The Industrial Internet of Things
Volume G8: Vocabulary

IIC:PUB:G8:V2.00:PB:20170719

ACKNOWLEDGEMENTS

We acknowledge the work of the members of the Vocabulary Task Group in the Technology Working Group led by Anish Karmarkar (Oracle), who have authored this document.

EDITORS

Anish Karmarkar (Oracle), Marcellus Buchheit (Wibu-Systems)

AUTHORS

The following persons have written substantial portion of material contained in this document:

Anish Karmarkar (Oracle), Frederick Hirsch (Fujitsu), Eric Simmon (NIST), Erin Bournival (Dell EMC), Marcellus Buchheit (Wibu-Systems), Rajive Joshi (RTI), Sven Schrecker (Intel), Shi-Wan Lin (Intel), Jesus Molina (Fujitsu), 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 have contributed valuable ideas and feedback that significantly improved the content and quality of this document:

Claude Baudoin (cébé IT & Knowledge Management), 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).

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*.

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

This Industrial Internet Vocabulary Technical Report specifies a common set of definitions for terms 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 which 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.

1.1 PRINCIPLES

This document contains terms and definitions that are considered relevant and important to the Industrial Internet of Things (IIoT). 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 a 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.

1.2 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 are described at the end of the table.

1.3 RELATIONSHIP WITH OTHER IIC DOCUMENTS

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

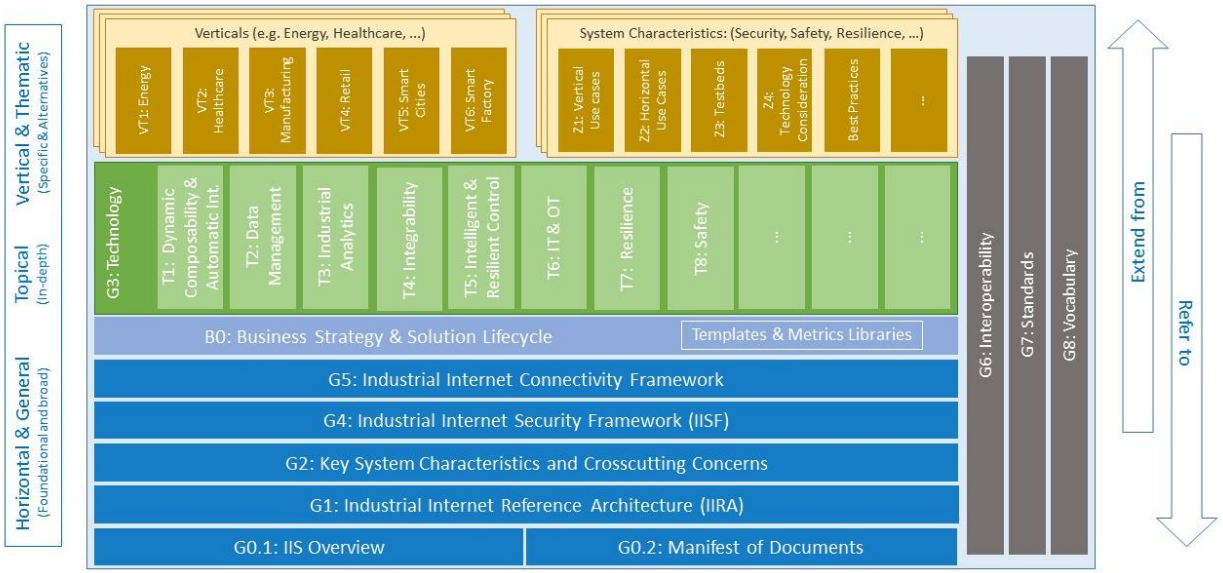

Figure 1-1: IIC Technical Publication Organization

2 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)]
analytics	synthesis of knowledge from information	NIST Interagency Publication 8401-1
application domain[(2)]	collection of functions implementing application logic that realizes specific business functionalities	IIRA
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	work product expressing the architecture of a system from the perspective of specific system concerns	ISO/IEC/IEEE 42010:2011
architecture viewpoint	work product establishing the conventions for the construction, interpretation and use of architecture views to frame specific system concerns	ISO/IEC/IEEE 42010:2011

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	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 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

Term	Definition	Source
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 development	creation, integration and deployment of new hardware and software for legacy systems	IIC
business impact analysis	process of analyzing operational functions and the effect that a disruption might have upon them	ISO/IEC 27031:2011
business viewpoint[(2)]	attends to the concerns of the identification of stakeholders and their business vision, values and objectives in establishing an industrial internet of things (IIoT) system in its business and regulatory context	IIRA
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 network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand **note**: examples of resources include servers, operating systems, networks, software, applications and storage equipment.	ISO/IEC 17788:2014

Term	Definition	Source
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 19104:2016
composability	capability 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, entity or processes	ISO/IEC 27000:2016
connectivity endpoint	interface that provides connectivity	IIC
control domain[(2)]	collection of functions that are performed by industrial control systems **note**: The core of these functions comprises fine-grained closed-loops, reading data from IoT sensors, applying rules and logic, and exercising control over the physical system through IoT actuators.	IIRA
countermeasure	action, device, procedure, technique or other measure that is designed to minimize vulnerability	ISO/IEC 2382:2015
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

Term	Definition	Source
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
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 at rest	stored data that is neither being processed nor transferred	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

Term	Definition	Source
digital representation	data element representing a set of properties of a physical entity	IIC
edge gateway	gateway that provides an entry point into enterprise or service provider core networks	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 so as to hide the information content of the data	ISO/IEC 9798-1:2010
endpoint	component that has computational capabilities and 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)
environment	context determining the setting and circumstances of all interactions and influences with the system of interest **note**: the environment of a system includes developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological and social influences.	ISO/IEC/IEEE 42010:2011(1)
event	any observable occurrence in a system and/or network	NIST SP 800-61
firmware	low-level software for booting and operating an intelligent device **note**: firmware generally resides in persistent memory on the device.	SNIA Dictionary 2016
functional component	functional building block needed to engage in an activity realized by an implementation	ISO/IEC 17789:2014

Term	Definition	Source
functional domain[2]	top-level functional decomposition of an industrial internet of things (IIoT) system that provides a predominantly distinct functionality in the overall 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 viewpoint[2]	functional components in an industrial internet of things (IIoT) system, their structure and interrelation, the interfaces and interactions between them, and the relation and interactions of the system with external elements in the environment, to support the usages and activities of the overall system	IIRA
gateway	forwarding component, enabling various networks to be connected	IOT-A[1]
greenfield development	creation and deployment of new hardware and software	IIC
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

Term	Definition	Source
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
implementation viewpoint[(2)]	technologies needed to implement functional components (functional viewpoint), their communication schemes and their lifecycle procedures **note**: these elements are coordinated by activities (usage viewpoint) and supportive of the system capabilities (business viewpoint).	IIRA
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 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 (IIoT) system	system that connects and integrates industrial control systems with enterprise systems, business processes and analytics **note 1**: industrial control systems contain sensors and actuators. **note 2:** typically, these are large and complicated system.	IIC

Term	Definition	Source
information domain[(2)]	collection of functions for gathering data from various domains, most significantly from the control domain and transforming, persisting, and modeling or analyzing those data to acquire high-level intelligence about the overall system	IIRA
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
infrastructure service	service that is essential for any IoT implementation to work properly **note**: Infrastructure services provide support for essential features of the IoT.	IOT-A
integrity	property of accuracy and completeness	ISO/IEC 27000:2016
interface	named set of operations that characterize the behavior of an entity	IOT-A
IoT actuator	IoT device that can change a property of a physical entity in response to an input	IIC
IoT device	endpoint that interacts with the physical world through sensing or actuating	IIC
IoT sensor	IoT device that observes properties of the physical world and converts them into a digital form	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

Term	Definition	Source
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
multi-tenancy	allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another	ISO/IEC 17788:2014
network	collection of communicating endpoints	IIC
non-functional requirement	requirement that defines the overall qualities or attributes of the resulting system **note**: 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 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[(2)]	collection of functions responsible for the provisioning, management, monitoring and optimization of the systems in the control domain	IIRA
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
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

Term	Definition	Source
personally identifiable information (PII)	any 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 that is the subject of monitoring and control actions	IIC
physical security	measures used to provide physical protection of resources against deliberate and accidental threats	ISO 7498-2:1989
PKI (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
privacy	right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed	ISO/TS 17574:2009
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

Term	Definition	Source
programmable logic controller (PLC)	electronic device designed for control of the logical sequence of events	ISO 13577-4:2014
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

Term	Definition	Source
risk evaluation	process of comparing the results of risk analysis with risk criteria to determine whether the 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	cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type	ISO/IEC 17788:2014

Term	Definition	Source
safety	the condition of the system operating without causing unacceptable risk of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment	ISO/IEC Guide 55:1999(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

Term	Definition	Source
service	distinct part of the functionality that is provided by an entity through interfaces	ISO/IEC TR 14252:1996
situational awareness	within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together risk); and the projection of their status into the near future	NISTIR 7298, rev 2
stakeholder	individual, team, organization or classes thereof, having an interest in the system of interest	ISO/IEC/IEEE 42010:2011[(1)]
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 level 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 disruptions, 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

Term	Definition	Source
usage viewpoint[2]	addresses the concerns of expected system usage **note**: it is typically represented as sequences of activities involving human or logical (e.g. system or system components) users that deliver its intended functionality in ultimately achieving its fundamental system capabilities.	IIRA
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
virtual entity	computational or data entity representing a physical entity	IIC
vulnerability	weakness of an asset or security controls that can be exploited by one or more threats	ISO/IEC 27000:2016[1]

Table 2-1: Defined Terms and Definitions

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

(2) This term and its definition are reproduced here from the Reference Architecture [IIC-IIRA2016] and the definition is likely to change in subsequent versions of both the IIRA and this document.

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

Table A-2: Revision History

Annex B TERMS CHANGE HISTORY

Term	Version	Changes Made
actuator	2.00	renamed to IoT actuator
application domain	2.00	added
architecture	2.00	added
architecture viewpoint	2.00	added
asset	2.00	added
attack surface	2.00	added
attack vector	2.00	redefined
attacker	2.00	added
attestation	2.00	added
audit	2.00	added
automatic	2.00	removed
automation	2.00	removed
brownfield development	2.00	added
business viewpoint	2.00	added
cloud computing	2.00	added
connectivity endpoint	2.00	added
control domain	2.00	added
controller	2.00	removed
coordinate	2.00	removed
coordination	2.00	removed
countermeasure	2.00	added
credential	2.00	added
cross-cutting concern	2.00	redefined
cross-cutting function	2.00	redefined
data at rest	2.00	added
data in motion	2.00	added
data in use	2.00	added
data integrity	2.00	added
databus	2.00	added
denial of service (DoS)	2.00	added
device	2.00	renamed to IoT device
device endpoint	2.00	removed
digital representation	2.00	added
element	2.00	redefined
encryption	2.00	added
endpoint	2.00	redefined
endpoint address	2.00	removed
event	2.00	added
functional viewpoint	2.00	added
greenfield development	2.00	added
identity	2.00	redefined
implementation viewpoint	2.00	added
incident response or incident response	2.00	added
industrial internet of thing (IIoT) system)	2.00	added
information domain	2.00	added

Term	Version	Changes Made
information security incident	2.00	added
integrability	2.00	removed
internet	2.00	removed
IoT actuator	2.00	renamed from actuator, redefined
IoT device	2.00	renamed from device, redefined
IoT sensor	2.00	renamed from sensor, redefined
IP endpoint	2.00	removed
malware	2.00	added
man-in-the-middle attack	2.00	added
multi-tenancy	2.00	added
network	2.00	redefined
non-repudiation	2.00	added
observer	2.00	removed
operational technology (OT)	2.00	added
operations domain	2.00	added
physical security	2.00	added
PKI (public key infrastructure)	2.00	added
policy	2.00	removed
process	2.00	added
programmable logic controller (PLC)	2.00	added
resilience	2.00	redefined
risk response	2.00	redefined
robustness	2.00	redefined
roots of trust	2.00	added
SaaS	2.00	added
security	2.00	redefined
security control	2.00	renamed to security controls
security controls	2.00	renamed from security control, redefined
security function	2.00	renamed from security functions, corrected
security functions	2.00	renamed to security function
security vulnerability assessment	2.00	added
sensitivity	2.00	removed
sensor	2.00	renamed to IoT sensor
thing	2.00	removed
trust	2.00	removed
trustworthiness	2.00	added
usage viewpoint	2.00	added
user	2.00	removed
user endpoint	2.00	removed
vulnerability assessment	2.00	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

[IIC-IIRA2016] Industrial Internet Consortium (IIC): Industrial Internet of Things, Volume G1: Reference Architecture, version 1.80, 2017-January-31, retrieved 2017-05-29
http://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-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-19104] International Organization for Standardization: ISO 19104:2016: Geographic information—Terminology, 2016-October, retrieved 2017-05-29 *https://www.iso.org/standard/63541.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-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-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

[SNIA-Dict2016] Storage Networking Industry Association (SNIA): SNIA Dictionary 2016, 2016-April, retrieved 2017-05-29
https://www.snia.org/content/download-snia-dictionary

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 listed above have granted to the Object Management Group, Inc. (OMG) and its Industrial Internet Consortium (the "IIC") a nonexclusive, irrevocable, 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 copyright holders listed above has agreed that no person shall be deemed to have infringed the copyright in the included material of any such copyright holder by reason of having copied, distributed or used such material set forth herein.

Subject to all of the terms and conditions below, the owners of the copyright in this Document hereby grant you a fully-paid up, non-exclusive, nontransferable, perpetual, 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 the IIC 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 disclaims 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 Licenses, 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. THE OBJECT MANAGEMENT GROUP, INC. (INCLUDING THE IIC) AND THE COPYRIGHT OWNERS LISTED ABOVE MAKE NO WARRANTY, REPRESENTATION OR CONDITIONS OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS DOCUMENT, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF TITLE OR OWNERSHIP, ANY IMPLIED WARRANTY OR MERCHANTABILITY OR ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE OR USE. IN NO EVENT SHALL THE OBJECT MANAGEMENT GROUP, INC. (INCLUDING THE IIC) OR ANY OF THE COPYRIGHT OWNERS BE LIABLE FOR ERRORS CONTAINED HEREIN OR FOR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, RELIANCE OR COVER DAMAGES, INCLUDING LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY ANY USER OR ANY THIRD PARTY IN CONNECTION WITH THE FURNISHING, PERFORMANCE, REPRODUCTION, DISTRIBUTION OR USE OF THIS MATERIAL, EVEN IF 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 Licenses 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 the 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 copyright holders listed above 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.