Industrial Internet Vocabulary

tech-vocab.tr.001 2015-05-07 Version 1.0 (approved)

TABLE OF CONTENTS

USE OF INFORMATION - TERMS, CONDITIONS & 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 company's products or services. The information contained in this Document is subject to change without notice.

LICENSES

PATENTS

The attention of readers is directed to the possibility that 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 shall not be 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 or other intellectual property.

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, IMPLIED WARRANTY OF MERCHANTABILITY OR 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, 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 license granted to you to use this Document.

IIC Issue Reporting

All IIC documents are subject to continuous review and improvement. As part of this process, we encourage members to report any ambiguities, inconsistencies, or inaccuracies they may find in this Document or other IIC materials by providing comments in the Technology Working Group Kavi workspace.

Acknowledgements

This document is a work product of the Industrial Internet Consortium Technology Working Group, co-chaired by Shi-Wan Lin (Intel) and Bradford Miller (GE), in collaboration with the Security Working Group, chaired by Sven Schrecker (Intel).

EDITORS

Shi-Wan Lin (Lead, Intel), Stephen Mellor (Lead, IIC), Bradford Miller (Lead, V1.5, GE), Jacques Durand (Fujitsu), Mark Crawford (SAP) and Robert Lembree (V1.5, Intel).

AUTHORS [1]

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

Shi-Wan Lin (Intel), Bradford Miller (GE), Jacques Durand (Fujitsu), Rajive Joshi (RTI), Paul Didier (Cisco), Amine Chigani (GE), Reinier Torenbeek (RTI), David Duggal (EnterpriseWeb), Robert Martin (MITRE), Graham Bleakley (IBM), Andrew King (University Of Pennsylvania), Jesus Molina (Fujitsu), Sven Schrecker (Intel), Robert Lembree (Intel), Hamed Soroush (RTI), Jason Garbis (RSA), Mark Crawford (SAP), Eric Harper (ABB), Kaveri Raman (AT&T), and Brian Witten (Symantec)

CONTRIBUTORS [2]

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

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)

We are also grateful to everyone who made comments on the draft version available to the Architecture Task Group, and will thank in advance anyone who provides further constructive comments on the current version.

We acknowledge the work by the members of the Vocabulary Team in the Technology Working Group led by Tom Rutt (Fujitsu), who have authored the Industrial Internet Vocabulary that is a companion document to this one.

[1] This list of authors may be incomplete at this time. If you contributed written material content to this draft but are not listed, please contact Stephen Mellor at mellor@iiconsortium.org.

[2] This list of contributors may be incomplete at this time. If you contributed substantial ideas and feedback to this draft but are not listed, please contact Stephen Mellor at mellor@iiconsortium.org.

Finally, we are grateful for the ongoing support of Aaron Soellinger (IIC), whose diligence with supporting the tools and the mechanics of the document writing have made this process possible.

1 Introduction

This specification is the Industrial Internet Vocabulary Technical Report. This Technical Report specifies a common set of definitions for terms, to be referenced and used by all IIC documentation.

Each of the terms is 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. The symbol ++ implies that our definition has modified the wording of the referenced source definition for consistency with the other definitions.

When a definition uses another term which is defined in the vocabulary, that term is shown using the style ***embeddedTerm,*** and is rendered as a hyperlinked cross reference to the definition of that term in the table.

The category column indicates a major section of the vocabulary the term is associated with:

- arch: these architecture related terms from ISO architecture standards, and the NIST CPS WG
- base: these terms are basic to IOT, and are aligned with IOT-A
- comp: these composition related terms are imported from ISO SOA Standards
- id: these identity related terms are imported from ISO security standards
- sec: these additional security related terms are imported from ISO security standards
- inf: information and data management terms

2 Definitions of Terms

Term	Definition	Source	Category
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 27000:2014	id
activity	a 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 ++	arch
actuator	A ***device*** which conveys digital information to effect a change of some property of a ***physical entity***	IOT-A++	base
analytics	synthesis of knowledge from information	NIST Interagency Publication 8401-1	inf
architecture description	work product used to express an architecture	ISO/IEC 42010:2011	arch
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 42010:2011	arch
architecture layer	A logical partitioning of the architecture	IIC	arch
architecture view	work product expressing the architecture of a system from the perspective of specific system ***concerns***	ISO/IEC 42010:2011	arch
architecture viewpoint	work product establishing the conventions for the construction, interpretation and use of ***architecture views*** to frame specific system ***concerns***	ISO/IEC 42010:2011	arch
assurance	grounds for justified confidence that a claim has been or will be achieved	ISO/IEC TR 15026-1:2010	sec
attack vector	path or means (e.g. viruses, e-mail attachment, Web pages, etc.) by which an attacker can gain access to a computer or network server in order to deliver malicious payloads or outcome.	IIC	sec

attribute	characteristic or property of an ***entity*** that can be used to describe its state, appearance, or other aspects	ISO/IEC 24760-1:2011	id
authenticated identity	***identity information*** for an ***entity*** created to record the result of ***identity authentication***	ISO/IEC 24760-1:2011	id
authentication	provision of assurance that a claimed characteristic of an ***entity*** is correct	ISO/IEC 27000:2014	id
authorization	granting of rights, which includes the granting of access based on access rights Note: Authorization results in privileges.	ISO 7498-2:1989	id
automatic	working by itself with little or no direct human control	ODE	comp
automation	The use or introduction of ***automatic*** equipment in a manufacturing or other process or facility. Note: Automation emphasizes efficiency, productivity, quality, and reliability, focusing on systems that operate without direct control, often in structured environments over extended periods, and on the explicit structuring of such environments.	ODE	comp
autonomy	The 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	comp
availability	property of being accessible and usable upon demand by an authorized ***entity***	ISO/IEC 27000:2014	sec
business impact analysis	process of analyzing operational functions and the effect that a disruption might have upon them	ISO/IEC 27031:2011	sec
choreography	Type of ***composition*** whose ***elements*** interact in a non-directed fashion with each ***autonomy*** part knowing and following an observable predefined pattern of behavior for the entire (global) ***composition***	ISO/IEC DIS 18834-1	comp

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 DIS 18834-1	comp
component	modular, deployable, and replaceable part of a system that encapsulates implementation and exposes a set of ***interfaces***	ISO/TS 19104:2008	base
composition	Result of assembling a collection of ***elements*** for a particular purpose	ISO/IEC DIS 18834-1	comp
composability	capability of a component to interact with any other component in recombinant fashion to satisfy requirements based on the expectation of the behaviors of the interacting parties.	IIC	comp
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 42010:2011	arch
confidentiality	property that information is not made available or disclosed to unauthorized individuals, ***entity***, or processes	ISO/IEC 27000:2014	sec
controller	***user*** that interacts across a network to affect a ***physical entity*** .	IOT-A ++	base
coordinate	Bring the different element**s** of (a complex activity or organization) into a harmonious or efficient relationship	ODE	comp
coordination	The organization of the different ***elements*** of a complex body or activity so as to enable them to work together effectively	ODE	comp
criticality	A 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 R2 ++	sec

cross-cutting concern	***concern*** that affects the whole system and thus may impact multiple layers of the architecture.	IIC	arch
cross-cutting function	a function that may be applied and realized across multiple layers of the architecture to address ***cross-cutting concerns***.	IIC	arch
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	sec
device	***physical entity*** embedded inside, or attached to, another ***physical entity*** in its vicinity, with capabilities to convey digital information from or to that ***physical entity*** .	IIC	base
device endpoint	***endpoint*** that enables access to a ***device*** and thus to the related ***physical entity*** .	IIC	base
edge gateway	***gateway*** that provides an entry point into enterprise or service provider core networks	IIC	base
element	Unit that is indivisible at a given level of abstraction and has a clearly defined boundary Note: An element can be any type of entity	ISO/IEC DIS 18834-1	comp
emergent behavior	behavior of a system realized by the interactions of its ***components***.	IIC	arch
endpoint	one of two ***components*** that either implements and exposes an ***interface*** to other ***components*** or uses the ***interface*** of another ***component***	ISO/IEC 24791-1:2010	base
endpoint address	data element designating the originating source or destination of data being transmitted	ISO 14814:2006	base
entity	item that has recognizably distinct existence Note: eg., a person, an organization, a device, a subsystem, or a group of such items	ISO/IEC 24760-1:2011 ++	id

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 42010:2011 ++	arch
firmware	low-level software for booting and operating an intelligent device. Note: Firmware generally resides in persistent memory on the device	SNIA Dictionary	sec
functional component	functional building block needed to engage in an ***activity*** realized by an implementation.	ISO/IEC 17789:2014	arch
functional domain	top-level functional decomposition of an Industrial Internet System that provides a predominantly distinct functionality in the overall system	IIC	arch
functional framework	a set of abstract re-useable ***functional components*** that can be extended/customized and applied to several applications in a specific domain.	IIC	arch
gateway	forwarding ***component***, enabling various networks to be connected.	IOT-A ++	base
identification	process of recognizing an ***entity*** in a particular ***identity domain*** as distinct from other ***entity***	ISO/IEC 24760-1:2011	id
identifier	identity ***information*** that unambiguously distinguishes one ***entity*** from another one in a given ***identity domain***	ISO/IEC 24760-1:2011	id
identity	the characteristics determining who or what a person or thing is	ODE	id
identity authentication	formalized process of ***identity verification*** that, if successful, results in an ***authenticated identity*** for an ***entity***	ISO/IEC 24760-1:2011	id
identity domain	environment where an ***entity*** can use a set of ***attributes*** for ***identification*** and other purposes	ISO/IEC 24760-1:2011	id

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	id
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	id
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	id
industrial internet	An ***internet*** of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes.	IIC	base
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	sec
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	base
integrability	capability to communicate with each other based on compatible means of signaling and protocols	IIC	comp
integrity	property of accuracy and completeness	ISO/IEC 27000:2014	sec
interface	named set of operations that characterize the behavior of an ***entity***.	IOT-A	base
internet	computer network connecting two or more smaller networks.	ODE	base
IP endpoint	***endpoint*** which has an IP ***endpoint address***.	IIC	base

Least Privilege	The 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 R2	sec
network	a system of interconnected ***endpoints***	IIC	sec
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 specifies external constraints that the system must meet.	IIC	arch
observer	***user*** that interacts across a network to monitor a ***physical entity*** .	IOT-A ++	base
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 DIS 18834-1	comp
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 ***activity*** Note: A party may assume more than one roles, and a role may be fulfilled by several parties (i.e. by any one of them).	IIC	arch
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	sec
physical entity	***entity*** that is the subject of monitoring and control actions.	IOT-A ++	base

policy	definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions	Merriam Webster Collegiate , 11th ed	id
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	sec
privacy risk assessment	overall process of risk identification, risk analysis and risk evaluation with regard to the processing of ***personally identifiable information – (PII)*** Note: This process is also known as a privacy impact assessment	ISO/IEC 29100:2011	sec
privilege	right granted to an individual, a program, or a process.	CNSSI-409	sec
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	sec
resilience	the condition of the system being able to avoid, absorb and/or manage dynamic adversarial conditions while completing assigned mission(s), and to reconstitute operational capabilities after casualties	IIC	sec

risk	effect of uncertainty on objectives Note 1 to entry: An effect is a deviation from the expected — positive or negative. Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence or likelihood. Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these. Note 4 to entry: 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 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives. Note 6 to entry: 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 27000:2014	sec
risk analysis	process to comprehend the nature of ***risk*** and to determine the level of ***risk*** Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Note 2 to entry: Risk analysis includes risk estimation	ISO/IEC 27000:2014	sec
risk assessment	overall process of ***risk identification***, ***risk analysis*** and ***risk evaluation***	ISO/IEC 27000:2014	sec
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 1 to entry: Risk evaluation assists in the decision about risk treatment .	ISO/IEC 27000:2014	sec
risk identification	process of finding, recognizing and describing ***risk*** Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs	ISO/IEC 27000:2014	sec
risk management	coordinated activities to direct and control an organization with regard to ***risk***	ISO/IEC 27000:2014	sec

risk response	Accepting, avoiding, mitigating, sharing, or transferring ***risk*** to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.	NISTIR 7298 R2	sec
risk tolerance	level of ***risk*** an ***entity*** is willing to assume in order to achieve a potential desired result.	NISTIR 7298 R2	sec
robustness	ability of an Information Assurance ***entity*** to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.	NISTIR 7298 R2	sec
role	set of ***usage capacity*** Note: A role is an abstraction for an entity which performs the set of activities Roles are fulfilled or assumed by parties.	IIC	arch
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 ++	sec
security	condition of the system being protected from unintended or unauthorized access, change or destruction. Note: Security is a property of a system by which ***confidentiality***, integrity, availability, accountability, authenticity, and reliability are achieved (ISO TR 15443-1:2012)	IIC	sec
security control	measure that is modifying ***risk*** Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk. Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.	ISO/IEC 27000:2014	sec

security functions	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	ISO/IEC 19790:2012 ++	sec
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 R2	sec
sensitivity	measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.	NISTIR 7298 R2	sec
sensor	***device*** that perceives certain characteristics of the real world and transfers them into a digital representation.	IOT-A	base
service	distinct part of the functionality that is provided by an ***entity*** through ***interfaces***	ISO/TR 14252:1996	base
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 R2	sec
stakeholder	individual, team, organization, or classes thereof, having an interest in the system of interest	ISO/IEC 42010:2011 ++	arch
task	a unit of work	IIC	arch
thing	physical object Note: In the term 'Internet of Things', thing denotes the same concept as a physical entity**.**	IOT-A	base
threat	potential cause of an unwanted incident, which may result in harm to a system or organization	ISO/IEC 27000:2014	sec

threat analysis	The examination of ***threat*** sources against system vulnerabilities to determine the threats for a particular system in a particular operational ***environment***.	NISTIR 7298 R2	sec
threat event	An event or situation that has the potential for causing undesirable consequences or impact.	NISTIR 7298 R2	sec
threat modeling	structured analysis to identify, quantify, and address the ***information security risk***s associated with an application or a system.	IIC	sec
trust	relationship between two ***entity*** and/or ***elements***, consisting of a set of ***activity*** and a ***security policy*** in which element x trusts element y if and only if x has confidence that y will behave in a well-defined way (with respect to the activities) that does not violate the given ***security policy***	ISO/IEC 27036-1:2014	sec
trust boundary	separation of different application or system domains in which different level of ***trust*** are required	IIC	sec
usage capacity	the ability to initiate, to participate in the execution of, or to consume the outcome of some ***tasks*** or functions.	IIC	arch
user	An ***entity*** that is interested in interacting with a particular ***physical entity*** .	IOT-A ++	base
user endpoint	An ***endpoint*** used by a ***user*** to interact.	IIC	base
validation	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled	ISO/IEC 27000:2014	sec
verification	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled Note 1 to entry: This could also be called compliance testing.	ISO/IEC 27000:2014	sec
virtual entity	computational or data element representing a ***physical entity*** .	IOT-A	base

vulnerability	weakness of an asset or ***security control*** that can be exploited by one or more ***threats***	ISO/IEC 27000:2014	sec
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 R2	sec

3 Sources

The list below references the sources used for the definitions.

CNNSI 409	Committee on National Security Systems National Information Assurance (IA) Glossary http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf
IHMC	http://www.ihmc.us/groups/datkinson/wiki/fcb0e/intelligent_system_autonomy_automation_robots_and_agents.html
IOT-A	EU IOT-A Terminology http://www.iot-a.eu/public/terminology/copy_of_term
ISO 27789:2013	Health informatics -- Audit trails for electronic health records
ISO 7498-2:1989	Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture
ISO TS 19104:2008	Geographic information – Terminology
ISO/IEC 14814:2006	Road transport and traffic telematics — Automatic vehicle and equipment identification — Reference architecture and terminology
ISO/IEC 18014-2:2009	Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens
ISO/IEC 19790:2012	Information technology -- Security techniques -- Security requirements for cryptographic modules
ISO/IEC 24745:2011	Information technology -- Security techniques -- Biometric information protection
ISO/IEC 24760-1:2011	Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts
ISO/IEC 24791-1:2010	Information technology — Radio frequency identification (RFID) for item management — Software system infrastructure — Part 1: Architecture
ISO/IEC 27000:2014	Information technology — Security techniques — Information security management systems — Overview and vocabulary http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip.
ISO/IEC 27005:2008	Information technology -- Security techniques -- Information security risk management

ISO/IEC 27036-1:2014	Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts
ISO/IEC 27040:2015	Information technology -- Security techniques -- Storage security
ISO/IEC 29100:2011	Information technology -- Security techniques -- Privacy framework
ISO/IEC DIS 18834-1	RA SOA – Terminology and Concepts
ISO/IEC TR 15026-1:2010	Systems and software engineering -- Systems and software assurance -- Part 1: Concepts and vocabulary
ISO/IEC TR 15443-1:2012	Information technology -- Security techniques -- Security assurance framework -- Part 1: Introduction and concepts
ISO/IEC/IEEE 42010:2011	Systems and software engineering -- Architecture description
ISO/TS 17574:2009	Electronic fee collection - Guidelines for security protection profiles
ISO/TS 19129:2009	Geographic information — Imagery, gridded and coverage data framework
NIST Interagency Publication 8401-1	DRAFT NIST Big Data Interoperability Framework: Volume 1, Definitions Draft Version 1 - http://bigdatawg.nist.gov/_uploadfiles/M0357_v2_4404462833.docx
NISTIR 7298 R2	Glossary of Key Information Security Terms http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
ODE	Oxford Dictionary of English, 2nd Edition, Oxford University Press

4 Annex A: Relationships between Base Vocabulary Terms

The following figure is a UML class model that shows the relationships between the base vocabulary terms as associations between UML Classes for each IIC Base Vocabulary Term.

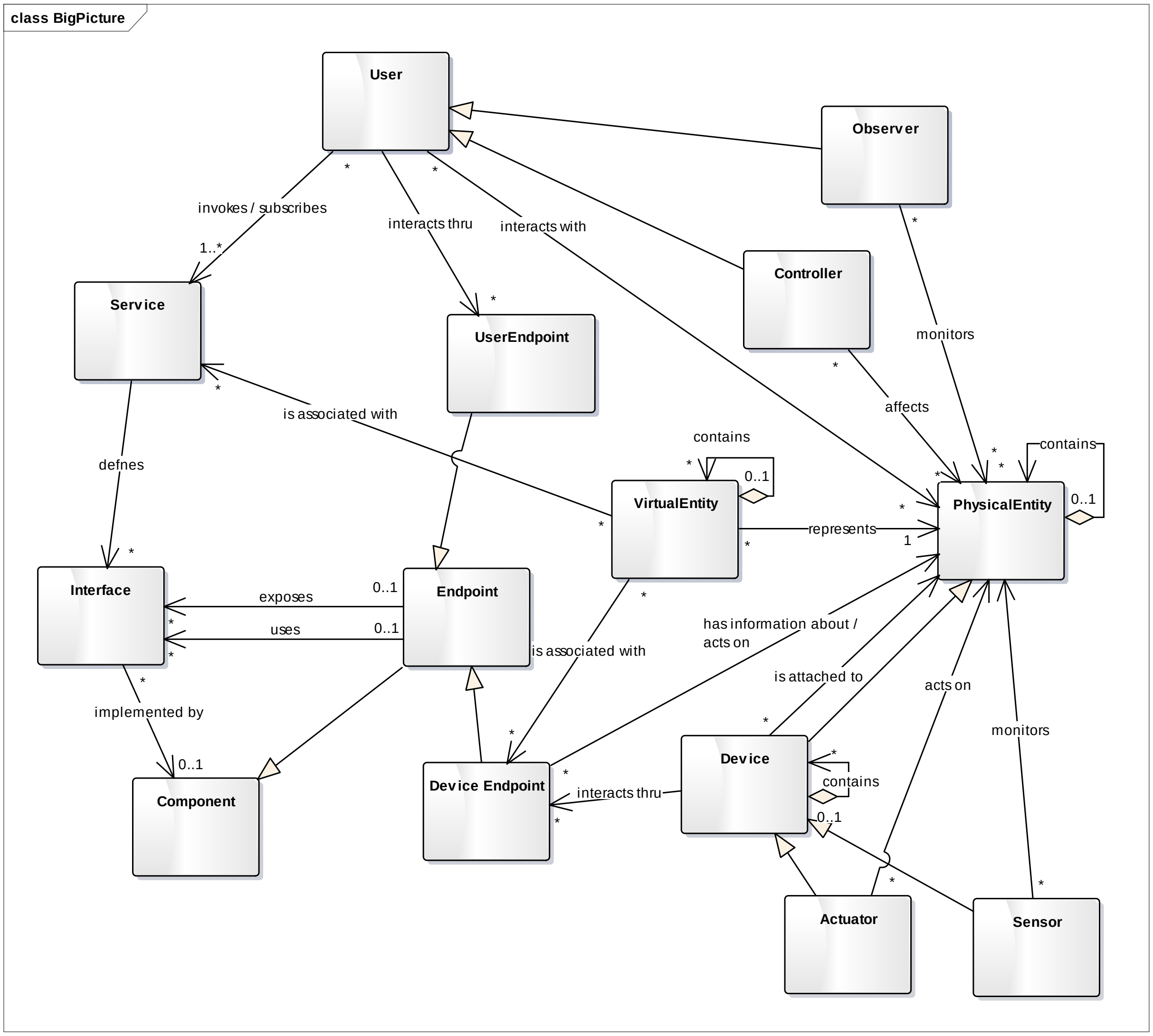

Figure 1: IIC Base Vocabulary Model

Each class on the model represents a defined term. Generalizations (is a relationships) are shown by an open triangle arrow head, aggregations by an open-diamond arrow head, and simple associations are shown using directed simple headed arrows. Cardinality constraints (when specified) are shown at each end of the associations. Some of the network related Base Vocabulary terms (e.g, endpoint address, gateway) are not shown in this diagram.

5 REFERENCES

There are no sources in the current document.