Industry Internet of Things Vocabulary

An Industry IoT Consortium Framework Publication

Version 3.00–2022-03-22

Claude Baudoin (cébé IT & Knowledge Management), Erin Bournival (Dell Technologies), Marcellus Buchheit (Wibu-Systems), Eric Simmon (NIST), Bassam Zarkout (IGnPower)

Contents

Figures

Tables

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

Each of the terms listed in the first column of Table 5-1 is rendered as a bookmark, which can be used for cross-references in any document that uses this table.

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

Table 5-1 also includes acronyms (for example, *IoT* for *internet of things*) and short forms (for example, *container* for *software container*).

1 PRINCIPLES

Perfection is achieved,
not when there is nothing more to add,
but when there is nothing left to take away.
Antoine de Saint-Exupéry, Airman's Odyssey

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.
- Terms with English dictionary definitions that are sufficient are generally not included in this vocabulary.
- An IIC-authored definition is used only when that term is not already defined in an existing specification or standard, such as ISO/IEC JTC 1 International Standard, or when the term has an existing definition that is not appropriate to be used in the context of industry IoT.
- 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 $^{(n)}$ style and appear at the end of the table.

3 GUIDANCE

When authoring documents that leverage the IIC Vocabulary, consider the following additional guidance:

- Terms listed in Table 6-1 have been identified as ambiguous or conflicting with accepted interpretations, and we instead suggest the use of approved alternatives.
- When you are unable to locate the definition for a given term, review Annex B to verify if your term has been removed from the IIC Vocabulary. If an alternative is available, it will be suggested in Table 6-1.
- To aid in the comprehension of your documents, we suggest avoiding inventing new terms for existing concepts. Leverage the IIC Vocabulary to streamline your work by importing established industry definitions into your working documents.

Additional guidelines for IIC members:

- We recommend that you reference the IIC Vocabulary in your documents, so that the full complement of IIC terms and definitions are available to the reader.
- If you encounter a term that should be in the IIC Vocabulary but does not presently have an entry, contact the IIC Vocabulary chairs to discuss this term's addition.

Additional guidelines for non-IIC members:

- If you encounter a term that should be in the IIC Vocabulary but does not presently have an entry, submit a contribution to the IIC at *vtg-chair@engage.inconsortium.org*, and request that your term be considered. We strongly suggest supplying a proposed definition and any pertinent context with your term, to ensure comprehension by the IIC Vocabulary team.
- While the IIC will strive to include such contributions, valid reasons can exist for not accepting them. The application of the principles in section 1 (page 3) may result in a contribution that is ineligible for inclusion.

Figure 3-1 and Figure 3-2 describe the IIC Vocabulary development process, first as an overview and then in greater detail.

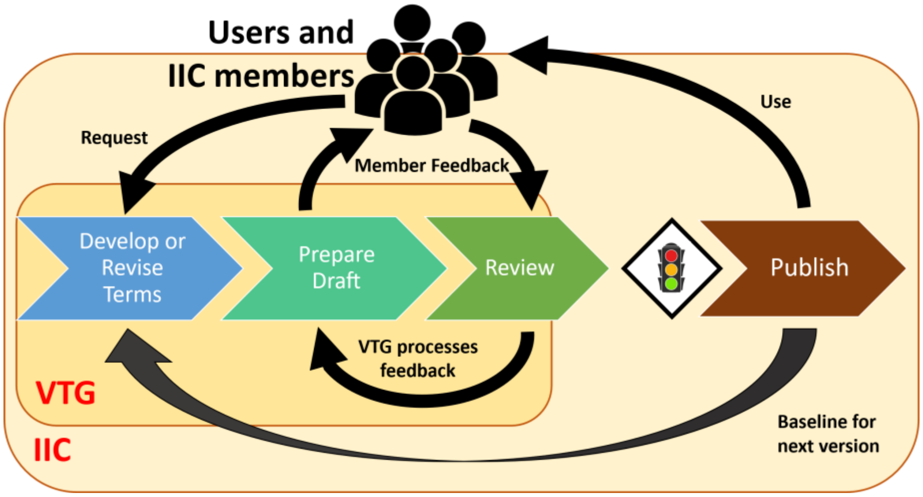
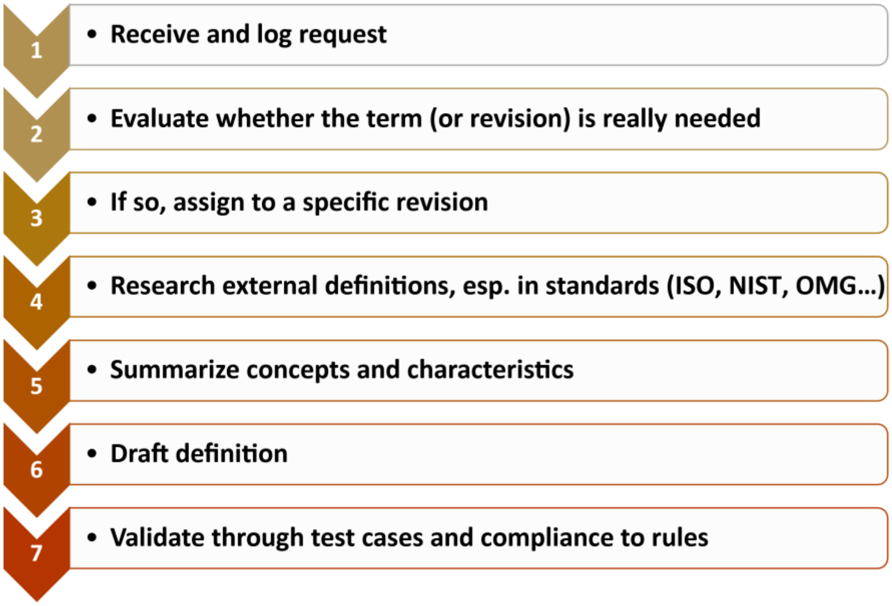


Figure 3-1: Vocabulary Development Process - Overview



- Receive and log request
- Evaluate whether the term (or revision) is really needed
- If so, assign to a specific revision
- Research external definitions, esp. in standards (ISO, NIST, OMG…)
- Summarize concepts and characteristics
- Draft definition
- Validate through test cases and compliance to rules

Figure 3-2: Vocabulary Development Process - Details

4 Relationship with Other IIC Content

This document fits in the IIC Technical Publication Organization shown in Figure 4-1, shown at the IIC Resource Hub.[1] This document does not have dependencies on other IIC documents.

[1] See *https://hub.iiconsortium.org/*

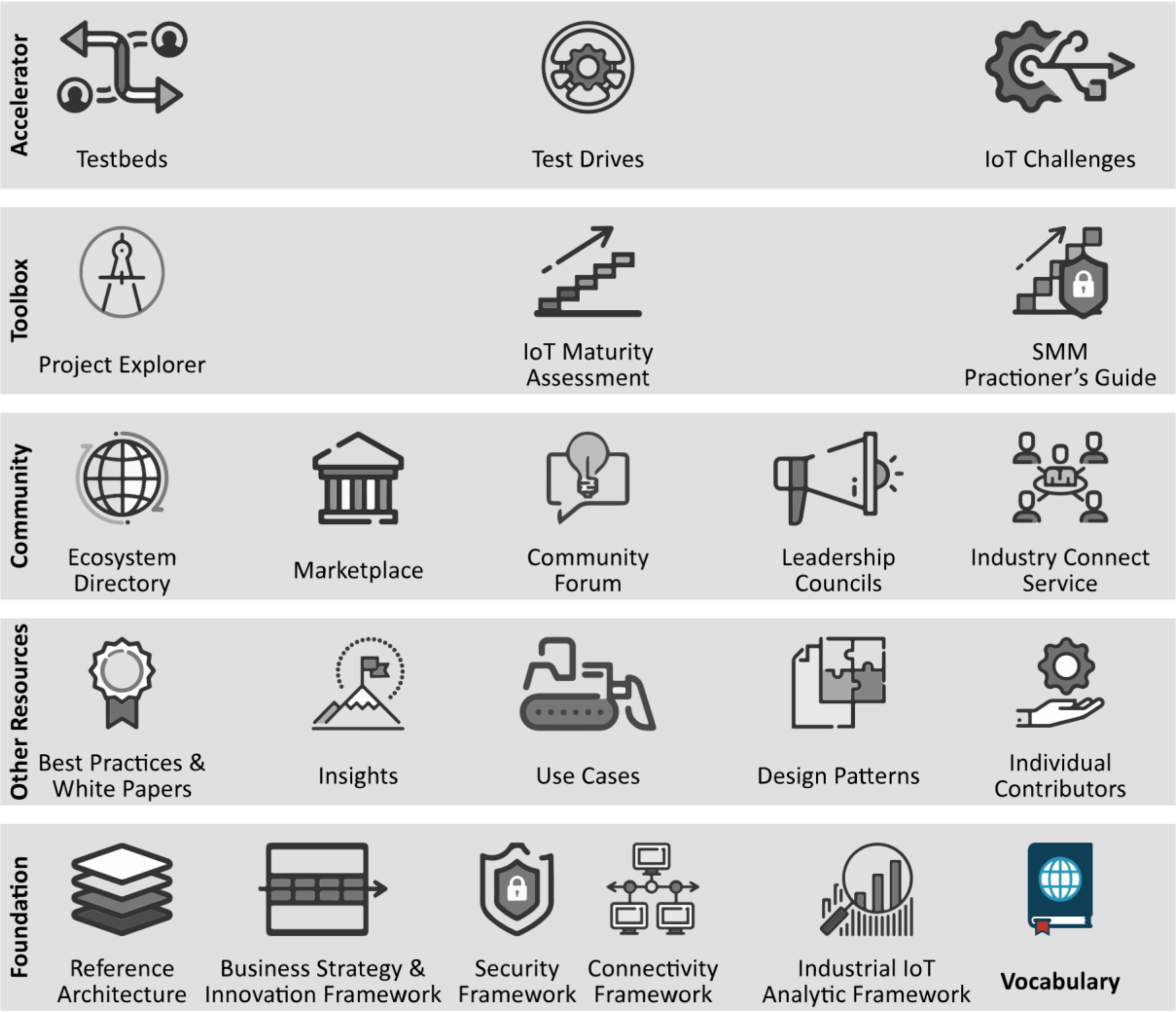


Figure 4-1: IIC Publication Organization

5 DEFINITIONS OF TERMS

Term	Definition	Source
access control	means to ensure that access to assets is authorized and restricted based on business and security requirements **note**: access control requires both authentication and authorization	ISO/IEC 27000:2016
activity	specified coordination of tasks that are required to realize the system capabilities **note**: an activity may be composed of other activities	ISO/IEC 17789:2014[(1)]
actuating	changing one or more properties of a physical entity in response to received information	IIC
analytics	synthesis of knowledge from information	NIST Interagency Publication 8401-1
application domain	functional domain for implementing application logic	IIC
architecture	fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution	ISO/IEC/IEEE 42010:2011
architecture description	work product used to express an architecture	ISO/IEC/IEEE 42010:2011
architecture framework	conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders	ISO/IEC/IEEE 42010:2011
architecture layer	logical partitioning of the architecture	IIC
architecture view[(2)]	work product expressing the architecture of a system from the perspective of specific system concerns **note**: in the context of the IIC, *view* is used as short form for architecture view.	ISO/IEC/IEEE 42010:2011

architecture viewpoint[2]	work product establishing the conventions for the construction, interpretation and use of architecture views to frame specific system concerns **note**: in the context of the IIC, *viewpoint* is used as short form for architecture viewpoint.	ISO/IEC/IEEE 42010:2011
asset	major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment or a logically related group of systems	NISTIR 7298, rev 2
assurance	grounds for justified confidence that a claim has been or will be achieved	ISO/IEC 15026-1:2013
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 digital networks, or to compromise availability to legitimate users of information system and network resources	ISO/IEC 27033-1:2015
attestation	issue of a statement, based on a decision that fulfillment of specified requirements has been demonstrated	ISO/IEC 29109-1:2009
attribute	characteristic or property of an entity that can be used to describe its state, appearance or other aspects	ISO/IEC 24760-1:2011
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	NISTIR 7298, rev 2

authenticated identity	identity information for an entity created to record the result of identity authentication	ISO/IEC 24760-1:2011
authentication	provision of assurance that a claimed characteristic of an entity is correct	ISO/IEC 27000:2016
authorization	granting of rights, which includes the granting of access based on access rights **note**: authorization results in privileges.	ISO 7498-2:1989
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	IHMC
availability	property of being accessible and usable upon demand by an authorized entity	ISO/IEC 27000:2016
brownfield	existing industrial system targeted for new functionality without operational disruptions	IIC
business impact analysis	process of analyzing operational functions and the effect that a disruption might have upon them	ISO/IEC 27031:2011
business view[2]	architecture view that frames the vision, values and objectives of the business stakeholders in establishing an internet of things system in its business and regulatory context	IIC
choreography	type of composition whose elements interact in a non-directed fashion with each autonomous part knowing and following an observable predefined pattern of behavior for the entire (global) composition **note 1**: choreography does not require complete or perfect knowledge of the pattern of behavior. **note 2**: see ISO/IEC 18384-3:2016, 8.3.	ISO/IEC 18384-1
cloud computing	paradigm for enabling digital network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand	ISO/IEC 17788:2014

	note: examples of resources include servers, operating systems, digital networks, software, applications and storage equipment.	
cloud service	one or more capabilities offered via cloud computing invoked using a defined interface	ISO/IEC 17788:2014
collaboration	type of composition whose elements interact in a non-directed fashion, each according to their own plans and purposes without a predefined pattern of behavior	ISO/IEC 18384-1
component	modular, deployable and replaceable part of a system that encapsulates implementation and exposes a set of interfaces	ISO 14813-5:2010
composability	ability of a component 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 elements for a particular purpose	ISO/IEC 18384-1
concern	interest in a system relevant to one or more of its stakeholders **note**: a concern pertains to any influence on a system in its environment, including developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological and social influences.	ISO/IEC/IEEE 42010:2011
confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities or processes	ISO/IEC 27000:2016
connectivity	ability of a system or application to communicate with other systems or applications via digital network(s)	IIC
connectivity endpoint	interface that provides connectivity	IIC
container	short form for software container	
control domain	functional domain for implementing industrial control systems	IIC

countermeasure	action, device, procedure, technique or other measure that is designed to minimize vulnerability	ISO/IEC 2382:2015
CPS	acronym for cyber-physical system	
credential	evidence or testimonials that support a claim of Identity or assertion of an attribute and usually are intended to be used more than once	CNSSI 4009
criticality	measure of the degree to which an organization depends on an entity for the success of a mission or of a business function	NISTIR 7298, rev 2[(1)]
cross-cutting concern	concern that affects the whole system and thus may impact multiple viewpoints of the architecture	IIC
cross-cutting function	function that may be applied and realized across multiple functional domains of the architecture to address cross-cutting concerns	IIC
cyber-physical system (CPS)	system comprised of digital and physical parts, where some of those parts are capable of sensing or affecting the physical world **note** an internet of things system is a specialization of a cyber-physical system that uses a digital network.	IIC
cryptography	discipline that embodies principles, means and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use	ISO/IEC 18014-2:2009
data	content represented in a digital and formalized manner suitable for communication, storage, interpretation or processing	IIC, inspired by ISO/IEC 2382:2015
data at rest	stored data that is neither being processed nor transferred	IIC

data center	facility containing a collection of connected equipment that provides computing resources	IIC
data in motion	data being transferred from one location to another	ISO/IEC 27040:2015
data in use	data being processed	IIC
data integrity	property that data has not been altered or destroyed in an unauthorized manner	ISO/IEC 27040:2015
databus	data-centric information sharing technology that implements a virtual, global data space, where applications exchange data **note**: key characteristics of a databus are: the applications directly interface with the operational data the databus implementation interprets and selectively filters the data, and the databus implementation imposes rules and manages quality of service (QoS) parameters, such as rate, reliability and security of data flow.	IIC
denial of service (DoS)	prevention of authorized access to resources or the delaying of time-critical operations	ISO/IEC 27033-1:2015
digital network	collection of endpoints that are interconnected in a many-to-many arrangement **note**: in the context of the IIC, *network* is used as short form for digital network.	IIC
digital twin	digital model of one or more real-world entities that is synchronized with those entities at a specified frequency and fidelity **note**: digital twin entities can be objects or processes	Digital Twin Consortium[(1)]
DoS	acronym for denial of service	
edge	boundary between the pertinent digital and physical entities, delineated by IoT devices	IIC
edge computing	distributed computing that is performed near the edge, where the nearness is determined by the system requirements	IIC

element	entity that is indivisible at a given level of abstraction and has a clearly defined boundary	ISO/IEC 18384-1(1)
emergent behavior	behavior of a system realized by the interactions of its components	IIC
encryption	reversible operation by a cryptographic algorithm converting data into ciphertext to hide the information content of the data	ISO/IEC 9798-1:2010
endpoint	component that has computational capabilities and digital network connectivity	IIC
entity	item that has recognizably distinct existence **note**: e.g. a person, an organization, a device, a subsystem or a group of such items	ISO/IEC 24760-1:2011(1)
event	observable occurrence in a system and/or digital network	NIST SP 800-61
functional component	functional building block needed to engage in an activity realized by an implementation	ISO/IEC 17789:2014
functional domain	collection of functions comprising a system	IIC
functional framework	set of abstract re-useable functional components that can be extended/customized and applied to several applications in a specific domain	IIC
functional view(2)	architecture view that frames the concerns related to the functional capabilities and structure of internet of things system and its components	IIC
greenfield	new industrial system without operational disruption concerns	IIC
IaaS	acronym for infrastructure as a service	
ICS	acronym for industrial control system	
identification	process of recognizing an entity in a particular identity domain as distinct from other entity	ISO/IEC 24760-1:2011

identifier	identity information that unambiguously distinguishes one entity from another one in a given identity domain	ISO/IEC 24760-1:2011
Identity	inherent property of an instance that distinguishes it from all other instances	ISO/IEC/IEEE 31320-2:2012
identity authentication	formalized process of identity verification that, if successful, results in an authenticated identity for an entity	ISO/IEC 24760-1:2011
identity domain	environment where an entity can use a set of attributes for identification and other purposes	ISO/IEC 24760-1:2011
identity information	set of values of attributes optionally with any associated metadata in an Identity **note**: in an information and communication technology system an Identity is present as identity information.	ISO/IEC 24760-1:2011
identity management	processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in Identity known in a particular identity domain	ISO/IEC 24760-1:2011
identity verification	process to determine that presented identity information associated with a particular entity is applicable for the entity to be recognized in a particular identity domain at some point in time	ISO/IEC 24760-1:2011
IIoT system	acronym for internet of things system	
implementation view[(2)]	architecture view that frames the concerns related to implementing the capabilities and structure of an internet of things system	IIC
incident response *or* intrusion response	action taken to protect and restore the normal operational conditions of information systems and the information stored in it when an attack or intrusion occurs	ISO/IEC 27039:2015
industrial control system (ICS)	combination of control components 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 data analytics for transformational business outcomes	IIC
Industrial Internet of Things system (IIoT system)	internet of things system used in an industrial context	IIC
information	data that within a certain context has a particular meaning	IIC, inspired by ISO/IEC 2382:2015
information domain	functional domain for managing and processing data	IIC
information security incident	single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security	ISO/IEC 27000:2016
information security risk	potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization	ISO/IEC 27005:2008
information technology (IT)	entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services **note**: Although information technology (IT) technologies are used in operational technology, information technology (IT) is traditionally considered to be distinct from operational technology (OT) due to a different set of requirements and concerns	Gartner IT Glossary
infrastructure as a service (IaaS)	capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources onto a cloud infrastructure where the consumer is able to deploy and run software, which can include operating systems and applications	NIST SP500-322[(1)]
infrastructure service	service that is essential for any IoT implementation to work properly	IOT-A

	note: Infrastructure services provide support for essential features of the IoT.	
integrity	property of accuracy and completeness	ISO/IEC 27000:2016
interface	named set of operations that characterize the behavior of an entity	IOT-A
internet of things (IoT)	concept where components are connected via a digital network and where one or more of those components interact with the physical world	IIC
internet of things system (IoT system)	system where the components are connected via a digital network and one or more of those components interact with the physical world	IIC
interoperability	ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged	ISO/IEC 17788:2014
IoT	acronym for internet of things	
IoT actuator	IoT device with the capability of actuating	IIC
IoT device	endpoint that interacts with one or more physical entities of interest through sensing or actuating	IIC
IoT environment	set of IoT components available to be composed into internet of things systems, the digital networks connecting the components and any associated services	NISTIR 8316[1]
IoT sensor	IoT device with the capability of sensing	IIC
IoT system	acronym for internet of things system	
IT	acronym for information technology	
IT/OT convergence	process of interweaving information technology and operational technology in order to create internet of things systems	IIC

least privilege	principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function	NISTIR 7298, rev 2
malware	malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity or availability	ISO/IEC 27040:2015
man-in-the-middle attack	attack in which the attacker intercepts a communications flow between two entities, appearing to each party as the other, while being able to read and modify messages in the communications flow	IIC
malware	malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity or availability	ISO/IEC 27040:2015
model	symbolic representation of an entity	IIC
model kind	conventions for a type of modelling	ISO/IEC/IEEE 42010:2011*(1)*
network	short form for digital network	
non-functional requirement	constraints on the quality attributes of a component or system **note**: quality attributes include trustworthiness, usability, durability, efficiency, and endurance.	IIC
non-repudiation	ability to prove the occurrence of a claimed event or action and its originating entities	ISO/IEC 27000:2016
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	Gartner IT Glossary
operations domain	functional domain for management and operation of the control domain	IIC

orchestration	type of composition where one particular element is used by the composition to oversee and direct the other elements **note**: the element that directs an orchestration is not part of the orchestration.	ISO/IEC 18384-1
OT	acronym for operational technology	
PaaS	acronym for platform as a service	
party	entity, human or logical (e.g. an administrator, a legal entity, an agent), that has some autonomy, interest and responsibility in the execution of an activity **note**: a party may assume more than one role, and a role may be fulfilled by several parties (i.e. by any one of them).	IIC
personally identifiable information (PII)	information that identifies or can be used to identify, contact or locate the person to whom such information pertains, from which identification or contact information of an individual person can be derived, or that is or might be directly or indirectly linked to a natural person	ISO/IEC 24745:2011
physical entity	entity in the physical world that can be the subject of sensing and/or actuating	IIC
physical entity of interest	physical entity that is the subject of sensing and/or actuating	IIC
physical security	measures used to provide physical protection of resources against deliberate and accidental threats	ISO 7498-2:1989
PII	acronym for personally identifiable information	
PKI	acronym for public key infrastructure	

platform as a service (PaaS)	capability provided to the consumer to deploy onto a cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider	NIST SP500-322
PLC	acronym for programmable logic controller	
privacy	ability of an individual or group to control the access, use and retention of personally identifiable information	IIC
privacy risk assessment	overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information **note**: this process is also known as a privacy impact assessment	ISO/IEC 29100:2011
privilege	right granted to an individual, a program or a process	CNSSI 4009
process	type of composition whose elements are composed into a sequence or flow of activities and interactions with the objective of carrying out certain work **note**: a process may also be a collaboration, choreography or orchestration.	ISO/IEC 18384-1
programmable logic controller (PLC)	electronic device designed for control of the logical sequence of events	ISO 13577-4:2014
public key infrastructure	structure of hardware, software, people, processes and policies that uses digital signature technology to provide relying parties with a verifiable association between the public component of an asymmetric key pair with a specific subject	ISO 21091:2013
reliability	ability of a system or component to perform its required functions under stated conditions for a specified period of time	ISO/IEC 27040:2015
resilience	ability of a system or component to maintain an acceptable level of service in the face of disruption	IIC

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

risk management	coordinated activities to direct and control an organization with regard to risk	ISO/IEC 27000:2016
risk response	acceptance, avoidance, mitigation, sharing or transfer of risk to organizational operations (i.e. mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation	NISTIR 7298, rev 2(1)
risk tolerance	level of risk an entity is willing to assume in order to achieve a potential desired result	NISTIR 7298, rev 2
robustness	ability of a system or component to continue functioning correctly in the presence of invalid inputs or stressful environmental conditions	IIC
role	set of usage capacity **note 1**: a role is an abstraction for an entity which performs the set of activities. **note 2**: roles are fulfilled or assumed by parties.	IIC
roots of trust	bases consisting of hardware, software, people and organizational processes used to establish confidence in the system	IIC
SaaS	acronym for software as a service	
safety	condition of a system operating, within a given context, with tolerable risk of injury or death to people	ISO/IEC Guide 51:2014(1)
security	property of being protected from unintended or unauthorized access, change or destruction ensuring availability, integrity and confidentiality	IIC
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	ISO 12812-1:2017

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	ISO/IEC 19790:2012[(1)]
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	NISTIR 7298, rev 2
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	NISTIR 7298, rev 2
semantic interoperability	interoperability such that the meaning of the exchanged information can be understood by the participating systems	IIC
sensing	observing one or more properties of a physical entity and converting those properties into information	IIC
service	distinct part of the functionality that is provided by an entity through interfaces	ISO/IEC TR 14252:1996
situational awareness	perception and understanding of an actor's environment	NISTIR 7298, rev 2
software as a service (SaaS)	capability provided to the consumer to use the provider's applications running onto a cloud infrastructure	NIST SP500-322

software container	single image, including code or data structures that can be deployed across different operating platforms **note**: in the context of the IIC, *container* is used as short form for software container.	IIC
stakeholder	individual, team, organization or classes thereof, having an interest in the system of interest	ISO/IEC/IEEE 42010:2011[1]
syntactic interoperability	interoperability such that the formats of the exchanged information can be understood by the participating systems	ISO/IEC 19941:2017
system	set of components interacting to achieve specific goals	IIC
task	unit of work	IIC
threat	potential cause of an unwanted incident, which may result in harm to a system or organization	ISO/IEC 27000:2016
threat analysis	examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment	NISTIR 7298, rev 2
threat event	event or situation that has the potential for causing undesirable consequences or impact	NISTIR 7298, rev 2
threat modeling	structured analysis to identify, quantify and address the information security risks associated with an application or a system	IIC
trust boundary	separation of different application or system domains in which different levels of trust are required	IIC
trustworthiness	degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks	IIC

usage capacity	ability to initiate, to participate in the execution of, or to consume the outcome of some tasks or functions	IIC
usage view[2]	architecture view that frames the concerns related to internet of things system usage	IIC
validation	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled	ISO/IEC 27000:2016
verification	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled **note**: this could also be called compliance testing.	ISO/IEC 27000:2016
view	short form for architecture view	
viewpoint[2]	short form for architecture viewpoint	
vulnerability[2]	weakness of an asset or security controls that can be exploited by one or more threats	ISO/IEC 27000:2016[1]

Table 5-1: Defined Terms and Definitions

[1] This definition has modified the wording of the referenced source definition for consistency with the other definitions

[2] In the Industrial Internet Reference Architecture [IIC-IIRA2019] views and viewpoints include *Business, Usage*, *Functional* and *Implementation*.

6 DISCOURAGED TERMS

The following terms have been identified by the Vocabulary Task Group as ambiguous or conflicting with accepted interpretations. To avoid misunderstandings, we recommend the use of approved alternatives in all future IIoT-related publications. Moreover, replacing the discouraged terms with recommended alternatives in existing documents should be performed when those documents undergo a revision.

Term	Recommended Alternative	Comment
cloud	cloud service	
device endpoint	endpoint	
thing	IoT device, physical entity of interest	
virtual entity	digital twin	

Table 6-1: Discouraged Terms

Annex A Revision History

Revision	Date	Editors	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
V2.3	2020-09-13	Buchheit/Bournival	Minor update, details see Annex B
V3.0	2022-01-31	Buchheit/Bournival	Major update, details see Annex B

Table A-1: Revision History

Annex B TERMS CHANGE HISTORY

Term	Version	Changes Made
Actuating	2.3	Added
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
Attacker	2.3	Updated
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 view	3.0	renamed from business viewpoint, redefined
business viewpoint	2.0	added
business viewpoint	2.1	redefined
business viewpoint	2.3	redefined
cloud computing	2.0	added
cloud computing	2.3	redefined
cloud service	2.3	added
Component	2.1	source changed
Composability	2.1	redefined
computer network	2.3	renamed from network, redefined
computer network	3.0	renamed to digital network
Confidentiality	2.2	redefined
Connectivity	2.1	added
Connectivity	2.3	redefined
connectivity endpoint	2.0	added
Container	3.0	added as short form
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
cyber-physical system	3.0	added
Data	2.1	added

data at rest	2.0	added
data center	2.3	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 representation	3.0	removed
digital twin	2.2	added
digital twin	3.0	redefined
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	2.3	redefined
endpoint address	2.0	removed
environment	3.0	removed
Event	2.0	added
Event	2.3	redefined
Firmware	2.1	removed
functional domain	2.1	redefined
functional view	3.0	renamed from functional viewpoint, redefined
functional viewpoint	2.0	added
functional viewpoint	2.1	redefined
functional viewpoint	2.3	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 view	3.0	renamed from implementation viewpoint, redefined
implementation viewpoint	2.0	added
implementation viewpoint	2.1	redefined
Implementation viewpoint	2.3	redefined
incident response or incident response	2.0	added
industrial control system (ICS)	2.1	added
Industrial Internet of Things (IIoT) system	2.0	added
Industrial Internet of Things (IIoT) system	2.3	redefined
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

infrastructure as a service	3.0	Added
Integrability	2.0	Removed
Internet	2.0	Removed
Internet of Things (IoT)	2.3	Added
Interoperability	2.1	Added
IoT actuator	2.0	renamed from actuator, redefined
IoT actuator	2.2	Redefined
IoT actuator	2.3	Redefined
IoT device	2.0	renamed from device, redefined
IoT device	3.0	Redefined
IoT environment	3.0	Added
IoT sensor	2.0	renamed from sensor, redefined
IoT sensor	2.2	Redefined
IoT sensor	2.3	Redefined
IP endpoint	2.0	Removed
IT/OT convergence	2.1	Added
IT/OT convergence	2.3	Redefined
malware	2.0	Added
man-in-the-middle attack	2.0	Added
model	3.0	Added
model kind	3.0	Added
multi-tenancy	2.0	Added
network	2.0	Redefined
network	2.3	renamed to computer network
network	3.0	added as short form
non-functional requirement	2.3	Added
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
platform as a service	3.0	Added
public key infrastructure (PKI)	2.0	Added
policy	2.0	Removed
privacy	3.0	Redefined
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
safety	3.0	Redefined
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
sensing	2.3	Added
sensitivity	2.0	Removed
sensor	2.0	renamed to IoT sensor
situation awareness	3.0	Redefined
software as a service	3.0	Redefined
syntactic interoperability	2.1	Added
system	2.3	Added
thing	2.0	Removed
trust	2.0	Removed
trustworthiness	2.0	Added
trustworthiness	2.1	Redefined
usage view	3.0	renamed from usage viewpoint, redefined
usage viewpoint	2.0	Added
usage viewpoint	2.1	Redefined
usage viewpoint	2.3	Redefined
user	2.0	Removed
user endpoint	2.0	Removed
view	3.0	added as short form
viewpoint	3.0	added as short form
virtual entity	2.2	Removed
vulnerability assessment	2.0	Removed

Table B-1: 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

[DTC-Glossary] Digital Twin Consortium, Glossary, *Digital Twin*, retrieved 2022-01-09
https://www.digitaltwinconsortium.org/glossary/glossary.html#digital-twin

[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

[IIC-IIRA2019] Industry IoT Consortium: Industrial Internet Reference Architecture Technical Report, v 1.9, 2019, retrieved 2021-04-28
https://www.iiconsortium.org/IIRA.htm

[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

[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

[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

[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*
[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 500-322]	National Institute of Standards and Technology (NIST) Special Publication 500-322: Evaluation of Cloud Computing, 2018-February, retrieved 2022-01-09
[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*

[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

[NISTIR-8316] National Institute of Standards and Technology (NIST) Internal Reports: Internet of Things (IoT) Component Capability Model for Research Testbed, 2020-September, retrieved 2022-01-09
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8316.pdf

AUTHORS AND LEGAL NOTICE

ACKNOWLEDGEMENTS

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

Authors: The following persons, in alphabetical order, contributed substantial written content to this document:

Claude Baudoin (cébé IT & Knowledge Management), Erin Bournival (Dell Technologies), Marcellus Buchheit (Wibu-Systems), Eric Simmon (NIST), Bassam Zarkout (IGnPower)

The following persons, in historical order, contributed substantial written content to former versions of this document:

Jacques Durand (Fujitsu), Ruben Guerrero (Toshiba), Frederick Hirsch (Fujitsu), Birgit Boss (Robert Bosch GmbH), 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), 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, in historical order, contributed valuable ideas and feedback that significantly improved the content and quality of this document:

Chuck Byers (IIC), Mitch Tseng (Tseng InfoServ), Peter van Schalkwyk (XMPro), Nina Tucker (Twin Oaks Computing), Denise Wahl (OMG), Todd Edmunds (Cisco), 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 CTO) oversaw the process of organizing the contributions of the above authors and contributors into an integrated document.