



# **The Industrial Internet of Things Vocabulary Technical Report**

Version 2.2

November 6, 2019

Copyright © 2019, Industrial Internet Consortium, a program of Object Management Group, Inc. (“OMG”).

## ACKNOWLEDGEMENTS

This document is a work product of the Industrial Internet Consortium Vocabulary Task Group in the Technology Working Group, co-chaired by Erin Bournival (Dell EMC) and Robert Martin (MITRE).

### EDITORS

Marcellus Buchheit (Wibu-Systems), Erin Bournival (Dell EMC)

### AUTHORS

The following persons contributed substantial written content to this document:

Erin Bournival (Dell EMC), Eric Simmon (NIST), Marcellus Buchheit (Wibu-Systems), Claude Baudoin (cébé IT & Knowledge Management), Frederick Hirsch (Fujitsu), Birgit Boss (Robert Bosch GmbH), Will Sobel (VIMANA), Anish Karmarkar (Oracle), Rajive Joshi (RTI), Sven Schrecker (Intel), Shi-Wan Lin (Thingwise), Jesus Molina (Waterfall Security), Tom Rutt (Fujitsu), Bradford Miller (GE), Jacques Durand (Fujitsu), Paul Didier (Cisco), Amine Chigani (GE), Reinier Torenbeek (RTI), David Duggal (EnterpriseWeb), Robert Martin (MITRE), Graham Bleakley (IBM), Andrew King (University Of Pennsylvania), Robert Lembree (Intel), Hamed Soroush (RTI), Jason Garbis (RSA), Mark Crawford (SAP), Eric Harper (ABB), Kaveri Raman (AT&T), Brian Witten (Symantec), Andrew Ginter (Waterfall Security) and David Meltzer (Tripwire).

### CONTRIBUTORS

The following persons contributed valuable ideas and feedback that significantly improved the content and quality of this document:

Peter van Schalkwyk (XM Pro), Nina Tucker (Twin Oaks Computing), Denise Wahl (OMG), Todd Edmunds (Cisco), Mitch Tseng (Huawei), Brett Murphy (RTI), Farooq Bari (AT&T), Tom Rutt (Fujitsu), Jack Weast (Intel), Lin Nease (HP), Ron Ambrosio (IBM), Omer Schneider (Cyber-X Labs), Pete MacKay (Wurldtech), Lance Dover (Micron).

### TECHNICAL EDITOR

Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Editors, Authors and Contributors into an integrated document.

## IIC ISSUE REPORTING

All IIC documents are subject to continuous review and improvement. As part of this process, we encourage readers to report any ambiguities, inconsistencies or inaccuracies they may find in this Document or other IIC materials by sending an email to [admin@iiconsortium.org](mailto:admin@iiconsortium.org).

## CONTENTS

---

<b>1 Principles</b> .....	<b>4</b>
<b>2 Conventions</b> .....	<b>4</b>
<b>3 Relationship with Other IIC Documents</b> .....	<b>4</b>
<b>4 Definitions of Terms</b> .....	<b>6</b>
<b>Annex A Revision History</b> .....	<b>23</b>
<b>Annex B Terms Change History</b> .....	<b>24</b>
<b>Annex C References</b> .....	<b>27</b>
<b>Authors and Legal Notice</b> .....	<b>31</b>
<b>Use of Information—Terms, Conditions and Notices</b> .....	<b>31</b>

## FIGURES

---

Figure 3-1: IIC Technical Publication Organization .....	5
--	---

## TABLES

---

Table 4-1: Defined Terms and Definitions .....	22
Table A-2: Revision History .....	23
Table B-3: Terms Change History.....	<b>Error! Bookmark not defined.</b>

This Industrial Internet Vocabulary Technical Report specifies a common set of definitions for terms that are considered relevant and important to the Industrial Internet of Things (IIoT) to be used by all IIC documentation.

Each of the terms listed in the first column of the table is rendered as a bookmark, which can be used for cross references in any document that imports this table.

Many of these definitions have been imported from other standards, as indicated in the *Source* column of these tables. IIC as a source indicates that this is a definition from IIC itself.

## 1 PRINCIPLES

---

We adhered to the following principles in this document:

- The definition of a term provides an in-place replacement for that term in a sentence.
- A term whose English dictionary definition is considered sufficient is not included.
- A new definition is created only when that term is not already defined in an existing specification or standard, such as ISO/IEC JTC 1 International Standard, or its definition is not appropriate for use in the Industrial Internet.
- In selecting appropriate references for existing terms, international standards are preferred over regional or national standards.

## 2 CONVENTIONS

---

When a definition uses another term that is defined in the vocabulary, that term is shown using the style term and is rendered as a hyperlinked cross reference to the definition of that term in the table. Specific notes in the table are using the <sup>(n)</sup> style and are described at the end of the table.

## 3 RELATIONSHIP WITH OTHER IIC DOCUMENTS

---

This document fits in the IIC Technical Publication Organization shown in Figure 3-1. This document does not have dependencies on other documents.

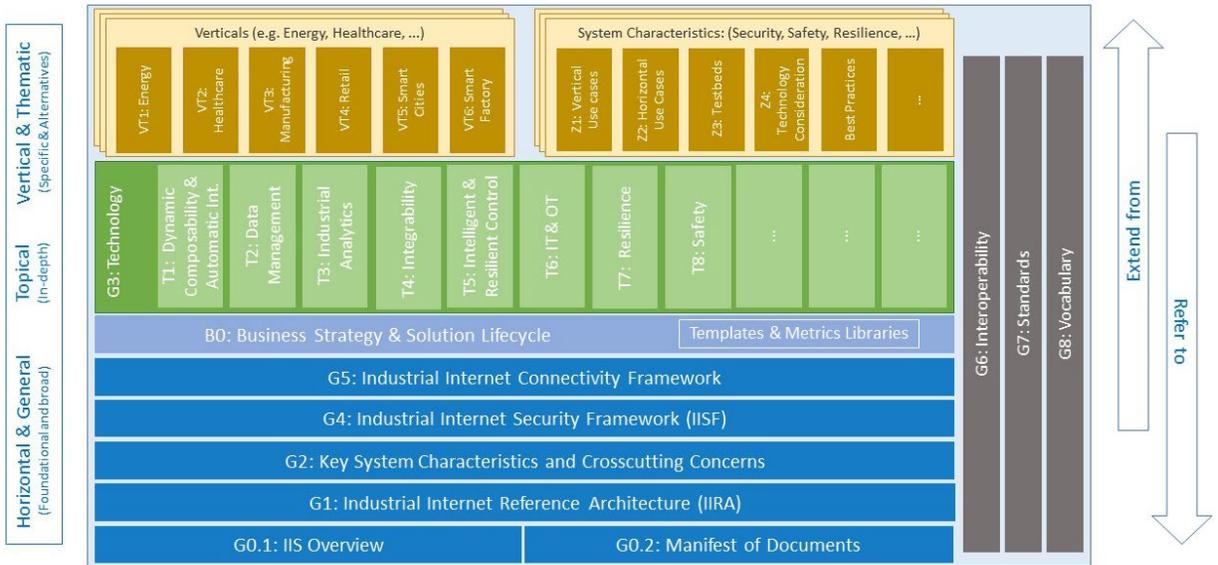


Figure 3-1: IIC Technical Publication Organization

## 4 DEFINITIONS OF TERMS

Term	Definition	Source
access control	means to ensure that access to <u>assets</u> is authorized and restricted based on business and <u>security</u> requirements <b>note:</b> access control requires both <u>authentication</u> and <u>authorization</u>	<u>ISO/IEC 27000:2016</u>
activity	specified coordination of <u>tasks</u> that are required to realize the system capabilities <b>note:</b> an activity may be composed of other activities	<u>ISO/IEC 17789:2014</u> <sup>(1)</sup>
analytics	synthesis of knowledge from <u>information</u>	<u>NIST Interagency Publication 8401-1</u>
application domain	<u>functional domain</u> for implementing application logic	IIC
architecture	fundamental concepts or properties of a system in its <u>environment</u> embodied in its <u>elements</u> , relationships, and in the principles of its design and evolution	<u>ISO/IEC/IEEE 42010:2011</u>
architecture description	work product used to express an <u>architecture</u>	<u>ISO/IEC/IEEE 42010:2011</u>
architecture framework	conventions, principles and practices for the description of <u>architectures</u> established within a specific domain of application and/or community of <u>stakeholders</u>	<u>ISO/IEC/IEEE 42010:2011</u>
architecture layer	logical partitioning of the <u>architecture</u>	IIC
architecture view	work product expressing the <u>architecture</u> of a system from the perspective of specific system <u>concerns</u>	<u>ISO/IEC/IEEE 42010:2011</u>
architecture viewpoint	work product establishing the conventions for the construction, interpretation and use of <u>architecture views</u> to frame specific system <u>concerns</u>	<u>ISO/IEC/IEEE 42010:2011</u>

Term	Definition	Source
asset	major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment or a logically related group of systems	<a href="#">NISTIR 7298, rev 2</a>
assurance	grounds for justified confidence that a claim has been or will be achieved	<a href="#">ISO/IEC 15026-1:2013</a>
attack surface	elements and interactions of a system that are vulnerable to attack	IIC
attack vector	path or means (e.g. viruses, e-mail attachment, web pages, etc.) by which an attacker can gain access to an entity	IIC
attacker	person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources	<a href="#">ISO/IEC 27033-1:2015</a>
attestation	issue of a statement, based on a decision that fulfillment of specified requirements has been demonstrated	<a href="#">ISO/IEC 29109-1:2009</a>
attribute	characteristic or property of an entity that can be used to describe its state, appearance or other aspects	<a href="#">ISO/IEC 24760-1:2011</a>
audit	independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures and to recommend necessary changes in controls, policies or procedures	<a href="#">NISTIR 7298, rev 2</a>
authenticated identity	identity information for an entity created to record the result of identity authentication	<a href="#">ISO/IEC 24760-1:2011</a>
authentication	provision of assurance that a claimed characteristic of an entity is correct	<a href="#">ISO/IEC 27000:2016</a>

Term	Definition	Source
authorization	granting of rights, which includes the granting of access based on access rights <b>note:</b> authorization results in <u>privileges</u> .	<u>ISO 7498-2:1989</u>
autonomy	ability of an intelligent system to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation	<u>IHMC</u>
availability	property of being accessible and usable upon demand by an authorized <u>entity</u>	<u>ISO/IEC 27000:2016</u>
brownfield	existing industrial system targeted for new functionality without operational disruptions	IIC
business impact analysis	<u>process</u> of analyzing operational functions and the effect that a disruption might have upon them	<u>ISO/IEC 27031:2011</u>
business viewpoint	<u>architecture viewpoint</u> that frames the vision, values and objectives of the business <u>stakeholders</u> in establishing an <u>industrial internet of things (IIoT) system</u> in its business and regulatory context	IIC
choreography	type of <u>composition</u> whose <u>elements</u> interact in a non-directed fashion with each autonomous part knowing and following an observable predefined pattern of behavior for the entire (global) composition <b>note 1:</b> choreography does not require complete or perfect knowledge of the pattern of behavior. <b>note 2:</b> see ISO/IEC 18384-3:2016, 8.3.	<u>ISO/IEC 18384-1</u>
cloud computing	paradigm for enabling <u>network</u> access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand <b>note:</b> examples of resources include servers, operating systems, networks, software, applications and storage equipment.	<u>ISO/IEC 17788:2014</u>

Term	Definition	Source
collaboration	type of <u>composition</u> whose <u>elements</u> interact in a non-directed fashion, each according to their own plans and purposes without a predefined pattern of behavior	<u>ISO/IEC 18384-1</u>
component	modular, deployable and replaceable part of a system that encapsulates implementation and exposes a set of <u>interfaces</u>	<u>ISO 14813-5:2010</u>
composability	ability of a <u>component</u> to interact with other components in recombinant fashion to satisfy requirements based on the expectation of the behaviors of the interacting parties	IIC
composition	result of assembling a collection of <u>elements</u> for a particular purpose	<u>ISO/IEC 18384-1</u>
concern	interest in a system relevant to one or more of its <u>stakeholders</u> <b>note:</b> a concern pertains to any influence on a system in its <u>environment</u> , including developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological and social influences.	<u>ISO/IEC/IEEE 42010:2011</u>
confidentiality	property that <u>information</u> is not made available or disclosed to unauthorized individuals, <u>entities</u> or <u>processes</u>	<u>ISO/IEC 27000:2016</u>
connectivity	ability of a system or application to communicate with other systems or applications via <u>network(s)</u>	IIC
connectivity endpoint	<u>interface</u> that provides <u>connectivity</u>	IIC
control domain	<u>functional domain</u> for implementing <u>industrial control systems</u>	IIC
countermeasure	action, device, procedure, technique or other measure that is designed to minimize	<u>ISO/IEC 2382:2015</u>
credential	evidence or testimonials that support a claim of <u>identity</u> or assertion of an <u>attribute</u> and usually are intended to be used more than once	<u>CNSSI 4009</u>

Term	Definition	Source
criticality	measure of the degree to which an organization depends on an <u>entity</u> for the success of a mission or of a business function	<u>NISTIR 7298, rev 2<sup>(1)</sup></u>
cross-cutting concern	<u>concern</u> that affects the whole system and thus may impact multiple viewpoints of the <u>architecture</u>	IIC
cross-cutting function	function that may be applied and realized across multiple <u>functional domains</u> of the <u>architecture</u> to address <u>cross-cutting concerns</u>	IIC
cryptography	discipline that embodies principles, means and mechanisms for the transformation of <u>data</u> in order to hide its <u>information</u> content, prevent its undetected modification and/or prevent its unauthorized use	<u>ISO/IEC 18014-2:2009</u>
data	content represented in a digital and formalized manner suitable for communication, storage, interpretation or processing	IIC, inspired by <u>ISO/IEC 2382:2015</u>
data at rest	stored <u>data</u> that is neither being processed nor transferred	IIC
data in motion	<u>data</u> being transferred from one location to another	<u>ISO/IEC 27040:2015</u>
data in use	<u>data</u> being processed	IIC
data integrity	property that <u>data</u> has not been altered or destroyed in an unauthorized manner	<u>ISO/IEC 27040:2015</u>
databus	<u>data</u> -centric <u>information</u> sharing technology that implements a virtual, global data space, where applications exchange data <b>note:</b> key characteristics of a databus are: <ul style="list-style-type: none"> <li>• the applications directly <u>interface</u> with the operational <u>data</u></li> <li>• the databus implementation interprets and selectively filters the <u>data</u>, and</li> </ul>	IIC

Term	Definition	Source
	<ul style="list-style-type: none"> <li>the database implementation imposes rules and manages quality of service (QoS) parameters, such as rate, <u>reliability</u> and <u>security</u> of <u>data</u> flow.</li> </ul>	
denial of service (DoS)	prevention of authorized access to resources or the delaying of time-critical operations	<u>ISO/IEC 27033-1:2015</u>
digital representation	<u>information</u> that represents <u>attributes</u> and behaviors of an <u>entity</u>	IIC
digital twin	<u>digital representation</u> , sufficient to meet the requirements of a set of use cases <b>note:</b> in this context, the entity in the definition of <u>digital representation</u> is typically an <u>asset</u> , <u>process</u> or system.	IIC
edge	boundary between the pertinent digital and <u>physical entities</u> , delineated by <u>IoT devices</u>	IIC
edge computing	distributed computing that is performed near the <u>edge</u> , where the nearness is determined by the system requirements	IIC
element	<u>entity</u> that is indivisible at a given level of abstraction and has a clearly defined boundary	<u>ISO/IEC 18384-1<sup>(1)</sup></u>
emergent behavior	behavior of a system realized by the interactions of its <u>components</u>	IIC
encryption	reversible operation by a cryptographic algorithm converting <u>data</u> into ciphertext so as to hide the <u>information</u> content of the data	<u>ISO/IEC 9798-1:2010</u>
endpoint	<u>component</u> that has computational capabilities and <u>network connectivity</u>	IIC
entity	item that has recognizably distinct existence <b>note:</b> e.g. a person, an organization, a device, a subsystem or a group of such items	<u>ISO/IEC 24760-1:2011<sup>(1)</sup></u>
environment	context determining the setting and circumstances of all interactions and influences with the system of interest	<u>ISO/IEC/IEEE 42010:2011<sup>(1)</sup></u>

Term	Definition	Source
	<b>note:</b> the environment of a system includes developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological and social influences.	
event	any observable occurrence in a system and/or <u>network</u>	<u>NIST SP 800-61</u>
functional component	functional building block needed to engage in an <u>activity</u> realized by an implementation	<u>ISO/IEC 17789:2014</u>
functional domain	collection of functions comprising a system	IIC
functional framework	set of abstract re-useable <u>functional components</u> that can be extended/customized and applied to several applications in a specific domain	IIC
functional viewpoint	<u>architecture viewpoint</u> that frames the <u>concerns</u> related to the functional capabilities and structure of <u>industrial internet of things (IIoT) system</u> and its <u>components</u>	IIC
greenfield	new industrial system without operational <u>disruption concerns</u>	IIC
identification	<u>process</u> of recognizing an <u>entity</u> in a particular <u>identity domain</u> as distinct from other entity	<u>ISO/IEC 24760-1:2011</u>
identifier	<u>identity information</u> that unambiguously distinguishes one <u>entity</u> from another one in a given <u>identity domain</u>	<u>ISO/IEC 24760-1:2011</u>
identity	inherent property of an instance that distinguishes it from all other instances	<u>ISO/IEC/IEEE 31320-2:2012</u>
identity authentication	formalized <u>process</u> of <u>identity verification</u> that, if successful, results in an <u>authenticated identity</u> for an <u>entity</u>	<u>ISO/IEC 24760-1:2011</u>
identity domain	<u>environment</u> where an <u>entity</u> can use a set of <u>attributes</u> for <u>identification</u> and other purposes	<u>ISO/IEC 24760-1:2011</u>
identity information	set of values of <u>attributes</u> optionally with any associated metadata in an <u>identity</u>	<u>ISO/IEC 24760-1:2011</u>

Term	Definition	Source
	<b>note:</b> in an <u>information and communication technology system</u> an <u>identity</u> is present as identity information.	
identity management	<u>processes</u> and policies involved in managing the lifecycle and value, type and optional metadata of <u>attributes</u> in <u>identity</u> known in a particular <u>identity domain</u>	ISO/IEC 24760-1:2011
identity verification	<u>process</u> to determine that presented <u>identity information</u> associated with a particular <u>entity</u> is applicable for the entity to be recognized in a particular <u>identity domain</u> at some point in time	ISO/IEC 24760-1:2011
implementation viewpoint	<u>architecture viewpoint</u> that frames the <u>concerns</u> related to implementing the capabilities and structure of an <u>industrial internet of things (IIoT) system</u>	IIC
incident response <i>or</i> intrusion response	action taken to protect and restore the normal operational conditions of <u>information systems</u> and the information stored in it when an attack or intrusion occurs	ISO/IEC 27039:2015
industrial control system (ICS)	combination of control <u>components</u> that act together to exercise control in the physical world	IIC
industrial internet	internet of things, machines, computers and people, enabling intelligent industrial operations using advanced <u>data analytics</u> for transformational business outcomes	IIC
industrial internet of things (IIoT) system	system that connects and integrates <u>industrial control systems</u> with enterprise systems, business <u>processes</u> and <u>analytics</u> <b>note 1:</b> <u>Industrial control systems</u> contain sensors and actuators. <b>note 2:</b> typically, these are large and complicated systems.	IIC
information	<u>data</u> that within a certain context has a particular meaning	IIC, inspired by ISO/IEC 2382:2015

Term	Definition	Source
information domain	<u>functional domain</u> for managing and processing <u>data</u>	IIC
information security incident	single or a series of unwanted or unexpected <u>information security events</u> that have a significant probability of compromising business operations and threatening information security	<u>ISO/IEC 27000:2016</u>
information security risk	potential that a given <u>threat</u> will exploit <u>vulnerabilities</u> of an <u>asset</u> or group of assets and thereby cause harm to the organization	<u>ISO/IEC 27005:2008</u>
information technology (IT)	entire spectrum of technologies for <u>information processing</u> , including software, hardware, communications technologies and related <u>services</u> <b>note:</b> Although information technology (IT) technologies are used in <u>operational technology (OT)</u> , information technology (IT) is traditionally considered to be distinct from operational technology (OT) due to a different set of requirements and <u>concerns</u>	<u>Gartner IT Glossary</u>
infrastructure service	<u>service</u> that is essential for any IoT implementation to work properly <b>note:</b> Infrastructure services provide support for essential features of the IoT.	<u>IOT-A</u>
integrity	property of accuracy and completeness	<u>ISO/IEC 27000:2016</u>
interface	named set of operations that characterize the behavior of an <u>entity</u>	<u>IOT-A</u>
interoperability	ability of two or more systems or applications to exchange <u>information</u> and to mutually use the information that has been exchanged	<u>ISO/IEC 17788:2014</u>
IoT actuator	<u>IoT device</u> that can change one or more properties of a <u>physical entity</u> in response to received <u>information</u>	IIC
IoT device	<u>endpoint</u> that interacts with the physical world through sensing or actuating	IIC

Term	Definition	Source
IoT sensor	<u>IoT device</u> that observes one or more properties of a <u>physical entity</u> and converts those properties into <u>information</u>	IIC
IT/OT convergence	<u>process</u> of interweaving <u>information technology (IT)</u> and <u>operational technology (OT)</u> in order to create <u>industrial internet of things (IIoT) systems</u>	IIC
least privilege	principle that a <u>security architecture</u> should be designed so that each <u>entity</u> is granted the minimum system resources and <u>authorizations</u> that the entity needs to perform its function	<u>NISTIR 7298, rev 2</u>
malware	malicious software designed specifically to damage or disrupt a system, attacking <u>confidentiality, integrity or availability</u>	<u>ISO/IEC 27040:2015</u>
man-in-the-middle attack	attack in which the <u>attacker</u> intercepts a communications flow between two entities, appearing to each <u>party</u> as the other, while being able to read and modify messages in the communications flow	IIC
multi-tenancy	allocation of physical or virtual resources such that multiple tenants and their computations and <u>data</u> are isolated from and inaccessible to one another	<u>ISO/IEC 17788:2014</u>
network	collection of communicating <u>endpoints</u>	IIC
non-functional requirement	requirement that defines the overall qualities or <u>attributes</u> of the resulting system  <b>note:</b> non-functional requirements place restrictions on the system being developed, the development process, and specify external constraints that the system must meet.	IIC
non-repudiation	ability to prove the occurrence of a claimed <u>event</u> or action and its originating entities	<u>ISO/IEC 27000:2016</u>

Term	Definition	Source
operational technology (OT)	hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise	<a href="#">Gartner IT Glossary</a>
operations domain	<u>functional domain</u> for management and operation of the <u>control domain</u>	IIC
orchestration	type of <u>composition</u> where one particular <u>element</u> is used by the composition to oversee and direct the other elements <b>note:</b> the element that directs an orchestration is not part of the orchestration.	<a href="#">ISO/IEC 18384-1</a>
party	<u>entity</u> , human or logical (e.g. an administrator, a legal entity, an agent), that has some <u>autonomy</u> , interest and responsibility in the execution of an <u>activity</u> . <b>note:</b> a party may assume more than one <u>role</u> , and a role may be fulfilled by several parties (i.e. by any one of them).	IIC
personally identifiable information (PII)	any <u>information</u> <ul style="list-style-type: none"> <li>• that identifies or can be used to identify, contact or locate the person to whom such information pertains,</li> <li>• from which <u>identification</u> or contact information of an individual person can be derived, or</li> <li>• that is or might be directly or indirectly linked to a natural person</li> </ul>	<a href="#">ISO/IEC 24745:2011</a>
physical entity	<u>entity</u> in the physical world that can be the subject of sensing and/or actuating	IIC
physical entity of interest	<u>physical entity</u> that is the subject of sensing and/or actuating	IIC
physical security	measures used to provide physical protection of resources against deliberate and accidental <u>threats</u>	<a href="#">ISO 7498-2:1989</a>

Term	Definition	Source
PKI (public key infrastructure)	structure of hardware, software, people, <u>processes</u> and policies that uses digital signature technology to provide relying parties with a verifiable association between the public <u>component</u> of an asymmetric key pair with a specific subject	<u>ISO 21091:2013</u>
privacy	right of individuals to control or influence what <u>information</u> related to them may be collected and stored and by whom and to whom that information may be disclosed	<u>ISO/TS 17574:2009</u>
privacy risk assessment	overall <u>process</u> of <u>risk identification</u> , <u>risk analysis</u> and <u>risk evaluation</u> with regard to the processing of <u>personally identifiable information</u> <b>note:</b> this process is also known as a <u>privacy</u> impact assessment	<u>ISO/IEC 29100:2011</u>
privilege	right granted to an individual, a program or a <u>process</u>	<u>CNSSI 4009</u>
process	type of <u>composition</u> whose <u>elements</u> are composed into a sequence or flow of activities and interactions with the objective of carrying out certain work <b>note:</b> a process may also be a <u>collaboration</u> , <u>choreography</u> or <u>orchestration</u> .	<u>ISO/IEC 18384-1</u>
programmable logic controller (PLC)	electronic device designed for control of the logical sequence of <u>events</u>	<u>ISO 13577-4:2014</u>
reliability	ability of a system or <u>component</u> to perform its required functions under stated conditions for a specified period of time	<u>ISO/IEC 27040:2015</u>
resilience	ability of a system or <u>component</u> to maintain an acceptable level of <u>service</u> in the face of disruption	IIC

Term	Definition	Source
risk	<p>effect of uncertainty on objectives</p> <p><b>note 1:</b> an effect is a deviation from the expected—positive or negative.</p> <p><b>note 2:</b> uncertainty is the state, even partial, of deficiency of <u>information</u> related to, understanding or knowledge of, an <u>event</u>, its consequence or likelihood.</p> <p><b>note 3:</b> risk is often characterized by reference to potential events and consequences, or a combination of these.</p> <p><b>note 4:</b> risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.</p> <p><b>note 5:</b> in the context of <u>information security</u> management systems, <u>information security risks</u> can be expressed as effect of uncertainty on information security objectives.</p> <p><b>note 6:</b> <u>information security risk</u> is associated with the potential that <u>threats</u> will exploit <u>vulnerabilities</u> of an <u>information asset</u> or group of information assets and thereby cause harm to an organization. (see definition of information security risk)</p>	ISO/IEC 27000:2016
risk analysis	<p><u>process</u> to comprehend the nature of <u>risk</u> and to determine the level of risk</p> <p><b>note 1:</b> risk analysis provides the basis for <u>risk evaluation</u> and decisions about risk treatment.</p> <p><b>note 2:</b> risk analysis includes risk estimation.</p>	ISO/IEC 27000:2016
risk assessment	<p>overall <u>process</u> of <u>risk identification</u>, <u>risk analysis</u> and <u>risk evaluation</u></p>	ISO/IEC 27000:2016
risk evaluation	<p><u>process</u> of comparing the results of <u>risk analysis</u> with <u>risk criteria</u> to determine whether the and/or its magnitude is acceptable or tolerable</p> <p><b>note:</b> risk evaluation assists in the decision about risk treatment.</p>	ISO/IEC 27000:2016
risk identification	<p><u>process</u> of finding, recognizing and describing <u>risk</u></p> <p><b>note 1:</b> risk identification involves the identification of risk sources, <u>events</u>, their causes and their potential consequences.</p> <p><b>note 2:</b> risk identification can involve historical <u>data</u>, theoretical analysis, informed and expert opinions, and <u>stakeholders'</u> needs</p>	ISO/IEC 27000:2016

Term	Definition	Source
risk management	coordinated activities to direct and control an organization with regard to <u>risk</u>	<u>ISO/IEC 27000:2016</u>
risk response	acceptance, avoidance, mitigation, sharing or transfer of <u>risk</u> to organizational operations (i.e. mission, functions, image or reputation), organizational <u>assets</u> , individuals, other organizations or the nation	<u>NISTIR 7298, rev 2<sup>(1)</sup></u>
risk tolerance	level of <u>risk</u> an <u>entity</u> is willing to assume in order to achieve a potential desired result	<u>NISTIR 7298, rev 2</u>
robustness	ability of a system or <u>component</u> to continue functioning correctly in the presence of invalid inputs or stressful <u>environmental</u> conditions	IIC
role	set of <u>usage capacity</u> <b>note 1:</b> a role is an abstraction for an <u>entity</u> which performs the set of activities. <b>note 2:</b> roles are fulfilled or assumed by parties.	IIC
roots of trust	bases consisting of hardware, software, people and organizational <u>processes</u> used to establish confidence in the system	IIC
SaaS	cloud <u>service</u> category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type	<u>ISO/IEC 17788:2014</u>
safety	the condition of the system operating without causing unacceptable <u>risk</u> of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to property or to the <u>environment</u>	<u>ISO/IEC Guide 55:1999<sup>(1)</sup></u>
security	property of being protected from unintended or unauthorized access, change or destruction ensuring <u>availability</u> , <u>integrity</u> and <u>confidentiality</u> .	IIC

Term	Definition	Source
security controls	management, operational and technical controls (i.e. safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information	<a href="#">ISO 12812-1:2017</a>
security function	cryptographic algorithms together with modes of operation, such as block ciphers, stream ciphers, symmetric or asymmetric key algorithms, message authentication codes, hash functions or other security functions, random bit generators, entity authentication and SSP generation and establishment all approved either by ISO/IEC or an approval authority	<a href="#">ISO/IEC 19790:2012<sup>(1)</sup></a>
security policy	rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems, particularly those which impact the systems and associated elements	<a href="#">NISTIR 7298, rev. 2</a>
security vulnerability assessment	systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation	<a href="#">NISTIR 7298, rev. 2</a>
semantic interoperability	interoperability such that the meaning of the exchanged information can be understood by the participating systems	IIC
service	distinct part of the functionality that is provided by an entity through interfaces	<a href="#">ISO/IEC TR 14252:1996</a>

Term	Definition	Source
situational awareness	within a volume of time and space, the perception of an enterprise's <u>security posture</u> and its <u>threat environment</u> ; the comprehension/meaning of both taken together <u>risk</u> ); and the projection of their status into the near future	<u>NISTIR 7298, rev 2</u>
stakeholder	individual, team, organization or classes thereof, having an interest in the system of interest	<u>ISO/IEC/IEEE 42010:2011<sup>(1)</sup></u>
syntactic interoperability	<u>interoperability</u> such that the formats of the exchanged <u>information</u> can be understood by the participating systems	<u>ISO/IEC 19941:2017</u>
task	unit of work	IIC
threat	potential cause of an unwanted incident, which may result in harm to a system or organization	<u>ISO/IEC 27000:2016</u>
threat analysis	examination of <u>threat</u> sources against system vulnerabilities to determine the threats for a particular system in a particular operational <u>environment</u>	<u>NISTIR 7298, rev 2</u>
threat event	<u>event</u> or situation that has the potential for causing undesirable consequences or impact	<u>NISTIR 7298, rev 2</u>
threat modeling	structured analysis to identify, quantify and address the <u>information security risks</u> associated with an application or a system	IIC
trust boundary	separation of different application or system domains in which different levels of <u>trust</u> are required	IIC
trustworthiness	degree of confidence one has that the system performs as expected with characteristics including <u>safety</u> , <u>security</u> , <u>privacy</u> , <u>reliability</u> and <u>resilience</u> in the face of <u>environmental</u> disturbances, human errors, system faults and attacks	IIC

Term	Definition	Source
usage capacity	ability to initiate, to participate in the execution of, or to consume the outcome of some <u>tasks</u> or functions	IIC
usage viewpoint	<u>architecture viewpoint</u> that frames the <u>concerns</u> related to <u>industrial internet of things (IIoT) system</u> usage	IIC
validation	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled	<u>ISO/IEC 27000:2016</u>
verification	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled <b>note:</b> this could also be called compliance testing.	<u>ISO/IEC 27000:2016</u>
vulnerability	weakness of an <u>asset</u> or <u>security controls</u> that can be exploited by one or more <u>threats</u>	<u>ISO/IEC 27000:2016</u> <sup>(1)</sup>

Table 4-1: Defined Terms and Definitions

(1) This definition has modified the wording of the referenced source definition for consistency with the other definitions

## Annex A REVISION HISTORY

Revision	Date	Editor	Changes Made
V1.0	2015-05-07	Rutt/Miller	Initial release
V2.0	2017-06-17	Karmarkar/Buchheit	Major update, details see Annex B
V2.1	2018-08-02	Karmarkar/Buchheit	Minor update, details see Annex B
V2.2	2019-09-03	Buchheit/Bournival	Minor update, details see Annex B

Table A-2: Revision History

## Annex B TERMS CHANGE HISTORY

Term	Version	Changes Made
actuator	2.0	renamed to IoT actuator
application domain	2.0	added
application domain	2.1	redefined
architecture	2.0	added
architecture viewpoint	2.0	added
asset	2.0	added
attack surface	2.0	added
attack vector	2.0	redefined
attacker	2.0	added
attestation	2.0	added
audit	2.0	added
automatic	2.0	removed
automation	2.0	removed
brownfield	2.1	renamed from brownfield development, redefined
brownfield development	2.0	added
brownfield development	2.1	renamed to brownfield
business viewpoint	2.0	added
business viewpoint	2.1	redefined
cloud computing	2.0	added
component	2.1	source changed
composability	2.1	redefined
confidentiality	2.2	redefined
connectivity	2.1	added
connectivity endpoint	2.0	added
control domain	2.0	added
control domain	2.1	redefined
controller	2.0	removed
coordinate	2.0	removed
coordination	2.0	removed
countermeasure	2.0	added
credential	2.0	added
cross-cutting concern	2.0	redefined
cross-cutting function	2.0	redefined
data	2.1	added
data at rest	2.0	added
data in motion	2.0	added
data in use	2.0	added
data integrity	2.0	added
databus	2.0	added
denial of service (DoS)	2.0	added
device	2.0	renamed to IoT device
device endpoint	2.0	removed
digital representation	2.0	added
digital representation	2.2	redefined
digital twin	2.2	added

Term	Version	Changes Made
edge	2.1	added
edge computing	2.1	added
edge gateway	2.1	removed
element	2.0	redefined
encryption	2.0	added
endpoint	2.0	redefined
endpoint address	2.0	removed
event	2.0	added
firmware	2.1	removed
functional domain	2.1	redefined
functional viewpoint	2.0	added
functional viewpoint	2.1	redefined
gateway	2.1	removed
greenfield	2.1	renamed from greenfield development, redefined
greenfield development	2.0	added
greenfield development	2.1	renamed to greenfield
identity	2.0	redefined
implementation viewpoint	2.0	added
implementation viewpoint	2.1	redefined
incident response or incident response	2.0	added
industrial control system (ICS)	2.1	added
industrial internet of thing (IIoT) system	2.0	added
information	2.1	added
information domain	2.0	added
information domain	2.1	redefined
information security incident	2.0	added
information technology	2.1	added
integrability	2.0	removed
internet	2.0	removed
interoperability	2.1	added
IoT actuator	2.0	renamed from actuator, redefined
IoT actuator	2.2	redefined
IoT device	2.0	renamed from device, redefined
IoT sensor	2.0	renamed from sensor, redefined
IoT sensor	2.2	redefined
IP endpoint	2.0	removed
IT/OT convergence	2.1	added
malware	2.0	added
man-in-the-middle attack	2.0	added
multi-tenancy	2.0	added
network	2.0	redefined
non-repudiation	2.0	added
observer	2.0	removed
operational technology (OT)	2.0	added
operations domain	2.0	added
operations domain	2.1	redefined
physical security	2.0	added
PKI (public key infrastructure)	2.0	added

Term	Version	Changes Made
policy	2.0	removed
process	2.0	added
programmable logic controller (PLC)	2.0	added
physical entity	2.2	redefined
physical entity of interest	2.2	added
resilience	2.0	redefined
risk response	2.0	redefined
robustness	2.0	redefined
roots of trust	2.0	added
SaaS	2.0	added
security	2.0	redefined
security control	2.0	renamed to security controls
security controls	2.0	renamed from security control, redefined
security function	2.0	renamed from security functions, corrected
security functions	2.0	renamed to security function
security vulnerability assessment	2.0	added
semantic interoperability	2.1	added
sensitivity	2.0	removed
sensor	2.0	renamed to IoT sensor
syntactic interoperability	2.1	added
thing	2.0	removed
trust	2.0	removed
trustworthiness	2.0	added
trustworthiness	2.1	redefined
usage viewpoint	2.0	added
usage viewpoint	2.1	redefined
user	2.0	removed
user endpoint	2.0	removed
virtual entity	2.2	removed
vulnerability assessment	2.0	removed

Table B-3: Terms Change History

---

**Annex C REFERENCES**

---

- [CNSS-4009] Committee on National Security Systems (CNSS): CNSSI No. 4009: Glossary, released 2015-April-06, retrieved 2017-05-29  
*<https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf>*
- [Gartner-ITG] Gartner: IT Glossary, retrieved 2017-05-29  
*<http://www.gartner.com/it-glossary>*
- [IHMC] Institute for Human & Machine Cognition (IHMC), Florida Institute for Human & Machine Cognition, retrieved 2017-05-29  
*<https://www.ihmc.us>*
- [IoT-A] Internet of Things—Architecture: Terminology, VDI/VDE Innovation+Technik GmbH  
*[https://web.archive.org/web/20160104220408/http://www.iot-a.eu/public/terminology/copy\\_of\\_term](https://web.archive.org/web/20160104220408/http://www.iot-a.eu/public/terminology/copy_of_term)*
- [ISO-Guide-51] International Organization for Standardization: ISO/IEC Guide 51:2014: Safety aspects—Guidelines for their inclusion in standards, 2014-April, retrieved 2017-05-29  
*<https://www.iso.org/standard/53940.html>*
- [ISO-2382] International Organization for Standardization: ISO/IEC 2382:2015: Information technology—Vocabulary, 2015-May, retrieved 2017-05-29  
*<https://www.iso.org/standard/63598.html>*
- [ISO-7498-2] International Organization for Standardization: ISO 7498-2:1989: Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture, 1989-February, retrieved 2017-05-29  
*<https://www.iso.org/standard/14256.html>*
- [ISO-9798-1] International Organization for Standardization: ISO/IEC 9798-1:2010: Information technology—Security techniques—Entity authentication—Part 1: General, 2010-July, retrieved 2017-05-29  
*<https://www.iso.org/standard/53634.html>*
- [ISO-12812-1] International Organization for Standardization: ISO/IEC 12812-1:2017: Core banking—Mobile financial services—Part 1: General framework, 2017-March, retrieved 2017-05-29  
*<https://www.iso.org/standard/57989.html>*
- [ISO-13577-4] International Organization for Standardization: ISO/IEC 13577-4:2014: Industrial furnace and associated processing equipment—Safety—Part 4: Protective systems, 2014-September, retrieved 2017-05-29  
*<https://www.iso.org/standard/57989.html>*

- [ISO-14252] International Organization for Standardization: ISO/IEC TR 14242:1996: Information technology—Guide to the POSIX Open System Environment (OSE), 1996-December, retrieved 2017-05-29  
<https://www.iso.org/standard/23985.html>
- [ISO-14813-5] International Organization for Standardization: ISO 14813-5:2010: Intelligent transport systems—Reference model architecture(s) for the ITS sector—Part 5: Requirements for architecture description in ITS standards, 2010-July, retrieved 2018-06-15  
<https://www.iso.org/standard/46008.html>
- [ISO-15026-1] International Organization for Standardization: ISO/IEC 15026-1:2013: Systems and software engineering—Systems and software assurance—Part 1: Concepts and vocabulary, 2013-November, retrieved 2017-05-29  
<https://www.iso.org/standard/62526.html>
- [ISO-17574] International Organization for Standardization: ISO/TS 17574:2009: Electronic fee collection—Guidelines for security protection profiles, 2009-September, retrieved 2017-05-29  
<https://www.iso.org/standard/52387.html>
- [ISO-17788] International Organization for Standardization: ISO/IEC 17788:2014: Information technology—Cloud computing—Overview and vocabulary, 2014-October, retrieved 2017-05-29  
<https://www.iso.org/standard/60544.html>
- [ISO-17789] International Organization for Standardization: ISO/IEC 17789:2014: Information technology—Cloud computing—Reference architecture, 2014-October, retrieved 2017-05-23  
<https://www.iso.org/standard/60545.html>
- [ISO-18014-2] International Organization for Standardization: ISO/IEC 18014-2:2009: Information technology—Security techniques—Time-stamping services—Part 2: Mechanisms producing independent tokens, 2009-December, retrieved 2017-05-29  
<https://www.iso.org/standard/50482.html>
- [ISO-18384-1] International Organization for Standardization: ISO/IEC 18384-1:2016: Information technology—Reference Architecture for Service Oriented Architecture (SOA RA)—Part 1: Terminology and concepts for SOA, 2016-June, retrieved 2017-05-24  
<https://www.iso.org/standard/63104.html>
- [ISO-19790] International Organization for Standardization: ISO/IEC 19790:2012: Information technology—Security techniques—Security requirements for cryptographic modules, 2012-August, retrieved 2017-05-29  
<https://www.iso.org/standard/52906.html>

- [ISO-19941] International Organization for Standardization: ISO 19941:2017: Information technology—Cloud computing—Interoperability and portability, 2017-December, retrieved 2018-06-25  
<https://www.iso.org/standard/66639.html>
- [ISO-21091] International Organization for Standardization: ISO 21091:2013: Health informatics—Directory services for healthcare providers, subjects of care and other entities, 2013-February, retrieved 2017-05-29  
<https://www.iso.org/standard/51432.html>
- [ISO-24745] International Organization for Standardization: ISO/IEC 24745:2011: Information technology—Security technique—Biometric information protection, 2011-June, retrieved 2017-05-29  
<https://www.iso.org/standard/52946.html>
- [ISO-24760-1] International Organization for Standardization: ISO/IEC 24760-1:2011: Information Technology—Security techniques—A framework for identity management, 2011-12-15, retrieved 2017-05-23  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=57914](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57914)
- [ISO-27000] International Organization for Standardization: ISO 27000:2016: Information technology—Security technique—Information security management systems—Overview and vocabulary, 2016, retrieved 2017-05-23  
[http://www.iso.org/iso/catalogue\\_detail?csnumber=66435](http://www.iso.org/iso/catalogue_detail?csnumber=66435)
- [ISO-27005] International Organization for Standardization: ISO 27005:2011: Information technology—Security technique—Information security risk management, 2011-June, retrieved 2017-05-29  
<https://www.iso.org/standard/56742.html>
- [ISO-27031] International Organization for Standardization: ISO/IEC 27031:2011: Information technology—Security technique—Guidelines for information and communication technology readiness for business continuity, 2011-March, retrieved 2017-05-29  
<https://www.iso.org/standard/44374.html>
- [ISO-27033-1] International Organization for Standardization: ISO/IEC 27033-1:2015: Information Technology—Security techniques—Network security—Part 1: Overview and concepts, 2015-August, retrieved 2017-05-23  
<https://www.iso.org/standard/63461.html>
- [ISO-27039] International Organization for Standardization: ISO/IEC 27039:2015: Information technology—Security technique—Selection, deployment and operations of intrusion detection and prevention systems (IDPS), 2015-February, retrieved 2017-05-29  
<https://www.iso.org/standard/44404.html>

- [ISO-27040] International Organization for Standardization: ISO/IEC 27040:2015: Information technology—Security technique—Storage security, 2015-January, retrieved 2017-05-29  
<https://www.iso.org/standard/44404.html>
- [ISO-29100] International Organization for Standardization: ISO/IEC 29100:2011: Information technology—Security technique—Privacy framework, 2011, retrieved 2017-05-23  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=45123](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123)
- [ISO-29109-1] International Organization for Standardization: ISO/IEC 29109-1:2013:2009: Information technology—Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794—Part 1: Generalized conformance testing methodology, 2009-August, retrieved 2017-05-29  
<https://www.iso.org/standard/45132.html>
- [ISO-31320-2] International Organization for Standardization: ISO/IEC/IEEE 31320-2:2012: Information technology—Modeling Languages—Part 2: Syntax and Semantics for IDEF1X97 (IDEFobject), 2012-September, retrieved 2017-05-29  
<https://www.iso.org/standard/60614.html>
- [ISO-42010] International Organization for Standardization: ISO/IEC/IEEE 42010:2011: System and software engineering—Architecture description, 2011-December, retrieved 2017-05-29  
<https://www.iso.org/standard/50508.html>
- [NIST-800-61] National Institute of Standards and Technology (NIST) Special Publication 800-61, revision 2: Computer Security, Incident Handling Guide, 2012-August, retrieved 2017-05-29  
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- [NISTIP-8401-1] National Institute of Standards and Technology (NIST) Interagency Publication 8401-1: DRAFT NIST Big Data Interoperability Framework: Volume 1, Definitions, NIST Big Data Public Working Group, Definitions and Taxonomies Subgroup, draft version 1, 2015-March-02, retrieved 2017-05-29  
[http://bigdatawg.nist.gov/\\_uploadfiles/M0357\\_v2\\_4404462833.docx](http://bigdatawg.nist.gov/_uploadfiles/M0357_v2_4404462833.docx)
- [NISTIR-7298] National Institute of Standards and Technology (NIST) Internal Reports: Glossary of Key Information, Security Terms, revision 2, Richard Kissel, Editor, Computer Security Division, Information Technology Laboratory, 2013-May, retrieved 2017-05-29  
<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>

## **AUTHORS AND LEGAL NOTICE**

---

Copyright © 2019, Industrial Internet Consortium, a program of Object Management Group, Inc. (“OMG”).

### **ACKNOWLEDGEMENTS**

This document is a work product of the Industrial Internet Consortium Vocabulary Task Group in the Technology Working Group, co-chaired by Anish Karmarkar (Oracle) and Robert Martin (MITRE).

### **EDITORS**

Marcellus Buchheit (Wibu-Systems), Erin Bournival (Dell EMC)

### **AUTHORS**

The following persons contributed substantial written content to this document:

Erin Bournival (Dell EMC), Eric Simmon (NIST), Marcellus Buchheit (Wibu-Systems), Claude Baudoin (cébé IT & Knowledge Management), Frederick Hirsch (Fujitsu), Boss (Bosch), Will Sobel (VIMANA), Anish Karmarkar (Oracle), Rajive Joshi (RTI), Sven Schrecker (Intel), Shi-Wan Lin (Thingswise), Jesus Molina (Waterfall Security), Tom Rutt (Fujitsu), Bradford Miller (GE), Jacques Durand (Fujitsu), Paul Didier (Cisco), Amine Chigani (GE), Reinier Torenbeek (RTI), David Duggal (EnterpriseWeb), Robert Martin (MITRE), Graham Bleakley (IBM), Andrew King (University Of Pennsylvania), Robert Lembree (Intel), Hamed Soroush (RTI), Jason Garbis (RSA), Mark Crawford (SAP), Eric Harper (ABB), Kaveri Raman (AT&T), Brian Witten (Symantec), Andrew Ginter (Waterfall Security) and David Meltzer (Tripwire).

### **CONTRIBUTORS**

The following persons contributed valuable ideas and feedback that significantly improved the content and quality of this document:

Nina Tucker (Twin Oaks Computing), Birgit Denise Wahl (OMG), Todd Edmunds (Cisco), Mitch Tseng (Huawei), Brett Murphy (RTI), Farooq Bari (AT&T), Tom Rutt (Fujitsu), Jack Weast (Intel), Lin Nease (HP), Ron Ambrosio (IBM), Omer Schneider (Cyber-X Labs), Pete MacKay (Wurldtech), Lance Dover (Micron).

### **TECHNICAL EDITOR**

Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Editors, Authors and Contributors into an integrated document.

### **USE OF INFORMATION—TERMS, CONDITIONS AND NOTICES**

This is an Industrial Internet Consortium document (the “Document”) and is to be used in accordance with the terms, conditions and notices set forth below. This Document does not

represent a commitment by any person to implement any portion or recommendation contained in it in any products or services. The information contained in this Document is subject to change without notice.

## LICENSES

The companies who contributed content to this Document (“Contributing Companies”) have granted to the Industrial Internet Consortium (the “IIC”), a program of Object Management Group, Inc. (“OMG”) a nonexclusive, irrevocable, sublicensable, royalty-free, paid up, worldwide license to copy and distribute this Document and to modify this Document and distribute copies of the modified version. Each of the Contributing Companies has agreed that no person shall be deemed to have infringed the copyright in the included material provided by any such copyright holder by reason of having copied, distributed or used such material as set forth herein.

Subject to the terms and conditions below, OMG (including its IIC program) and the Contributing Companies hereby grant you a fully-paid up, non-exclusive, nontransferable, royalty-free, worldwide license (without the right to sublicense) to use, copy and distribute this Document (the “Permission”), provided that: (1) both the copyright notice above, and a copy of this Permission paragraph, appear on any copies of this Document made by you or by those acting on your behalf; (2) the use of the Document is only for informational purposes in connection with the IIC’s mission, purposes and activities; (3) the Document is not copied or posted on any network computer, publicly performed or displayed, or broadcast in any media and will not be otherwise resold or transferred for commercial purposes; and (4) no modifications are made to this Document.

This limited Permission is effective until terminated. You may terminate it at any time by ceasing all use of the Document and destroying all copies. The IIC may terminate it at any time by notice to you. This Permission automatically terminates without notice if you breach any of these terms or conditions. Upon termination, or at any time upon the IIC’s express written request, you will destroy immediately any copies of this Document in your possession or control.

The Licenses and Permission relate only to copyrights and do not convey rights in any patents (see below).

## PATENTS

Compliance with or adoption of any advice, guidance or recommendations contained in any IIC reports or other IIC documents may require use of an invention covered by patent rights. *OMG and its IIC program are not responsible for identifying patents for which a license may be required to comply with any IIC document or advice, or for conducting legal inquiries into the legal validity or scope of those patents that are brought to its attention. IIC documents are informational and advisory only. Readers of this Document are responsible for protecting themselves against liability for infringement of patents and other intellectual property that may arise from following any IIC recommendations or advice. OMG and its IIC program disclaim all responsibility for such infringement.*

## GENERAL USE RESTRICTIONS

This Document contains content that is protected by copyright. Any unauthorized use of this Document may violate copyright laws, trademark laws and communications regulations and statutes. Except as provided by the above Permission, no part of this work covered by copyright may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping or information storage and retrieval systems—without permission of the copyright owner(s).

## DISCLAIMER OF WARRANTY

WHILE THIS DOCUMENT IS BELIEVED TO BE ACCURATE, IT IS PROVIDED “AS IS” AND MAY CONTAIN ERRORS OR MISPRINTS. OMG (INCLUDING ITS IIC PROGRAM) AND THE CONTRIBUTING COMPANIES MAKE NO WARRANTIES, REPRESENTATIONS OR CONDITIONS OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS DOCUMENT, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF TITLE OR OWNERSHIP, OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE OR USE, OR AGAINST INFRINGEMENT. OMG (INCLUDING ITS IIC PROGRAM) MAKES NO REPRESENTATIONS, WARRANTIES, GUARANTIES, OR CONDITIONS AS TO THE QUALITY, SUITABILITY, TRUTH, ACCURACY, OR COMPLETENESS OF THIS DOCUMENT.

IN NO EVENT SHALL OMG (INCLUDING ITS IIC PROGRAM) OR ANY OF THE CONTRIBUTING COMPANIES BE LIABLE FOR ERRORS CONTAINED HEREIN OR FOR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, RELIANCE OR COVER DAMAGE, OR DAMAGE FOR LOSS OF PROFITS, REVENUE, DATA OR USE, HOWEVER IT ARISES, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, INCURRED BY ANY USER OR ANY THIRD PARTY IN CONNECTION WITH THE FURNISHING, PERFORMANCE, REPRODUCTION, DISTRIBUTION OR USE OF THIS MATERIAL, EVEN IF PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The entire risk as to the quality and performance of any software or technology developed using this Document is borne by you. This disclaimer of warranty constitutes an essential part of the Permission granted to you to use this Document.

## LIMITED RIGHTS NOTICE

This Document contains technical data that was developed at private expense and (i) embodies trade secrets, or (ii) is confidential and either commercial or financial. This document was not produced in the performance of a government contract and is not in the public domain. The use, duplication or disclosure of this Document by the U.S. Government is subject to the restrictions set forth in 48 C.F.R. 52.227-14–Rights in Data “Limited Rights Notice (Dec. 2007) (a) and (b),” or as specified in 48 C.F.R. 12.211 of the Federal Acquisition Regulations and its successors, as applicable. This data may only be reproduced and used by the U.S. Government with the express limitation that it will not, without written permission of the copyright owners, be used for purposes of manufacture nor disclosed outside the Government. The copyright owners are as indicated above and may be contacted through Object Management Group, Inc., 109 Highland Avenue, Needham, MA 02494, U.S.A.

## TRADEMARKS

The trademarks, service marks, trade names and other special designations that appear on and within the Document are the marks of OMG, the Contributing Companies and possibly other manufacturers and suppliers identified in the Document and may not be used or reproduced without the express written permission of the owner, except as necessary to reproduce, distribute and refer to this Document as authorized herein.