: ()
- JP: IEC 61508

* Examples
Capturing of Complicated Claims-Evidence Relationships
OMG Structured Assurance Case MetaModel

Exchange and Composition of Assurance Cases between tools and programs
Evidence of Trustworthiness as Assurance Cases

**Resilience***
- EU: NIS
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog NIS

**Reliability***
- EU: GDPR
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog GDPR

**Security***
- Evidence-based Assurance Case supporting Reliability claims
- Evidence-based Assurance Case supporting Security claims

**Privacy***
- EU: IEC 61508/62626
- UK: … (after Brexit)
- US: IEC 61508
- CN: ()
- JP: IEC 61508

**Safety***
- EU: NIS
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog NIS
ALIGNMENT OF THE SECURITY FRAMEWORK, REFERENCE ARCHITECTURE VIEWS

IISF Security Framework

IIIRA Functional View

IIoT System View

© 2017 IIC. All rights reserved, used with permission.

Approved for Public Release; Distribution Unlimited. Case Number 16-4794
THREAT AND VULNERABILITIES TO IIoT ENDPOINTS

- Development Environment
- Security Model & Policy
- Configuration Management
- Monitoring & Analysis
- Endpoint Data

Deployment Environment
- Native OS Apps/API
- Runtime Env
- Containers

Boot
- Bare Metal Apps
- Guest OS or RTOS

UEFI BIOS
- Processor
- Memory
- Peripherals
Relevant Trustworthiness Assurance Standards

- OMG Structured Assurance Case Metamodel (SACM) Standard 2.0
- OMG Dependability Assurance Framework for Safety-Sensitive Consumer Devices (DAF)
- Open Group Dependability through Assurance Standard
- OMG Threat & Risk Model RFP
- OMG Cyber Risk Assessment Framework (CRAF) Metamodel RFC
- Safety and Reliability for UML RFP
- OMG Automated Source Code Maintainability Measure Standard (ASCMM)
- OMG Automated Source Code Performance Efficiency Measure Standard (ASCPEM)
- OMG Automated Source Code Reliability Measure Standard (ASCRM)
- OMG Automated Source Code Security Measure Standard (ASCSEM)
- ITU-T Common Vulnerabilities and Exposures (X.1520 – CVE)
- ITU-T Common Vulnerabilities Scoring System (X.1521 – CVSS)
- ITU-T Common Weakness Enumeration (X.1524 – CWE)
- ITU-T Common Weakness Scoring System (X.1525 – CWSS)
- Extensible Configuration Checklist Description Format (XCCDF) ISO/IEC 18180:2013
Collaboration within the Industrial Internet Consortium

IIC Working Groups have individual charters, inter-related outcomes both within the Working Groups and with external organizations.
Approved Testbed Portfolio

25 Approved Testbeds

INFINITE: Dell EMC
CM & PM: IBM, NI, SparkCognition
Connected Care: Infosys, GE, PTC, RTI, MD PnP
Track & Trace: Bosch, Tech Mahindra, Cisco, SAP
Factory Operations Visibility & Intelligence: Fujitsu, Cisco
Smart Manufacturing Connectivity: TE Connectivity, SAP
Smart Asset Outage Management: Genpact, GE, NI
Smart Energy Management: Infosys, Schneider Electric, PTC
Connected Vehicle Urban Traffic Mgmt: Infosys, RTI, Bosch, Microsoft
Intelligent Urban Water Supply: Water & Process Group, Thingswise, CAICT
Smart Airline Baggage Management: GE, M2Mi, Oracle, Boeing, Infosys
Factory Automation Platform as a Service: Hitachi, Mitsubishi Electric, Intel
Asset Efficiency: Infosys, PTC, Bosch, Intel, GE, IBM, NI, Foghorn, KUKA
Security Claims Evaluation: Xilinx, UL, Aicas, RTI, Infineon, GMO GlobalSign
Smart Supply Chain: Manufacturing: TCS, Cisco, Siemens, Oracle, Infineon, Tego
Manufacturing Quality Management: Huawei, Haier Group, China Telecom, CAICT
Time Sensitive Networks: Cisco, Bosch, GE, KUKA, NI, TTTech, Intel, Schneider Electric, B&R, Innovasic
Smart Water Management: Infosys, GE, EMC, Cisco

Edge Intelligence: HP, RTI
High-Speed Network: GE
Microgrid: TRI, NI, Cisco, IBM
Industrial Digital Thread: Infosys, GE
Precision Crop Management: Infosys
Smart Factory Web: KETI, Fraunhofer IOSB
Deep Learning Facility: Toshiba, Dell EMC

© 2017 MITRE. All rights reserved, all other material used with permission.
Approved Testbed Portfolio
Collaboration within the Industrial Internet Consortium

IIC Working Groups have individual charters, inter-related outcomes both within the Working Groups and with external organizations.
The IIC has three primary areas of activity: Community Engagement, Technology & Security, and Testbeds.
270+ Member Organizations