

IEEE Standard for an Architectural Framework for the Internet of Things (IOT)

IEEE Computer Society

Developed by the
IEEE SA Board of Governors/Corporate Advisory Group (BoG/CAG)

IEEE Std 2413™-2019

STANDARDS

IEEE Standard for an Architectural Framework for the Internet of Things (IoT)

Developed by the

IEEE SA Board of Governors/Corporate Advisory Group (BoG/CAG)
of the
IEEE Computer Society

Approved 21 May 2019

IEEE SA Standards Board

Abstract: An architecture framework description for the Internet of Things (IoT) which conforms to the international standard ISO/IEC/IEEE 42010:2011 is defined. The architecture framework description is motivated by concerns commonly shared by IoT system stakeholders across multiple domains (transportation, healthcare, Smart Grid, etc.). A conceptual basis for the notion of things in the IoT is provided and the shared concerns as a collection of architecture viewpoints is elaborated to form the body of the framework description.

Keywords: architectural framework, IEEE 2413™, Internet of Things (IoT)

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2020 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 10 March 2020. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-5886-3 STD23719
Print: ISBN 978-1-5044-5887-0 STDPD23719

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/ipr/disclaimers.html>.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and

adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore at <http://ieeexplore.ieee.org/> or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for IEEE standards can be accessed via <https://standards.ieee.org/standard/index.html>. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore: <https://ieeexplore.ieee.org/browse/standards/collection/ieee/>. Users are encouraged to periodically check for errata.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE standard was completed, the Internet of Things (IoT) Architecture Working Group had the following membership:

Oleg Loginov, *Chair*
Ludwig Winkel, *Vice Chair*

Siby Abraham
Yoshiaki Adachi
Chuck Adams
Roberto Aiello
Jim Allen
Wilson Ang
Masayuki Ariyoshi
Marilyn Arndt
Yasuo Bakke
Martin Bauer
Rajdeep Bhowmik
Zhen Bin
Josef Blanz
Pat Brett
Paul Brooks
Dennis Brophy
Phillip Brown
Timothy Carey
Joseph Carr
Samita Chakrabarti
Rabindra Chakraborty
Lihao Chen
Penny Chen
Howard Choe
Koh Lian Chong
Sim Bak Chor
Andrew Cofler
Graham Cunliffe
Nicolas Damour
Chen De
Jean-Pierre Desbenoit
Wael Diab
Jeff Drake
Sophie Dumas
Ed Eckert
Rouzbeh Farhoumand
Jean Philippe Faure
Jeff Fedders
Ray Forbes
Ingo Friese
Rob Gillan
Tim Godfrey
Tinlin Gug
Sebastian Hans
Xuan He
Bob Heile
Juergen Heiles
SeonMeyong Heo
Betsy Hawkinson
Martin Hoglinger
Thomas Hott

Joel Huloux
Paul Hunkar
Daisuke Ishii
Naoki Ito
Shogo Iwaki
Antonio Jara
Emery Jou
Rajah Kalipatnapu
Jay Kalra
Jeffrey Katz
David Kaufman
Anil Keshavamurthy
Taizo Kinoshita
Douglas Knisely
Soumitri Kolavennu
Semen Kort
Bruce Kraemer
Victor Kueh
Sue Leight
Gadi Lenz
Jidong Li
Jinhui Li
Min Liu
Mark Lynass
Santosh Madathil
Brenda Mancuso
Hiroshi Mano
Hirofumi Masukawa
Tetsushi Matsuda
Toshiko Matsumoto
John Messina
Pascal Moniot
Masaki Nakano
Haewoon Nam
Philippe Nappey
Lee Neitzel
Vien Nguyen
Lei Ning
Hiroaki Nishi
Shinji Oda
Marie-Paule Oadini
Ken Ogiso
Nobuyuki Ogura
Richard Oh
François Oudot
Harirajan Padmanabhan
Jing Pan
Sylvain Paineau
Andreas Pfaff
Harish Pillay
Nathan Pocock

Benoit Ponsard
Daniel Popa
Steve Pridie
Buaey Qui
Demir Rakanovic
Imir Rashid
Tobin Richardson
Mika Rissa
Sandra Roggeveen
Eric Rotvold
Ekaterina Rudina
Francesco Russo
Manas Saksena
Rashid Sangi
Jun Sato
Maik Seewald
Yang Shan
Mayank Sharma
Jie Shen
Masahiro Shimohori
Hitoshi Shirakabe
Eric Simmon
Rodney Sloan
Matthew D. Smith
Daniel Smolinski
Joe So
Alexandru Soceanu
Praveena Sridhar
Klaus Starnberger
Gary Stuebing
Padmakumar Subramani
Stefan Svensson
Masaki Tanaka
Mukesh Taneja
Shigeyuki Tani
Antonio Tassone
Pat Thaler
Gilles Thonet
Larry Wagoner
Yasushi Wakayama
Joachim Walewski
Andy Wang
Dun Wang
Guichun Wang
Xiaofeng Wang
Cliff Whitehead
Euntae Won
Chen Wu
Tao Xing
Dayin Xu
Daoyan Yang

Mike Yao
Wei Yong
Nie Yongfeng

Kohei Yoshida
Tao Zhang
Tengji Zhang

Yongjing Zhang
Slava Zolotnikov
Juan Carlos Zuniga

The following members of the entity balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Beckhoff Automation
BII Group Holdings Ltd.
Chaincomp Technologies Co.,
Ltd.
Cisco Systems, Inc.
Electric Power Research
Institute, Inc. (EPRI)

Ericsson AB
Huawei Technologies Co., Ltd.
IoTecha Corp.
Kaspersky Labs Limited
National Taiwan University
Nokia
Panasonic Corporation of North
America

Power Plus Communications AG
Rockwell Automation
Schneider Electric
Siemens Corporation
STMicroelectronics
Wi-SUN Alliance
Yokogawa Electric Corporation

When the Standards Board approved this standard on 21 May 2019, it had the following membership:

Gary Hoffman, *Chair*
Ted Burse, *Vice Chair*
Jean-Philippe Faure, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
Stephen D. Dukes
J. Travis Griffith
Guido Hiertz
Christel Hunter
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick

David J. Law
Joseph Levy
Howard Li
Xiaohui Liu
Kevin Lu
Daleep Mohla
Andrew Myles
Annette D. Reilly

Dorothy Stanley
Sha Wei
Phil Wennblom
Philip Winston
Howard Wolfman
Feng Wu
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2413-2019, IEEE Standard for an Architectural Framework for the Internet of Things (IoT).

This document has four logical parts:

- **Part 1: IoT domains**
 - Description of behaviors and applications of IoT domains (see Clause 4)
- **Part 2: Domain commonalities and shared concerns**
 - Discussion of the core characteristics across IoT domains (see Clause 5)
- **Part 3: IoT architecture framework**
 - ISO/IEC/IEEE 42010:2011 conformant description of the architecture framework (see Clause 6)¹
- **Part 4: Examples of IoT architectures**
 - Domain-specific ISO/IEC/IEEE 42010:2011 conformant architectural description

¹ Information on references can be found in Clause 2.

Contents

1. Overview	12
1.1 Scope	12
1.2 Purpose	12
1.3 Introduction to the Internet of Things (IoT)	13
1.4 Architecture method	16
2. Normative reference	17
3. Definitions, acronyms, and abbreviations	17
3.1 Definitions	17
3.2 Acronyms and abbreviations	22
4. IoT domains.....	25
4.1 Abstract IoT Domain	25
4.2 Smart Manufacturing	26
4.3 Smart Grid	27
4.4 Smart buildings.....	28
4.5 Intelligent Transport Systems	28
4.6 Smart Cities	30
4.7 Healthcare.....	35
5. Domain commonalities and common concerns	36
5.1 Stakeholders	36
5.2 Common concerns	36
6. Architecture framework.....	40
6.1 General information.....	40
6.2 Viewpoints and model kinds	41
6.3 Architecture development.....	44
6.4 Rationale for key decisions.....	44
6.5 Stakeholders and concerns.....	44
6.6 Viewpoint catalogue	44
7. Architecture examples	163
7.1 General	163
7.2 Example architecture of system A	163
7.3 Example architecture of adequate design for required security	163
7.4 Example architecture of edge computing	168
7.5 Example architecture of IoT platform for Smart Cities	173
7.6 Example architecture of OPC Unified Architecture (UA).....	188
7.7 Example architecture of a distributed computing architecture for a chemical process in a Smart Manufacturing Ecosystem using BATCH control	194
7.8 Example architecture of oneM2M	227
7.9 Example architecture of Industrial Value Chain Initiative—reference architecture (IVI-RA).....	236
Annex A (informative) Examples of system collaboration based on collaboration viewpoint.....	244
A.1 Introduction	244
A.2 Symbiotic ADS.....	244
A.3 Examples	248
Annex B (informative) Common concerns and stakeholder mapping	253

B.1 Common concerns mapping.....	253
B.2 IoT stakeholder mapping	255
Annex C (informative) An example based on threat model viewpoint	256
Annex D (informative) An example based on an adequate design for required security viewpoint.....	259
D.1 Example	259
D.2 Information for better understanding of this viewpoint	259
Annex E (informative) Bibliography.....	261
Annex F ANSI INCITS 359-2004, American National Standard for Information Technology Role Based Access Control (RBAC).	261

IEEE Standard for an Architectural Framework for the Internet of Things (IoT)

1. Overview

1.1 Scope

This standard defines an architecture framework description for the Internet of Things (IoT). The architecture ontology and methodology of the framework architecture conforms to the international standard ISO/IEC/IEEE 42010:2011.

The architecture framework description is motivated by concerns commonly shared by IoT system stakeholders across multiple domains (transportation, healthcare, Smart Grid, etc.). This standard provides a conceptual basis for the notion of things in the IoT and then elaborates the shared concerns as a collection of architecture viewpoints that form the body of the framework description.

1.2 Purpose

The IoT is predicted to become one of the most significant drivers of growth in many technology markets. The architectural framework defined in this standard will promote cross-domain interaction, aid system interoperability and functional compatibility, and further fuel the growth of the IoT market. The standard will address stakeholder concerns to help them build a connected world that can interoperate while meeting both the needs of enterprises and society for trustworthiness of IoT systems. The adoption of a unified approach to the development of IoT systems will reduce industry fragmentation and create a critical mass of multi-stakeholder activities around the world.

The motivation for the standard as informed by stakeholder concerns and desired outcome is to build stakeholder confidence through the following:

- a) Provide a framework for vendors to build conformant, interoperable, secure, IoT systems that can span multiple application domains.
- b) Provide a framework for buyers to make comparisons and assessments of such systems.
- c) Provide a framework for system designers to accelerate design, implementation, and deployment processes of such systems.

Business goals trigger and frame system concerns and thus the system architecture. In fact, the U.S. National Institute of Standards and Technology (NIST) CPS Public Working Group generated a list of concerns for cyber-physical systems (CPS) as listed in the Framework for Cyber-Physical Systems (NIST SP 1500-201 [B88]). The framework includes a business aspect that defines “concerns about enterprise, time to market, environment, regulation, cost, etc.” The concerns in the present document as derived from the NIST concerns incorporate business elements that acknowledge that systems need to be integrated into business processes to successfully meet the business goals. There is no common approach to addressing the business viewpoint and, therefore, this standard does not include a business architecture viewpoint. The relevance of the business goal of value creation and the desire for differentiable value propositions in the market are implied throughout the standard. Business goals are important for any viable system architecture.

This document provides both a normative part (Clause 6) with the architecture viewpoints intended to be the basis for describing the architecture for an IoT system, and an informative part (Clause 7) with examples of architecture descriptions associated with architecture views that conform to the architecture viewpoints.

1.3 Introduction to the Internet of Things (IoT)

Subclause 1.3 provides a high-level discourse of IoT systems. More information on the core concepts of IoT systems are provided in the conceptual viewpoint (see 6.6.2).

In the context of this standard, a *thing* is an IoT component or IoT system that has functions, properties, and ways of information exchange (see Figure 1). Furthermore, the information maintained within the thing, or when being exchanged, is appropriately secured. Note that the information exchange could be very limited and one way (e.g., bar code, visual recognition).

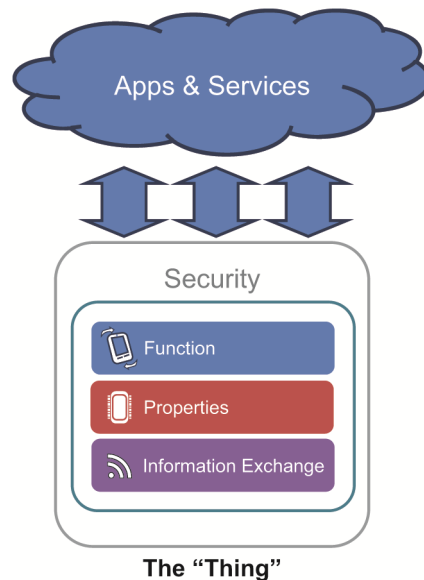


Figure 1—The meaning of *thing* in the context of this standard

It is important to understand what the IoT is and what the difference is between the IoT environment and an IoT system. A simple definition of an IoT system is “a system of entities (including cyber-physical devices, information resources, and people) that exchange information and interact with the physical world by sensing, processing information, and actuating.”

The set of IoT components available to be composed into IoT systems, the networks connecting the components, and any associated services that provide the mechanisms for discovery, composition, and orchestration can be called an *IoT environment*. Although an IoT environment contains the IoT components that may be used to create IoT systems, it does not necessarily contain any functioning IoT systems (if no IoT components have been instructed to interact as a system). On a similar note, an IoT environment may be used to create non-IoT systems (conventional IT systems) by excluding IoT components that have sensing or actuating capabilities. In its current state, the Internet may be considered an IoT environment.

At the most fundamental level, IoT systems address the interaction of computing resources with physical entities through sensors and actuators, while an IoT environment is an environment of connected components that can be combined to form IoT systems.

Core to the idea of IoT is this interaction with physical entities. An entity of interest is a physical entity that is of interest to a human or organization for the completion of a goal. A physical entity is a discrete, identifiable part of the physical environment. Physical entities can be any physical object: humans, animals, cars, store or logistics-chain items, mechanical devices, computing devices, etc. These entities range from solid items to bulk matter such as liquids or gases (e.g., air). The sensors and actuators required depend on the type of physical entity and the property of concern.

Interconnected and integrated IoT systems can provide new functionalities to improve the quality of life and to enable technological advances in areas such as personalized healthcare, emergency response, traffic-flow management, manufacturing, defense and homeland security, and energy supply and use. The impacts of IoT will be revolutionary and pervasive; this is already evident in emerging technologies such as autonomous vehicles, Smart Transportation, Smart Logistics, intelligent buildings, Smart Mining, Smart Energy Systems, Smart Manufacturing, multi-purpose robots, Smart Agriculture, Smart Forestry, and Smart Medical Devices.

An IoT system is composed of components that interact with each other to achieve a set of goals.² Typically, components are distributed. A component that is a technical artifact and that has an element of computation and interacts with the physical world through sensing and actuation of physical entities with a focus on the physical entity itself, is referred to as *cyber-physical device* (CPS Public Working Group [B20]). Actuation, sensing, and control (using sensing and actuation together) of entities of interest are the fundamental interaction patterns in IoT systems. Examples of other types of devices include dedicated storage devices and networking equipment such as routers, switches, and transceivers.

Cyber-physical devices can be understood as “information transducers,” in that they mediate the translation of physical properties into information by using a function, see function viewpoint in 6.6.7, and vice versa. These devices are part of a common trend toward the “dematerialization” of interactions. These information transducers include both sensors for observing the physical world and actuators for changing the physical world.

The sensing capability of a cyber-physical device captures specific physical states of an entity of interest and translates these states into an estimation of a property. Consider a cyber-physical device that senses light emissions—for example, a light sensor (such as a photodiode or photo resistor) with a bandpass filter. In the presence of an entity giving off light centered at a wavelength of 670 nm, the sensor translates this emission into the observation “*the color of the entity of interest is red.*” The properties of an entity can also be prescribed in a common data dictionary and be used by a normative name to describe aspects of an IoT system and its context, see IEC 61360 [B39].

Information in IoT systems is usually captured in digital form. While that information is necessary for an IoT system to fulfill its goal, it is not sufficient. What is needed is knowledge, i.e., information with context and significance. Definitions of data, information, and knowledge, and how the three relate to each other,

² A component may also be considered a system.

are provided in the information viewpoint (see 6.6.6) and the compatibility-level viewpoint (see 6.6.3) to help classify the kind of communication. Information exchange (see Figure 1) demands semantic information of the data on the transmitter and receiver side to interpret the data as information. Some network components, which have the function of forwarding information, do not need to interpret the data in a frame. They are interconnectable in the sense of no need to interpret the frame, but are also interworkable in the sense interpreting the header and tail around a data frame in a communication network.

It is important to understand that digital representations are representations of properties of the physical world, based on some simplification (model) of the world. As such, a digital representation is only an estimation of the property and has errors that may be expressed as an uncertainty (Taylor and Kuyatt [B136]). While in many cases the uncertainty of a given system is small enough that it can be ignored, information uncertainty should be evaluated and understood for every system due to the consequences of failure in an IoT system. This exercise feeds into ascertaining the significance of gathered information. The properties of a thing (see Figure 1) are part of the properties of the physical world.

Once a property has been observed using a sensor and converted into a digital representation, the data/information is processed to create useful knowledge. This is done by processors that combine the sensor data with data from other sensors and *a priori* knowledge stored in information archives or other sources. In the case of complex IoT systems, this is likely a combination of information from a variety of heterogeneous sources. To effectively combine this information, a thorough understanding of the information is required. This includes meta-information about the physical context (time, place, and property) and uncertainties related to the information.

This process of generating knowledge from data/information is complex, and in IoT this often falls under the category of Big Data and analytics. The processing may be done with one processor or may be distributed among many processors.

The action or *actuation* capability converts information into action on a physical entity in the physical world, changing the state of the physical entity. Actuation is the process of effecting change in the physical world. On the one hand, this could be interpreted as the end goal of all IoT observations and knowledge generation, and on the other hand it may be out of the scope of a given IoT system (some knowledge may be stored for later use). As with digital representations, there is a disconnection between the desired change and the actual change. This error shall be accounted for and is often referred to as *tolerance*. In many cases the error is well below a required threshold and can be considered insignificant, but it is important to verify this through measurement or calculation. The confidence about the IoT system's ability to consistently produce the same values and behaviors across different copies of the same system and time is assurance. Depending upon the impact of an IoT system not fulfilling the intended behavior, the justification needed to support that the claimed behavior can be achieved will vary.

For closed-loop control systems, the result of actuation can be sensed to create a feedback based on the error between the observed change and the desired change creating a negative feedback control loop.

The components in an IoT system are typically distributed and can interact by aid of communication networks. While IoT does not have an explicit set of communication protocols, IoT communication is usually characterized by packet-based, end-to-end connectivity that occurs, by default, over ad hoc paths through the network.

Humans (people) assume several roles in IoT systems. They may be developers/builders, defining the goals that an IoT system has to enable. They may be users, using the IoT system to accomplish those defined goals. In addition, they may participate as an element of the IoT system, interacting with other components of the system to achieve the defined goals. Finally, they can be entities of interest themselves.

The person as an element of an IoT system is particularly interesting. People have the ability to sense, act, process, store data, and communicate. In other words, people can be considered a biological part of IoT systems. While people can perform these functions, they do so in a manner significantly different from engineered electronics-based IoT systems. Not only do people sense, process, store data, and act differently

than computer-based IoT, they also exchange information in a different manner. An IoT system with people participating within the system needs to be able to convert machine-type information into a form people can process, and vice versa.

Automobile brakes can be used to illustrate how cyber-physical systems have evolved from traditional mechanical systems. Early automobile brakes used mechanical systems with Bowden cables or linkages between the brake pedal and the brake itself. In most contemporary systems, the mechanical system is replaced by a hydraulic system. However, cyber-physical solutions for braking are currently developed and also in use. In the cyber-physical solution, the engagement of the brake pedal is recorded by a sensor that converts the brake-pedal pressure into an electrical current or voltage. This current or voltage is then converted into digital data through some type of analog-to-digital converter. These data are translated into information, which is communicated to the electronic controller for the brake. The controller then converts the digital information into an analog signal through a digital-to-analog converter that actuates a servo causing the brake to engage. The communication can take place via dedicated communication links or via on-board communication networks. In the case of such an electronic brake system, two information transducers are used in order to achieve the same function as in a purely mechanical brake: the transducer at the pedal senses the engagement of the pedal and turns it into information, while the actuator at the brake turns the received information into action, i.e., the engagement of the brake. Sensing produces data that is translated into information while actuation in the controller is driven by data that is derived from information. This example is focused on an embedded approach, but the approach could as easily be distributed across a network.

Important characteristics of IoT systems include:

- Modularity/interoperability—each component can be connected to other components to form systems
- Agility/dynamic—a system can be quickly modified once it is built and components can be quickly added or removed
- Shared—components can be shared among systems
- Trustworthiness
- Resilience
- Assurance—inspiration of confidence in the performance of the system

These characteristics along with example application domains are addressed within the viewpoints provided in this document.

1.4 Architecture method

This standard adheres to the architecture ontology and methodology outlined in ISO/IEC/IEEE 42010:2011.

ISO/IEC/IEEE 42010:2011 architecture descriptions use viewpoints (framing a group of stakeholders concerns), which are addressed by architecture views. The views are work products that express the architecture of a system from the perspective of a viewpoint. Architecture viewpoints establish “conventions for the construction, interpretation and use of architecture views to frame specific system concerns” in ISO/IEC/IEEE 42010:2011. According to ISO/IEC/IEEE 42010:2011, an architecture framework, as provided in this document, is the collection of viewpoints that frame the concerns of an identified group of stakeholders (see Clause 4, Clause 5, and Clause 6). Architecture examples for a certain system within an application domain are described in Clause 7. Accordingly, the architecture examples in Clause 7 describe specific framed concerns and their stakeholders versus the generic viewpoints in Clause 6. Architecture views that provide specific implementation descriptions are provided in Clause 7.

Figure 2 illustrates the process how the present document was built.

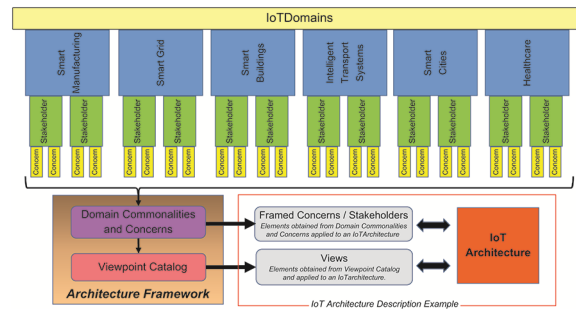


Figure 2—Architecture development process

2. Normative reference

The following referenced document is indispensable for the application of this document (i.e., it must be understood and used, so the referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ISO/IEC/IEEE 42010:2011, Systems and software engineering— Architecture description.^{3, 4}

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁵

Italicized terms are defined within 3.1.

adversary: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

NOTE—See CNSSI No.4009 [B17].⁶

application: Functional unit that is specific to the solution of a problem. Note that an application may be distributed among resources, and may communicate with other applications.

NOTE—See [B44] IEC 61804-2:2016.

³ The IEEE standards or products referred to in Clause 2 are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

⁴ IEEE publications are available from the Institute of Electrical and Electronics Engineers (<http://standards.ieee.org/>).

⁵ *IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>.

⁶ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

architectural framework: See *architecture framework*.

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.”

NOTE—See ISO/IEC/IEEE 42010:2011.

architecture description: Work product used to express an *architecture*.

NOTE—See 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.

NOTE—See ISO/IEC/IEEE 42010:2011.

architecture view: Work product expressing the architecture of a system from the perspective of specific system concerns.

NOTE—See 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.

NOTE—See ISO/IEC/IEEE 42010:2011.

assurance: Grounds for justified confidence that a claim has been or will be achieved.

NOTE—See ISO/IEC 15026 [B60].

Attack: An attempt to destroy, expose, alter, disable, steal, gain unauthorized access to, or make unauthorized use of, an asset.

NOTE—See ISO/IEC 27000:2016 [B64].

attribute: Property or characteristic of an entity.

NOTE—See IEC 61499-1:2012 [B41].

availability: Property of being accessible and usable upon demand by an authorized entity.

NOTE—See 2.9 of ISO/IEC 27000:2016 [B64].

coexistence: Ability of two or more devices to operate independently of one another in the same network respecting the common rules for sharing the same medium.

NOTE—See IEC 61804-2:2016 [B44].

concern: Interest in a system relevant to one or more of its *stakeholders*.

NOTE—See ISO/IEC/IEEE 42010:2011.

confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

NOTE—See ISO/IEC 27000:2016 [B64].

configuration (of a system or device): Selecting functional units, assigning their locations, and defining their interconnections.

NOTE—See IEC 61499-1:2012 [B41].

cyber-physical device: “A device that has an element of computation and interacts with the physical world through sensing and actuation.”

NOTE—See CPS Public Working Group [B136].

data: Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human beings or by automatic means.

NOTE—Based on IEC 61499-1:2012 [B41].

data type: A set of values together with a set of permitted operations.

NOTE— See IEC 61499-1:2012 [B41].

dependability: Ability to perform as, and when, required to meet specified communication and operational requirements.

NOTE—See IEC 61907 [B46].

device: Independent physical entity capable of performing one or more specified functions in a particular context and delimited by its interfaces.

NOTE—See IEC 61499-1:2012 [B41].

domain: A particular area of interest based on a one or more viewpoints. In the context of this document the following domains are considered:

- Application domains which define areas of related applications like Smart Grid, Smart Home, and Smart Manufacturing.
- Technology domains which define a specific technology area, such as IoT.

Domains of responsibility which cover areas that are under the responsibility of a specific actor/user such as an end customer, a distribution network operator, or a factory.

entity: A particular thing, such as a person, place, process, object, concept, association, or event.

NOTE—See IEC 61499-1:2012 [B41].

event: Instantaneous occurrence that is significant to scheduling the execution of an algorithm.

NOTE 1—See IEC 61499-1:2012 [B41].

NOTE 2—The execution of an algorithm may make use of variables associated with an event. Occurrence or change of a particular set of circumstances. (See ISO/IEC 27000:2016 [B64])

NOTE 3—An event can be one or more occurrences, and can have several causes.

NOTE 4—An event can consist of something not happening.

NOTE 5—An event can sometimes be referred to as an “incident” or “accident.”

exchangeability: Ability of one device to fulfill exactly the same role of another device in the physical process and distributed application as required by the process design

NOTE—See IEC 61804-2:2016 [B44].

function: Intended purpose of an entity or its characteristic action.

NOTE—Based on IEC 61499-1:2012 [B41].

hardware: Physical equipment, as opposed to programs, procedures, rules, and associated documentation.

NOTE—See IEC 61499-1:2012 [B41].

interconnectivity: Ability of two or more devices to operate with one another using the same communications protocols and communication interface.

NOTE—See IEC 61499-1:2012 [B41].

interface: Shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics as appropriate.

NOTE—See IEC 60050-351:2013 [B37].

Internet: The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

NOTE—See CNSSI No.4009 [B58].

Internet of Things (IoT): A system of entities (including cyber-physical devices, information resources, and people) that exchange information and interact with the physical world by sensing, processing information, and actuating.

NOTE—See 1.3.

interoperability: Ability of two or more devices to work together in one or more distributed applications with the shared knowledge of the data types and the semantics of the data transmitted.

NOTE—See IEC 61804-2:2016 [B44].

interworkability: Ability of two or more devices to support the transfer of data between devices with the shared knowledge of the data types of the data transmitted.

NOTE 1—The content of the data is unknown, e.g., a text string that can be displayed but not interpreted by the receiver device itself, or the content is a value but the unit is unknown.

NOTE 2—See IEC 61804-2:2016 [B44].

lifecycle (also: life cycle): Evolution of a system, product, service, project, or other human-made entity from conception through retirement.

NOTE—See ISO/IEC/IEEE 15288 [B66].

model: Representation of a real world process, device, or concept.

NOTE—Based on IEC 61499-1:2012 [B41].

performance: Quantitative or qualitative level of a property at any point in time considered.

NOTE—Based on ISO 15686-1:2011 [B58].

physical entity: “A physical entity is a discrete, identifiable part of the physical environment that is of interest to the user for the completion of her goal. Physical entities can be almost any physical object or environment; from humans or animals to cars; from store or logistics chain items to computers; from electronic appliances to closed or open environments.”

NOTE—See Carrez [B14].

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.

NOTE—See ISO TS 17574 [B67].

property: Characteristic common to all members of an object class.

NOTE—See ISO/IEC 11179-1 [B63].

Reference model: A “reference model is an abstract framework for understanding significant relationships among the entities of some environment. It enables the development of specific reference or concrete *architectures* using consistent standards or specifications supporting that environment. A reference model consists of a minimal set of unifying concepts, axioms and relationships within a particular problem domain, and is independent of specific standards, technologies, implementations, or other concrete details. A reference model may be used as a basis for education and explaining standards to non-specialists.”

NOTE—See OASIS [B91].

reliability: The ability of an item to perform a required function under given conditions for a given time interval.

NOTE—See IEC TR 62511 [B51].

resilience: Ability of a system or component to maintain an acceptable level of service in the face of disruption.

NOTE—See IIC Vocabulary 2.0 [B57].

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.

NOTE—See ISO Guide 51 [B65].

security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach.

NOTE—See CNSSI No.4009 [B17].

semantics: Relationships between the symbolic elements and their meanings, interpretation, and use.

NOTE—Based on [B38].

service: The means by which the needs of a consumer are brought together with the capabilities of a provider.

NOTE—See OASIS [B91].

stakeholder: “An individual, team, or organization (or classes thereof) with interests in, or concerns relative to, a system” (ISO/IEC/IEEE 42010:2011).

system: Set of interrelated elements considered in a defined context as a whole and separated from its environment.

NOTE 1—Such elements may be both material objects and concepts as well as the results thereof (e.g., forms of organization, mathematical methods, and programming languages).

NOTE 2—The system is considered to be separated from the environment and other external systems by an imaginary surface, which can cut the links between them and the considered system (based on [B37]).

technical artifact: “Entity that is designed by humans and that has a composition. The composition of the technical artifact enables functions that are accessible to humans and other technical artifacts.”

NOTE—See De Vries [B144].

Thing: Any *physical entity* in combination with its digital representation.

NOTE—See Carrez [B14].

threat: Threat is potential cause of an unwanted incident, which may result in harm to a system or organization.

NOTE—See ISO/IEC 27000:2016 [B64].

trustworthiness: Degree of confidence that the system performs as expected with characteristics including safety, security, reliability, and resilience.

NOTE—See IIC Vocabulary 2.0 [B57].

view: See *architecture view*.

viewpoint: See *architecture viewpoint*.

virtual entity: “Computational or data element representing a *physical entity*.”

NOTE—See Carrez [B14].

vulnerability: Weakness of an asset or control that can be exploited by one or more threats.

NOTE—See ISO/IEC 27000:2016 [B64].

3.2 Acronyms and abbreviations

ABAC	attribute-based access control
AC	access control

ACL	access control list
ADS	autonomous decentralized system
ADS-net	autonomous decentralized system-network
API	application programming interface
AS	authorization server
BPEL	Business Process Execution Language
BPMN	Business Process Model and Notation
CA	certifying authority
CNSSI	Committee on National Security Systems Instructions
CoAP	Constrained Application Protocol
CPS	cyber-physical system
CPU	central processing unit
CR	correspondence rule
CRC	cyclic redundancy check
DAC	discretionary access control
DIKW	data, information, knowledge, wisdom
DSCP	differentiated services codepoint
EMI	electromagnetic interference
ENISA	European Union Agency for Network and Information Security
EPC	event-driven process chain
EU	European Union
EV	electrical vehicle
EVWPT	electric vehicle wireless power transfer
FB	function block
FoF	factories of the future
GDPR	General Data Protection Regulation
GIS	geography information system
GPS	global positioning system
HMI	human-machine interface
HTTP	hypertext transfer protocol
H-ARC	hardening—adaptivity, responsiveness, cooperativity
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	information and communication technologies
IdP	identity provider
IDS	intrusion detection system
IEC	International Electrotechnical Commission

IIC	Industrial Internet Consortium
IOC	Intelligent Operation Center
IOI	item of interest
IoT	Internet of Things
IP	Internet Protocol
IPS	intrusion prevention system
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	information technology
ITS	Intelligent Transportation Systems
ITU	International Telecommunication Union
MAC	media access control
MIT	Massachusetts Institute of Technology
MQTT	message queue telemetry transport
MTTR	mean time to repair
NIST	National Institute of Standards and Technology
NPE	non-person entity
OASIS	Organization for the Advancement of Structured Information
OCL	Object Constraint Language
OIX	Open Identity Exchange
OODA	observe, orient, decide, act
OPC	Open Platform Communications
OPC UA	OPC Unified Architecture
OSI	open systems interconnection
OT	operational technology
OWASP	Open Web Application Security Project
OWL	Web Ontology Language
PAP	policy administration point
PCN	Process Control Network
PDCA	plan, do, check, act
PDP	policy decision point
PEP	policy enforcement point
PIN	personal identification number
PIP	policy information point
PKI	public key infrastructure
QoS	quality of service
RADIUS	remote authentication dial-in user service

RBAC	role-based access control
REST	representational state transfer
RFC	Request for Comments
RFID	radio frequency identification
R&D	research and development
SAL	security assurance level
SCADA	supervisory control and data acquisition
SELinux	Security Enhanced Red Hat Linux
SI	International System of Units
SMS	short message service
SNMP	simple network management protocol
SoS	system of systems
SSL	secure sockets layer
ST	structured text
SysML	System Modeling Language
S-ADS	symbiotic-autonomous decentralized system
TACACS	terminal access controller access control system
TCP	transmission control protocol
TOGAF	The Open Group Architecture Framework
TR	technical report
TS	technical specification
TSN	time-sensitive networking
UDP	user datagram protocol
UMA	user-managed access
UML	Unified Modeling Language
UNESCO	United Nations Educational, Scientific and Cultural Organization
UUID	universally unique identifier
WWW	World Wide Web
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

4. IoT domains

4.1 Abstract IoT Domain

The Abstract IoT Domain captures the common characteristics and behaviors across IoT systems.

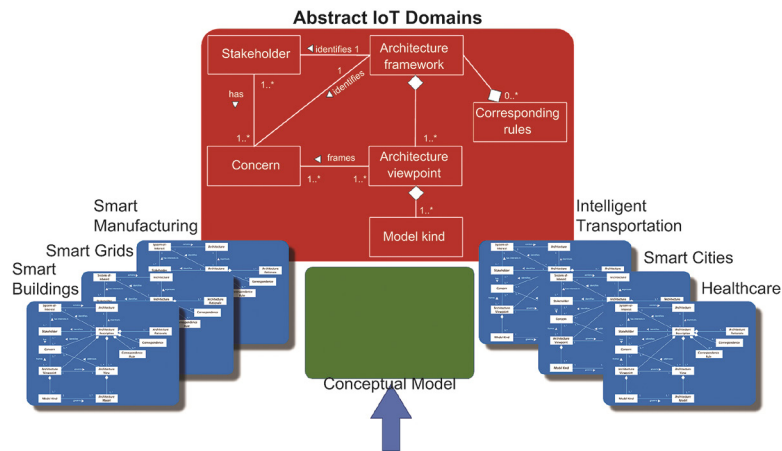


Figure 3—Example of IoT domains

As shown in Figure 3, the Abstract IoT Domain is based on the conceptual model which is the foundation of this architecture framework. The conceptual model informs a key architecture viewpoint, the conceptual viewpoint (see 6.6.2), which clarifies how the IoT is to be understood in the context of the present document.

In the present document, architecture viewpoints are elaborated based on commonalities identified across concrete IoT domains.

As shown in Figure 2, six representative domains are considered: *Smart Manufacturing*, *Smart Grid*, *Smart Buildings*, *Intelligent Transport*, *Smart Cities*, and *Healthcare*.

The six domains were informally examined with reference to the aspects and concerns of cyber-physical systems identified in NIST SP 1500-201 [B88]⁷ and the outcomes of that process were used to motivate the architecture viewpoints described in Clause 6.

4.2 Smart Manufacturing

There are several terms commonly used in this area which overlap in scope: Smart Automation, Smart Factory, Intelligent Factory, Smart Manufacturing, and Industry 4.0. Here, the term *Smart Manufacturing* refers to the shared vision of enhanced intelligence, flexibility, and dynamics over entire manufacturing processes and production chains.

According to Bulik [B11]:

The Smart, and mostly digital, factory concept focuses on an integrated planning and monitoring process that includes product design, process planning, and overall integration and implementation of the manufacturing operation, making the manufacturing process more efficient and responsive to change.

All aspects of production from suppliers, logistics, through to the lifecycle management of products are impacted: factory design, production planning, logistics, enterprise resource planning, manufacturing machinery and systems, control technologies, and devices in the field.

⁷ The numbers in brackets correspond to those of the bibliography in Annex E.

Further, the devices and computing elements distributed throughout the process chains and production lines have degrees of intelligence and autonomy, are capable of analytics and decision making, and can dynamically modify, guide, and optimize operations in flight.

As with other domains, stakeholders in Smart Manufacturing are a broad and diverse group, including: shareholders, board members, executives, production teams, customers, suppliers, and industry regulators.

Equally broad is the range of benefits that are derived from the approach, including: process optimizations, production optimizations, reduced downtime, reduced material waste, leaner operations, shorter cycle times, reduced energy consumption, reduced greenhouse emissions, and increased worker safety.

Among the key drivers of Smart Manufacturing (and all overlapping terms and initiatives) are energy and resource optimization. Consequently, there are broad sustainability implications which also bring the environment and society in general into the stakeholder group.

Smart Manufacturing and Factories of the Future are components of the European Commission's digital single market strategy (European Commission [B25]):

The European strategy on smart specialization aims to strengthen the competitive advantages of EU regions in terms of ICT skills, R&D capability, industrial output and infrastructures while linking up similar strategies at regional & national levels, and offering incentives for growth and differentiation.

Similar policies are emerging in developed economies globally.

4.3 Smart Grid

The term *Smart Grid* refers to an electricity power infrastructure in which digital computing and communications technologies are deployed to enhance the ability of stakeholders to better understand and control the energy being pushed into the grid, the energy being drawn from the grid, and the state of the grid itself.

The smartness enhances insight into both the grid as a power network and the grid as a system of systems. Enhanced insight improves controllability and predictability, both of which drive improved operation and economic performance and both of which are prerequisites for the sustainable and scalable integration of renewables into the grid and the potential transition to new grid architectures.

The U.S. Department of Energy provides the following definition [B140]:

An automated, widely distributed energy delivery network, the Smart Grid will be characterized by a two-way flow of electricity and information and will be capable of monitoring everything from power plants to customer preferences to individual appliances. It incorporates into the grid the benefits of distributed computing and communications to deliver real-time information and enable the near-instantaneous balance of supply and demand at the device level.

The fundamental intersection of the Smart Grid and IoT is derived from a view of the domain as a collection of interconnected networks of independently addressable objects capable, to varying degrees, of processing, sensing, actuating, and communicating.

Overviews of Smart Grid networks can be found in Garner [B28] and Al-Omar, Al-Ali, Ahmed, and Landolsi [B95]. Smart Grid networks operate over a wide range of technologies and protocols (Al-Ali and Aburukba [B2]) and typically span: home area networks, neighborhood area networks, access networks, backhaul networks, and core and external networks.

In developed economies, the Smart Grid is a ubiquitous infrastructure and most households, commercial concerns, governmental, regulatory, and societal organizations will be stakeholders with dependencies on the grid. Stakeholders vary over regions and between countries depending on the form of regulation, the market, and the level of development of the local physical infrastructure.

Emerging economies share the global drivers of a Smart Grid rollout. More specifically, a Smart Grid helps enable access to electricity for all, reduces transmission and distribution losses, improves quality of power supply, helps peak load management, promotes prosumer concepts, and integrates renewable energy.

Smart Grid benefits spread across a broad spectrum, but generally include improvements in: power reliability and quality, grid resiliency, power usage optimization, operational insights, renewable integration, insight into energy usage, safety, and security.

4.4 Smart buildings

According to RCR Wireless News [B121]:

A smart building is any structure that uses automated processes to automatically control the building's operations including heating, ventilation, air conditioning, lighting, security and other systems. A smart building uses sensors, actuators and microchips, in order to collect data and manage it according to a business' functions and services.

Smart buildings drive benefits for a range of stakeholders including owners, tenants, visitors, caretakers, and the environment. Multiple aspects of such buildings (lighting, heating, air conditioning, safety, security, access, systems, etc.) are managed by autonomous agents (from simple sensors and actuator to sophisticated subsystems) monitoring, analyzing, collaborating, coordinating, and ultimately acting to deliver stakeholder benefits.

As described in Building Efficiency Initiative [B10]:

Smart buildings use information technology during operation to connect a variety of subsystems, which typically operate independently, so that these systems can share information to optimize total building performance. Smart buildings look beyond the building equipment within their four walls. They are connected and responsive to the smart grid, and they interact with building operators and occupants to empower them with new levels of visibility and actionable information.

4.5 Intelligent Transport Systems

4.5.1 General

Intelligent Transport, Smart Transport, and Smart City Transport are overlapping terms which refer to the intelligent coordination of assets and information within transport networks. This includes networks and assets which are in public, private, and commercial ownership. This domain also provides an example of the cross-domain nature of IoT as it includes elements of other domains.

Embedding and connecting intelligence across transport systems (both within the environment and within vehicles) will open up possibilities for significant benefits:

- Greater insight for citizens and authorities into the state of traffic and transport within a locality

- Enhanced ability for the transport system to self-heal in response to scheduled and unscheduled events
- More effective exploitation and usage of supporting infrastructure (parking, park-and-ride systems)

Greater transparency on the mobility of citizens and their usage of transport asset drives serious concerns over data confidentiality, data usage, anonymization, and long-term persistency of data. Conversely, it also raises concerns over the ability of such intelligent ecosystems to be subverted by injection of false information and the derivation of misleading analytics.

Intelligent transport is about the networking of assets which are capable of sensing, rationalizing, communicating, and acting on acquired and derived information to provide improved levels of efficiency which deliver, economic, and environmental benefits across society (United Nations Economic Commission for Europe [B139]).

In Intelligent Transportation Systems (ITS), IoT plays a central role in providing passive safety and traceability services for vehicles, bicycles, and pedestrians. The ultimate objective of ITS is to attain sustainable mobility. The system was originally a combination of vehicle navigation systems, electric road pricing, systems for supporting safe driving, traffic management, roadway management, and effective operation of public transportation, emergency vehicles, and pedestrians. In order to achieve these systems and services, a holistic system that integrates environmental and positioning sensors, wireless communication devices, and low-power computational nodes shall be connected to the Internet. In other words, the integration of IoT devices is indispensable. In fact, some such integration has already been established, affecting our daily lives. However, there are still many elements for discussion in the IoT domain of ITS, especially from the viewpoint of introducing electric vehicles (EVs).

4.5.2 EVs as an element of the ITS domain

EVs are more than just a simple transportation means. They are strongly expected to help build strong linkages with roads, grids, and communication systems as illustrated in Figure 4.



Figure 4—Intelligent Transport Systems overview

First, linkages with roads can support electrical vehicles (EVs) from several different perspectives. Electric vehicle wireless power transfer (EVWPT) is a cutting-edge technology for charging and, in some cases, discharging EV batteries even when traveling along a road, especially in an EV lane. Unfortunately, alignment errors might occur, degrading the efficiency of power transmission and leading to inefficient EV charging and discharging. In these situations, communication and sensing using the IoT can offer one solution for making EV charging and discharging more efficient.

As for the installation cost of EVWPT, battery replacement is considered to be one method of reducing cost because a replaceable battery can leverage IoT sensors for managing battery charging and lifecycle control.

The connection between EVs and roads in ITS can be applied to automatic fare rate management of EV lanes, as this comes with an Internet environment and cloud services. If a floating exchange rate system is applied to electricity prices for EVs, the changing rate would control the timing of EV charging, giving rise to new services.

This linkage also provides various information-based services. Generally, emergency vehicles should be prioritized over others in traffic, while, in general, effective navigation considering driver comfort, energy efficiency, and traffic control is crucial for sustainable mobility in transportation. In meeting these requirements, ITS can control traffic signals as well as navigation systems aboard EVs based on the information obtained by IoT devices. In that sense, IoT devices will certainly play a pivotal role in system control and optimization.

In cases of disasters, EVs with IoT features are of great importance. For example, the remaining battery power of EVs can be used for communication systems, such as smartphones. This can also be an energy resource for any other electrical devices. In evacuation centers, the management of EV discharging can be conducted using IOT devices aboard EVs.

Secondly, linkage with the power grid and micro-grids engenders peak shifting of electricity usage, spinning reserve for quick power recovery from grid failures, and voltage and frequency control for grid stabilization. Additionally, linkage with buildings leads to peak shifting and spinning reserve. The above applications call for automated measurement of electricity usage and device control, which are effectively performed by IoT technologies.

Finally, regarding linkage with communication systems, ITS can be an integral part of the overall system. Cars were once just a means of transportation; however, they are gaining considerable attention currently as communication devices. Communication for cars begins with ITS, as seen in traffic control, in an attempt to reduce congestion, accidents, road closures, and travel time. Furthermore, ITS shall provide other services, such as congestion information on parking lots and rest areas, or tourism information, such as sightseeing and events of interest to tourists. Vehicle-to-vehicle (V2V) and vehicle-to-road (V2R) communication, both of which are based directly on communication with EVs, have recently emerged. Both V2V and V2R enable traffic accident prevention, especially near intersections where pedestrians and bicycles may be involved. These communication forms can also lend themselves to sending control signals to EVs in order to give priority to emergency vehicles. Another form of communication, vehicle-to-home (V2H) and vehicle-to-building (V2B) communication are very promising. Although EV battery deterioration and initial cost should be taken into account, EV batteries can be used for “buying low and selling high” when EVs are connected to a home or building’s energy management system. Another type of application could be a car-sharing service that shares cars for users. IoT technologies can inform users of locations and wait times for each car in a car park. All of these linkages and services with communication systems are supported by IoT itself.

4.6 Smart Cities

4.6.1 General

According to Zanella et al. [B147], Smart Cities are about making better use of the public resources, increasing the quality of the services offered to the citizens, and reducing the operational costs of the public administrations. This domain also provides an example of the cross-domain nature of IoT as it includes elements of other domains.

In typical urban environments, such resources and services include transport, parking, lighting, security and surveillance, air quality, maintenance of public areas, preservation of cultural heritage, garbage collection, and many more. Smart Cities therefore have strong synergies and dependencies on other “smart” verticals, such as Intelligent Transport Systems, Smart Buildings, Smart Grid, etc.

There is an expectation that Smart City concepts will alleviate pressures on administrative and operational resources by simplifying access to services, increasing transparency, and enabling efficiencies. Further, there is significant potential for new value to emerge as social networks and city services blend and cross-pollinate to build new digital communities, for example, for education, self-help, and entertainment, to enhance the quality of urban life.

Over the last couple of decades, there has been a trend of strong growth in information, communication, and computation technologies. Modern high-performance computing systems date back to the mid-1990s with cluster computing, the structure of which was one of the main topics of discussion. As its successor, grid computing, has been devised in an attempt to extend its usability. Recent years have seen the development of cloud computing, which has been discussed from the perspective of service provision. On the other hand, the electric power grid, as a typical example of all infrastructure, stems from bulk generation. The micro-grid as a distributed grid added to the debate over grid structure in the early 2000s. The Smart Grid, developed in the 2010s, extends its application range to services for both generators and consumers. Along with the advent of service-aware cloud computing and Smart Grids, the field of communication technology has also advanced without exceptions. Sensor networks were independently constructed in the 1990s for collecting sensing data and issuing commands for device manipulation. They technically form the foundation of IoT, which itself includes the idea of providing services. By means of IoT, the infrastructure in medical services, transportation, agriculture, water and sewerage, and other industries are now transforming into Smart Infrastructure, including Smart Medical Services, Smart Transportation, Smart Agriculture, and Smart Water Infrastructure. Therefore, discussion on IoT could be divided into industrial domains from the service perspective.

The Smart City is one of the IoT domains, and concurrently, it is the integration of Smart Infrastructures in and of itself. The IoT in a Smart City is one of the most important issues of discussion. Currently, a large volume of data is collected and used for services in Smart Infrastructure; however, these data and services are confined within their target Smart Infrastructure. For instance, the data of an electric power grid will not be used in medical infrastructure. The quintessence of a Smart City is the interaction among different types of Smart Infrastructure. Figure 5 typically describes the situation. The integration of Smart Infrastructure creates new services, such as data brokerage, data mining, and recommendation. The IoT in each type of Smart Infrastructure has to work in conjunction with each other when applied to Smart City services, which requires both unified naming and identification method.

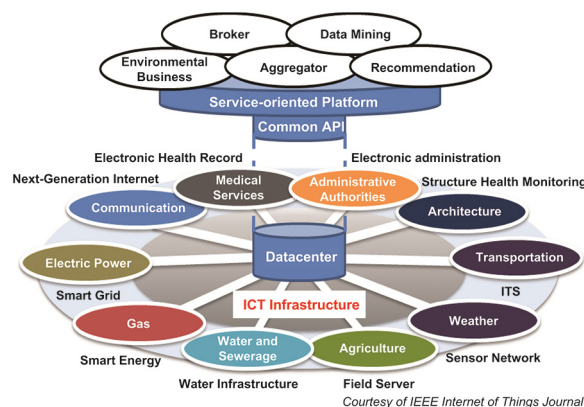
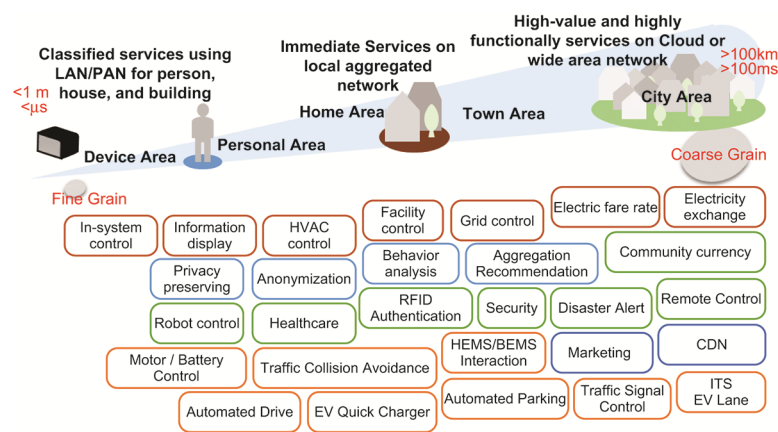


Figure 5—Smart City Subdomains

The Smart City is a sustainable living entity whose brain, nervous system, and organs collaborate with each other to sense and improve the physical world. New information and communication technology (ICT)—such as cloud computing, IoT, Big Data, and mobility—will make all things sensible, connected, and intelligent. The technologies aggregate, share, and converge city-wide resources to provide real-time, efficient, and intelligent information services.

To deliver these Smart City services, the IoT system should be integrated into the existing network and computing systems. Figure 6 illustrates the relationship between the typical examples of Smart City services and service providing positions. As shown in Figure 6, each service should be executed in the correct location. In other words, the most suitable processing device should be chosen to execute application software intended for the service. A simple idea is to execute the software in the cloud, but the figure is contrary to this idea and indicates the necessity of rebuilding the network architecture for the IoT era. Figure 7 depicts the relationship between network locations and attributes of service applications. Every service has its optimal execution platform in terms of data size, privacy control, latency, and other attributes defined by network locations. Motor or battery control should be achieved in a dedicated device or machine. Heating, ventilation, and air conditioning (HVAC) control should be executed in each household. If HVAC control is offered as a cloud service, a nonintrusive load-monitoring problem has to be solved, which implies that all the households should be warned of the risks of using cloud services. Electricity exchange service is a kind of aggregation service in which data integration is indispensable. Therefore, it should be offered as a cloud service. All the above things considered, the IoT system needs sharing for its effective use in the coming years. It should also be noted that an IoT system shall be independently shared in order to execute each service separately at its optimized location.



Courtesy of IEEE Internet of Things Journal

Figure 6—Smart City services and data sources

	Sensor Network	Access Network	Router	Cloud	
Target Area	Narrow Building <100m	Town <10km	City <100km	Worldwide	Wide
Allowable Processing Delay	Short	Power System Stabilization Auto drive Collision Avoidance <10ms	Facility Control <1s	Dynamic Pricing <30min	Long
Calculation Cost Computing Platform	Small	Embedded Microcontroller	Server	Cluster Datacenter	Big
Anonymity	Weak	Plain	Weak Anonymization	Strong Anonymization	Strong
Amount of Data	Small	<KB	<MB	>GB	Big

Fine-grain data

Coarse-grain data

Courtesy of IEEE Internet of Things Journal

Figure 7—Network locations and attributes of service applications

Enabled by the Smart Government, residents can submit service requests through government self-service terminals, service halls, websites, and mobile apps. The Intelligent Operation Center (IOC) can aggregate a wide range of data to visualize the city running status, enable efficient emergency collaboration across agencies, and facilitate decision-making based on Big Data.

Smart Cities need viable platforms to constantly grow and evolve. Ultra-wideband networks, cloud computing, Big Data, and IoT technologies can be used to build open platform for Smart City construction. Building a better Smart City is a common aspiration of governments, telecom operators, telecom equipment suppliers, independent software vendors (ISVs), and residents.

Normally the Smart City ICT infrastructure has the following networks, cloud centers, and platforms as shown in Figure 8.

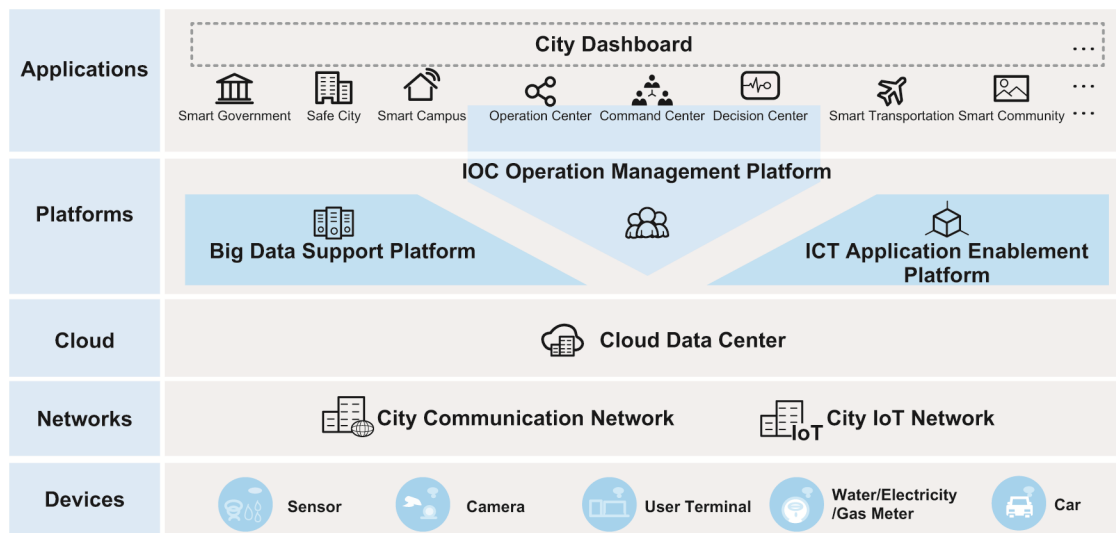


Figure 8—Smart Cities ICT infrastructure

Two networks: The urban communications network and the urban IoT. It combines wired and wireless broadband networks to enable ubiquitous broadband access in a city. In the IoT field, a diversity of access gateways and wireless access technologies are used, adapting to complex access environments, including high-density, large-volume, ground and underground scenarios.

One cloud center: The cloud data center which includes a rich portfolio of cloud products and service solutions, such as cloud computing and cloud storage.

- Three platforms: The Big Data Support Platform, ICT Application Enablement Platform, and Intelligent Operation Center (IOC)
- Big Data Support Platform: Enables data sharing and exchange, and provides data support for intelligent applications
- ICT Application Enablement Platform: Allows partners to develop intelligent applications
- IOC: Aggregates a wide range of data to visualize the city running status, enable efficient emergency collaboration across agencies, and facilitate decision-making based on Big Data.

The IOC will be described in detail in 4.6.2.

4.6.2 Intelligent Operation Center as an element of a Smart Cities domain

With the increase of urban population and the limitation of resources, cities around the world are facing more and more problems about the day-to-day city operation. In order to help ensure public safety and to provide water, electricity, transport, and other services more efficiently, the city government needs to collect and analyze more and more information by real-time communication and collaboration among different industries and departments.

For most cities, routine information and critical information are often distributed in different systems of functional departments. It is difficult for the city governments to make the correct and on-time decisions since they cannot have a clear view of the whole situation. An Intelligent Operation Center (IOC) is needed to make the cities operation and public service more efficient.

The Intelligent Operation Center acts like a brain and central nervous system for Smart Cities, integrating and interconnecting information and processes. And it also provides a platform for technology, operation, and management:

- Monitors city operations so professional staff can stay informed of conditions
- Accelerates emergency response with cross-agency collaboration
- Simulates city operations and facilitates intelligent decision-making with unified city development planning and data mining and analytics
- An open source data system offers personalized, smart data services for citizens

Figure 9 illustrates the IOC-based IoT, and Figure 10 illustrates the Intelligent Operation Center architecture.

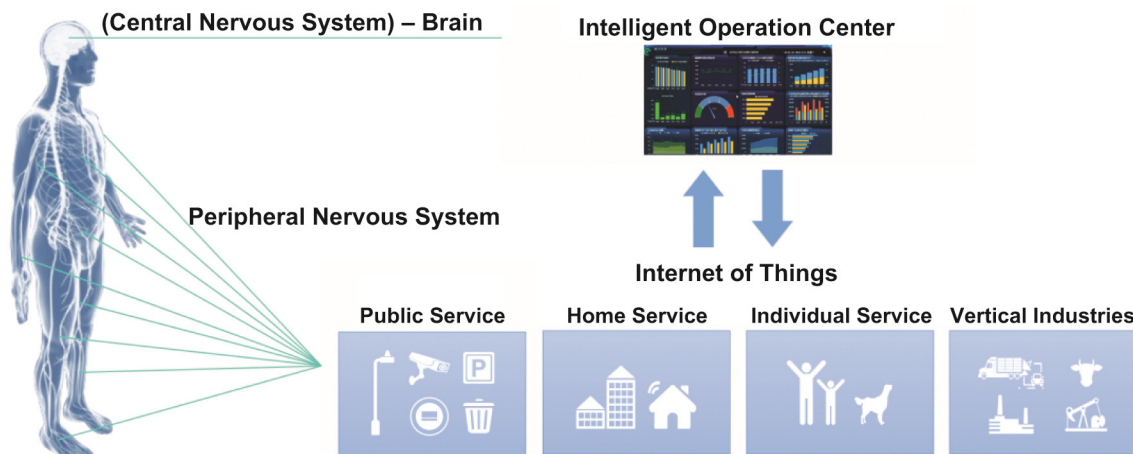


Figure 9—IOC Based on IoT

The Intelligent Operation Center is normally based on the cloud-based information and communication technology (ICT) infrastructure. What's more, an Intelligent Operation Center normally has comprehensive features such as city management databases, data support and resource services, and cross-agency applications. The Intelligent Operation Center may include:

- ICT infrastructure: A Cloud Platform centrally allocates and manages IT infrastructure and data resources such as computing, storage, and network resources.
- City management databases: Population, housing, macro economy, and geographic information support flexible data sharing and decision-making.

- Data support and resource services: Exploit the full benefits of Big Data by converging data across geographically-dispersed industries.
- Cross-agency service applications: City operations status displays for monitoring and alerts, collaborative handling and command of emergencies, simulation and unified planning, open city data and information services, and cyber security management.
- City operation center: Large-screen display, digital conferencing, sound reinforcement, video and audio switching, central control systems, and other facilities.

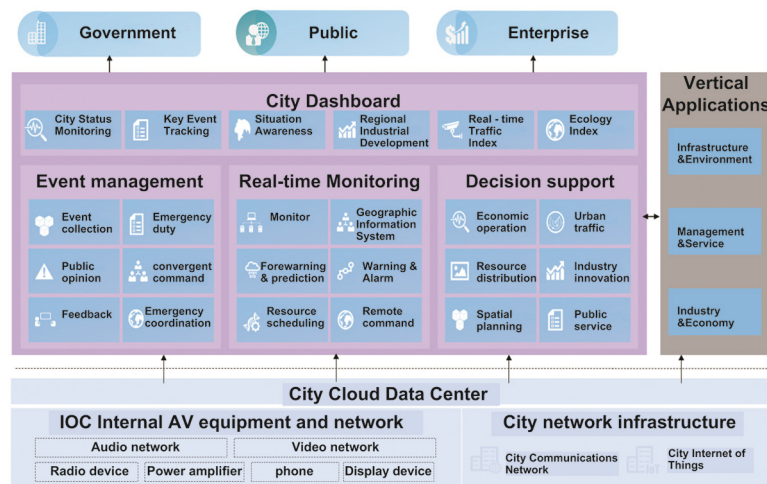


Figure 10—Intelligent Operation Center architecture

The benefits of deployment of Intelligent Operation Center include:

- Comprehensive monitoring
- Collaborative emergency handling and command
- Unified planning
- Data openness for open-source cities and personalized, Smart Citizen Services

4.7 Healthcare

Healthcare has a history of maintaining pace with technology. Patient records have been tracked electronically for many years, mobile solutions are commonly used to capture, monitor, and report patient data and to provide access to healthcare providers. As more affordable, intelligent connected devices become available, the healthcare sector is taking advantage of them.

Healthcare is evolving from an e-health perspective, in which technology was used to provide a level of automation, to a Smart Health perspective, in which healthcare systems exploit the advantages that supporting networks of context aware, autonomous intelligent agents can offer (Russo [B128]).

Connected devices which embed context aware, autonomous intelligent agents have the potential to provide significant support to patients—for example, for those patients self-managing chronic conditions. They can also support performance and lifestyle improvements (note the success of personal activity trackers worn as wrist-bands) and potentially help address behavior modification (such as reducing alcohol intake and stopping smoking).

Given the sensitivities around health data and the potential repercussions that the leaking of such data could have, confidentiality of data is a key concern.

Somewhat in contrast to that, there is potential value in enabling cross-pollination with social networks and Smart City services to build digital communities for patients, community care-givers, and health professionals.

5. Domain commonalities and common concerns

5.1 Stakeholders

Architecture descriptions are framed around the concerns of stakeholders in a system-of-interest (ISO/IEC/IEEE 42010:2011). Here, the system-of-interest is a framework which captures the commonalities across IoT domains and the initial stakeholders are a set of generalized roles shown in Table 1.

Table 1—IoT common stakeholders

Stakeholder	Role
Acquirers	Oversee the procurement of the IoT system or product
Assessors	Oversee the IoT system's conformance to standards and legal regulation
Builders	Construct and deploy the IoT system from specifications (or lead the teams that do this)
Communicators	Explain the IoT system to other stakeholders via its documentation and training materials
Developers	Construct and deploy the IoT system from specifications (or lead the teams that do this)
Maintainers	Manage the evolution of the IoT system once it is operational
Operators	Run the IoT system once it has been deployed
Owners	Derive the benefits of the IoT system when in use
Production engineers	Design, deploy, and manage the hardware and software environments in which the IoT system will be built, tested, and run
Regulators	Define the legal, regulatory, and domain-specific norms of practice/rules that the IoT system shall fulfill with regards to safety, reliability, security, privacy, and resilience
Suppliers	Build and/or supply the hardware, software, or infrastructure on which the IoT system will run
Support staff	Provide support to users for the IoT product or system when it is running
System administrators	Run the IoT system once it has been deployed
Testers	Test the IoT system to help ensure that it is suitable for use
Users	Define the IoT system's functionality and ultimately make use of it

Each viewpoint may provide unique stakeholder names that interpret and can be cross-referenced to the stakeholders in Table 1. The cross-reference is provided within each viewpoint description and in Annex B.

5.2 Common concerns

In the context of this standard, common concerns represent stakeholder concerns which have been:

- Identified in multiple IoT domains or
- Identified in a single IoT domain, but are considered to have broader applicability

A list of common concerns was derived from consideration of stakeholder concerns across the representative domains presented in 3.2. This list was then compared to those compiled by the NIST CPS Public Working Group in the Framework for Cyber-Physical Systems (NIST SP 1500-201 [B88]). An IoT system can be considered a type of cyber-physical system as it has one or more sensors and/or actuators. The resultant list of common IoT domain concerns is shown in Table 2 (without prioritization or weighting).

Table 2—IoT concerns

Concern	Description	Source ^a
Actuation	Concerns related to the ability of the cyber-physical system (CPS) to effect change in the physical world.	NIST SP 1500-201 [B88]
Adaptability	Concerns related to the ability of the CPS to achieve an intended purpose in the face of changing external conditions such as the need to upgrade or otherwise reconfigure a CPS to meet new conditions, needs, or objectives.	NIST SP 1500-201 [B88]
Assurance	The level of confidence that a CPS is free from vulnerabilities, either intentionally designed into it or accidentally inserted during its lifecycle, and that the CPS functions in the intended manner.	NIST SP 1500-201 [B88]
Autonomy	Concerns related to optimal functionality under independent operating conditions in a changing environment.	IEC White Paper 2015 [B52], Nonaka et al. [B89]
Behavioral	Concerns related to interdependence among behavioral domains. Concerns related to the ability to successfully operate a CPS in multiple application areas.	NIST SP 1500-201 [B88]
Collaboration	Concerns related to formation of two or more systems that form an ecosystem that guarantees value delivery.	IEC White Paper 2015 [B52], Nonaka et al. [B89]
Communication	Concerns related to the exchange of information internal to the CPS and between the CPS and other entities.	NIST SP 1500-201 [B88]
Complexity	Concerns related to our understanding of the behavior of CPS due to the richness and heterogeneity of interactions among its components, such as existence of legacy components and the variety of interfaces.	NIST SP 1500-201 [B88]
Conceptual	Concerns related to requirements engineering and concept engineering (including architecture development).	The present document
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes	ISO/IEC 270000:2016 [B64]
Constructivity	Concerns related to the ability to combine CPS modular components (hardware, software, and data) to satisfy user requirements.	NIST SP 1500-201 [B88]
Controllability	Ability of a CPS to control a property of a physical thing. There are many challenges to implementing control systems with CPS including the non-determinism of cyber systems, the uncertainty of location, time, and observations or actions, their reliability and security, and complexity. Concerns related to the ability to modify a CPS or its function, if necessary.	NIST SP 1500-201 [B88]
Cost	Concerns related to the direct and indirect investment or monetary flow or other resources required by the CPS throughout its lifecycle.	NIST SP 1500-201 [B88]
Data semantics	Concerns related to the agreed and shared meaning(s) of data held within, generated by, and transiting a system.	NIST SP 1500-201 [B88]
Data velocity	Concerns related to the speed with which data operations are executed.	NIST SP 1500-201 [B88]
Data volume	Concerns related to the volume or quantity associated with a CPS's operation.	NIST SP 1500-201 [B88]
Deployability	Concerns related to the ease and reliability with which a CPS can be brought into productive use.	NIST SP 1500-201 [B88]
Discoverability	Concerns related to the ease and reliability with which a CPS component can be observed and understood (for purposes of leveraging the component's functionality) by an entity (human, machines). Concerns related to the ease and reliability with which a CPS component's functions can be ascertained (for purposes of leveraging that functionality) by an entity (human, machines).	NIST SP 1500-201 [B88]
Disposability	Concerns related to the impacts that may occur when the CPS is taken physically out of service.	NIST SP 1500-201 [B88]
Engineerability	Concerns related to the ease and reliability with which a CPS design concept can successfully be realized via a structured engineering process.	NIST SP 1500-201 [B88]
Enterprise	Concerns related to the economic aspects of CPS throughout their lifecycle.	NIST SP 1500-201 [B88]

Concern	Description	Source ^a
Environment	Concerns related to the impacts of the engineering and operation of a CPS on the physical world.	NIST SP 1500-201 [B88]
Evolvability	Concerns related to the system's ability to evolve and to be functional with newer technology (backward compatibility).	IEC White Paper 2015 [B52]
Functionality	Concerns related to the function that a CPS provides.	NIST SP 1500-201 [B88]
Human factors	Concern about the characteristics of CPS with respect to how they are used by humans.	NIST SP 1500-201 [B88]
Identity	Concerns related to the ability to accurately recognize entities (people, machines, and data) when interacting with or being leveraged by a CPS.	NIST SP 1500-201 [B88]
Integrity	Property of accuracy and completeness.	ISO/IEC 270000:2016 [B64]
Logical time	Concerns related to the order in which things happen (causal order relation) or event driven.	NIST SP 1500-201 [B88]
Maintainability	Concerns related to the ease and reliability with which the CPS can be kept in working order.	NIST SP 1500-201 [B88]
Manageability	Concerns related to the management of CPS function. For example, managing timing in a complex CPS or SoS is a new issue with CPS that did not exist before.	NIST SP 1500-201 [B88]
Measurability	Concerns related to the ability to measure the characteristics of the CPS.	NIST SP 1500-201 [B88]
Monitorability	Concerns related to the ease and reliability with which authorized entities can gain and maintain awareness of the state of a CPS and its operations. Includes logging and audit functionality.	NIST SP 1500-201 [B88]
Networkability	Concerns related to the ease and reliability with which a CPS can be incorporated within a (new or existing) network of other systems.	NIST SP 1500-201 [B88]
Operability	Concerns related to the operation of the CPS when deployed.	NIST SP 1500-201 [B88]
Operations on data	Concerns related to the ability to create/read/update/delete system data and how the integrity of CPS data and behaviors may be affected.	NIST SP 1500-201 [B88]
Optimization	Concerns related to the ability of systems or resources to perform optimally.	IEC White Paper 2015 [B52], Nonaka et al. [B89]
Performance	Concerns related to the ability of a CPS to meet required operational targets.	NIST SP 1500-201 [B88]
Physical	Concerns about purely physical properties of CPS including seals, locks, safety, and EMI.	NIST SP 1500-201 [B88]
Physical context	Concerns relating to the need to understand a specific observation or a desired action relative to its physical position (and uncertainty). While this information is often implied and not explicit in traditional physical systems, the distributed, mobile nature of CPS makes this a critical concern.	NIST SP 1500-201 [B88]
Policy	Concerns related to the impacts of treaties, statutes, and doctrines on a CPS throughout its lifecycle.	NIST SP 1500-201 [B88]
Privacy	Concerns related to the ability of the CPS to prevent entities (people, machines) from gaining access to data stored in, created by, or transiting a CPS or its components such that individuals or groups cannot seclude themselves or information about themselves from others. Privacy is a condition that results from the establishment and maintenance of a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within or among systems or through the manipulation of physical environments.	NIST SP 1500-201 [B88]
Procureability	Concerns related to the ease and reliability with which a CPS can be obtained.	NIST SP 1500-201 [B88]
Producibility	Concerns related to the ease and reliability with which a CPS design can be successfully manufactured.	NIST SP 1500-201 [B88]

Concern	Description	Source ^a
Quality	Concerns related to the ease and reliability of assessing whether a CPS meets stakeholder (especially customer) expectations.	NIST SP 1500-201 [B88]
Regulatory	Concerns related to regulatory requirements and certifications.	NIST SP 1500-201 [B88]
Relationship between data	Concerns related to how and why sets of data shall, may, or may not be associated with each other and the value or harm that can be derived from those associations.	NIST SP 1500-201 [B88]
Relevance	Concerns related to interpretation of fit based on situational context and significance.	IEC White Paper 2015 [B52], Murdock et al. [B78]
Reliability	Concerns related to the ability of the CPS to deliver stable and predictable performance in expected conditions.	NIST SP 1500-201 [B88]
Resilience	Concerns related to the ability of the CPS to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.	NIST SP 1500-201 [B88]
Responsibility	Concerns related to the ability to identify the entity or entities authorized to control the operation of a CPS.	NIST SP 1500-201 [B88]
Safety	Concerns related to the ability of the CPS to help ensure the absence of catastrophic consequences on the life, health, property, or data of CPS stakeholders and the physical environment.	NIST SP 1500-201 [B88]
Security	Concerns related to the ability of the CPS to help ensure that all of its processes, mechanisms (both physical and cyber), and services are afforded internal or external protection from unintended and unauthorized access, change, damage, destruction, or use. Confidentiality: Preserving authorized restrictions on access and disclosure. Integrity: Guarding against improper modification or destruction of a system, and includes ensuring non-repudiation and authenticity. Availability: Ensuring timely and reliable access to and use of a system.	NIST SP 1500-201 [B88]
Sensing	Concerns related to the ability of a CPS to develop the situational awareness required to perform its function.	NIST SP 1500-201 [B88]
Standardization	Concerns related to the availability and applicability of standards and the need for standards. Standards can help to achieve compatibility, ^b safety, security, repeatability, and quality. Standards can also facilitate commoditization of technologies and processes.	The present document
States	Concerns related to the states of a CPS. For example, the functional state of a CPS is frequently used to allow for variation in the CPS response to the same set of inputs. Variation in response based on state is sometimes referred to as functional modes.	NIST SP 1500-201 [B88]
Synchronization	Concerns for synchronization are that all associated nodes have timing signals traceable to the same time scale with accuracies as required. There are three kinds of synchronization that might be required: time, phase, and frequency synchronization, although frequency synchronization is also called <i>syntonization</i> .	NIST SP 1500-201 [B88]
Time awareness	Concerns that allow time correctness by design. The presence or absence of time explicitly in the models used to describe, analyze, and design CPS and in the actual operation of the components. This is a lifecycle concern as well as a concern for the ability to build devices without the need for extensive calibration of the timing properties.	NIST SP 1500-201 [B88]
Time to market	Concerns related to the time period required to bring a CPS from need realization through deployment.	NIST SP 1500-201 [B88]

Concern	Description	Source ^a
Time interval and latency	Specifying requirements for timing generally involves requirements for time intervals between pairs of events. A time interval is the duration between two instants read on the same time scale. CPS timing requirements are generally expressed as constraints on the time intervals (TI) between pairs of system significant events. These can be categorized in terms of bounded TIs or latency, deterministic TIs, and accurate TIs.	NIST SP 1500-201 [B88]
Uncertainty	Managing the effects of uncertainties is a fundamental challenge in CPS. Sources of uncertainty in CPS can be grouped into statistical (aleatoric) uncertainty, lack of knowledge (epistemic) uncertainty, or systematic uncertainty. In CPS, statistical uncertainty is caused by randomness of accuracy of sensing and actuation, often caused by uncertainty of manufacturing processes. Systematic uncertainty is caused by incomplete knowledge either due to limits of acquired knowledge or due to simplification in modeling. Typical manifestations of epistemic uncertainty are limited validity of models of physical processes or limits of computability of properties of mathematical models.	NIST SP 1500-201 [B88]
Usability	Concerns related to the ability of a CPS to be used to achieve its functional objectives effectively, efficiently, and to the satisfaction of users (see ISO 9241-210). The combination of physical and cyber into complex systems creates challenges in meeting usability goals. Complexity is a major issue. The diversity of interfaces creates a significant learning curve for human interaction.	NIST SP 1500-201 [B88]
Utility	Concerns related to the ability of a CPS to provide benefit or satisfaction through its operation. Utility reflects a business concern, especially when considered as the numerator when computing value, which equals utility divided by costs.	NIST SP 1500-201 [B88]

^a If coming from an external source.

^b Interoperability is a level of compatibility.

6. Architecture framework

6.1 General information

Figure 11 shows a model of the architecture framework being described in the present document. Subclause 3.2 and Clause 5 have provided background in terms of representative domains, stakeholders, and views of the concerns to be addressed. Clause 6 now uses that background to construct the body of the architecture description as described in ISO/IEC/IEEE 42010:2011.

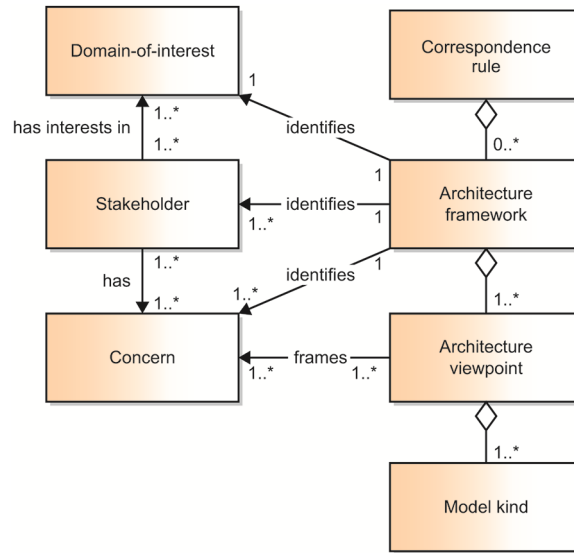


Figure 11—Conceptual model of an architecture framework (based on ISO/IEC/IEEE 42010:2011)

6.2 Viewpoints and model kinds

Viewpoints and model kinds are the foundation of the architecture framework. Subclause 6.6 presents a catalogue of viewpoints which frame the concerns described in 5.2. The viewpoints and model kinds govern the conventions for constructing, interpreting, using, and analyzing architecture views and models.

The following are different viewpoints abbreviations used for correspondence rule (CR) numbers:

- 6.3.2 CNC: Conceptual viewpoint
- 6.3.3 CMP: Compatibility viewpoint
- 6.3.4 LFC: Lifecycle viewpoint
- 6.3.5 COM: Communication viewpoint
- 6.3.6 INF: Information viewpoint
- 6.3.7 FUN: Function viewpoint
- 6.3.8 THM: Threat model viewpoint
- 6.3.9 SSM: Security and safe monitoring viewpoint
- 6.3.10 ACA: Access control viewpoint
- 6.3.11 ADS: Adequate design for required security viewpoint
- 6.3.12 PTR: Privacy and trust viewpoint
- 6.3.13 COL: Collaboration viewpoint
- 6.3.14 CPR: Computing resources viewpoint

An overview of the viewpoints provided in this standard, including pertinent correspondence rules, is provided in Table 3.

Table 3—Correspondence rules

Viewpoint	Subclause	Correspondence rule	Addressed viewpoint	Comment
Conceptual	6.6.2	CNC-CR-1	Compatibility	
		CNC-CR-2	Threat model	
		CNC-CR-3	Security and safety monitoring	
		CNC-CR-4	Access control architecture	
		CNC-CR-5	Adequate design for architecture	
		CNC-CR-6	Communication	
		CNC-CR-7	Collaboration	
		CNC-CR-8	Lifecycle	
Compatibility	6.6.3	CMP-CR-1	Conceptual	
		CMP-CR-2	Compatibility	
		CMP-CR-3	Lifecycle	
		CMP-CR-4	Communication	
		CMP-CR-5	Information	
		CMP-CR-6	Function	
		CMP-CR-7	Threat model	
		CMP-CR-8	Security and safety monitoring	
		CMP-CR-9	Access control architecture	
		CMP-CR-10	Adequate design for required security	
		CMP-CR-11	Privacy and trust	
		CMP-CR-12	Collaboration	
Lifecycle	6.6.4	—	All other viewpoints	The lifecycle is used to pattern all other architecture views.
Communication	6.6.5	COM-CR-1	Conceptual	
		COM-CR-2	Compatibility	
		COM-CR-3	Lifecycle	
		COM-CR-4	Communication	
		COM-CR-5	Information	
		COM-CR-6	Functional	
		COM-CR-7	Threat model	
		COM-CR-8	Security and safety monitoring	
		COM-CR-9	Access control architecture	
		COM-CR-10	Adequate design for required security	
		COM-CR-11	Privacy and trust	
		COM-CR-12	Collaboration	
Information	6.6.6	—	—	Influences the expression of model kinds in the viewpoints lifecycle, communication, collaboration, and information.
Functional	6.6.7	FUN-CR-1	Conceptual	
		FUN-CR-2	Compatibility	
		FUN-CR-3	Lifecycle	
		FUN-CR-4	Communication	
		FUN-CR-5	Information	
		FUN-CR-6	Threat model	
		FUN-CR-7	Security and safety monitoring	

Viewpoint	Subclause	Correspondence rule	Addressed viewpoint	Comment
		FUN-CR-8	Access control architecture	
		FUN-CR-9	Adequate design for required security	
		FUN-CR-10	Privacy and trust	
		FUN-CR-11	Collaboration	
Threat model	6.6.8	THM-CR-1	Functional and information viewpoint	
		THM-CR-2	All security-related viewpoints	
Security and safety monitoring	6.6.9	SSM-CR-1	Conceptual	Threat and security policy viewpoints should govern monitoring system sensor deployment.
		SSM-CR-2	Conceptual	All significant security and safety events and possible attacks should be monitored by monitoring system sensors.
		SSM-CR-3	Functional and informational	The functional and informational viewpoints govern endpoint IoT device interface monitoring. Signature detection should be provided for all user-visible device interfaces.
		SSM-CR-4	Conceptual	The deployment model should include monitoring system components.
Access control architecture	6.6.10	ACA-CR-1	Functional	
		ACA-CR-2	Threat model and functional	
		ACA-CR-3	Security and safety monitoring	
Adequate design for required security	6.6.11	ADS-CR-1	Security-related viewpoints	
		ADS-CR-2	Security-related viewpoints	
		ADS-CR-3	Treat model	
		ADS-CR-4	Security-related viewpoints	
		ADS-CR-5	Security-related viewpoints	
		ADS-CR-6	Security-related viewpoints	
		ADS-CR-7	Collaboration	
Privacy and trust	6.6.12	—	—	
Collaboration	6.6.13	COL-CR-1	Conceptual	
		COL-CR-2	Adequate design for required security	
		COL-CR-3	All other viewpoints	
Computing resources	6.6.14	CPR-CR-1	Communication	
		CPR-CR-2	Functional	

6.3 Architecture development

The architects select appropriate viewpoints to help them develop views addressing specific concerns based on the target system. It is not required to use all the viewpoints provided in 6.6. It is anticipated that architects may develop additional viewpoints and model kinds to apply in concert with those in 6.6 when addressing concrete systems of interest (Hilliard [B32]).

Guidance on the use of the framework is given in ISO/IEC/IEEE 42010:2011.

6.4 Rationale for key decisions

The rationale for the key decisions for an architecture of a system, with the framed concerns and their stakeholders and the architecture view, shall be specified according to the application needs.

6.5 Stakeholders and concerns

The stakeholders and concerns are presented in Clause 5.

6.6 Viewpoint catalogue

6.6.1 Overview

Subclause 6.6 describes the different detailed viewpoints of the IoT architecture framework. The viewpoint definition based on ISO/IEC/IEEE 42010:2011.

6.6.2 Conceptual viewpoint

6.6.2.1 General information and key features

The conceptual viewpoint is intended to assist architects in the design, analysis, and expression of system architectures employing a shared language. It frames a number of architecture concerns related to the concepts within architecture description and the use of such descriptions. It is important to address the conceptual view as a part of architecture to ensure that stakeholders are provided with a common vocabulary and semantics when talking about IoT systems.

The definition of conceptual models, i.e., of entities and their relationships, stimulates coherence and consistency of architecting products (architecture descriptions, built systems, etc.). Conceptual models foster communication over application-domain borders, organizational borders (e.g., across teams), and cultural borders (e.g., world regions). Conceptual models also foster communication across stakeholder “generations,” e.g., successive employee generations. Also, instantiating the conceptual view fosters an architecture description language that remains stable during revisions and during reuse, e.g., when creating architecture descriptions for new systems of interest. Conceptual models are especially helpful for stakeholders interested in more than one system. This interest can manifest over time or at once. An example for the former is a builder who designs new product generations.

The conceptual viewpoint employs six model kinds: the entity model kind, the system model kind, the intent model kind, the IoT component model kind, the IoT component capability model kind, and the representation model kind.

6.6.2.2 Stakeholders and concerns

Stakeholders for this viewpoint are as defined in 5.1. An architect is an additional stakeholder of this viewpoint.

Table 4 shows the concerns of the conceptual viewpoint.

Table 4—Conceptual viewpoint; concerns

Concern from common concerns list	Elements of the concerns framed by the architecture framework
Assurance	How can we convince stakeholders we have met our obligations for being safe, reliable, resilient, secure, and meeting privacy expectations?
Concept	How can we make system concepts reusable, e.g., over product generations and/or across engineering teams?
Concept	How can we make architecture descriptions—and the concepts they employ—comparable to each other?
Concept, cost	How can we improve the communication between teams? ^a
Constructivity	How can we increase the standardized composition of component interfaces?
Engineerability	How can we aid architects and implementers with the design of component interfaces?
Standardization	How can we support the clarification where IoT standardization is needed?
Standardization	How can we support gap analyses of IoT standards?
Procureability	How can system offers be made more comparable?

^a For a thorough discussion of the architectural implications of communication borders see Conway [B19].

6.6.2.3 Anti-concerns for this viewpoint

This viewpoint does not address implementation details, e.g., how an IoT component is implemented, nor how interfaces between IoT components shall be implemented.

6.6.2.4 Model kinds

6.6.2.4.1 General

The main model kinds for any conceptual view intended to describe an IoT system architecture include:

- Entity model kind
- System model kind
- Intent model kind
- IoT component model kind
- IoT component capability model kind
- Representation model kind

6.6.2.4.2 Entity model kind

6.6.2.4.2.1 Objective

In order to differentiate distinguishable manifestations from others and how they are described, e.g., distinguishing a human from a sensor, we introduce the entity model kind.

6.6.2.4.2.2 Conventions

6.6.2.4.2.2.1 General

An entity has a physical manifestation and/or a conceptual representation. Note that a conceptual representation has at least one physical manifestation, for instance an XML file on a hard disk, but the physical manifestation of a conceptual representation is likely abstracted out of view.

The concept of an entity is not used in its wider ontological sense (see, for instance, Hohendorf [B33]), i.e., that anything perceivable is an entity. Rather, the entity concept is used in a narrow sense: Only manifestations and representations pertaining to an IoT system are modeled as entities, while related categories—for instance attributes of these manifestations—are not. Attributes are abstractions that represent the interpreter's understanding of an entity. Examples for attributes are color, temperature, and spatial dimensions.

6.6.2.4.2.2.2 Model kind languages or notations

This model is presented in UML 2.2 [B94], particularly the class-diagram pattern. Other modeling languages that are capable of representing ontologies are also feasible, including natural languages.

6.6.2.4.2.2.3 Model kind meta-model

The ontology of the concept entity is shown in Figure 12.

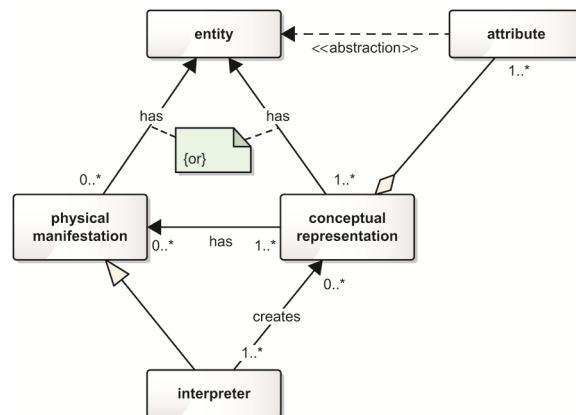


Figure 12—Ontology of the concept entity (class diagram)

6.6.2.4.2.3 Correspondence rules

The entity concept is used in all other model kinds in this viewpoint.

6.6.2.4.3 System model kind

6.6.2.4.3.1 Objective

One of the central concepts used in this standard is that of a system. This model kind provides the reader with a list of axioms that all systems fulfill. Subclause 6.6.2.4.3 also refers to an open list of propositions tied to each of the axioms and it discusses the most relevant propositions. Note that some of these propositions are addressed in other model kinds (see 6.6.2.4.7.3).

6.6.2.4.3.2 Conventions

The following axioms apply to all designed systems, and thus to all IoT systems (Whitney et al. [B146]):

- The centrality axiom states that central to all systems are two pairs of propositions: emergence and hierarchy, and communication and control.
- The contextual axiom states that system meaning is informed by the circumstances and factors that surround the system.
- The design axiom states that system design is a purposeful balancing of resources and relationships.
- The goal axiom states that systems achieve specific goals through purposeful behavior using pathways and means.
- The information axiom states that systems create, possess, transfer, and modify information.

An open list of propositions aligned with these axioms can be found elsewhere in the literature (Whitney et al. [B146]). Every IoT system adhering to this standard adheres to the axioms above, but it does not need to adhere to all of the aforementioned propositions. Let us next address a proposition that all IoT systems fulfill.

Hierarchy (centrality axiom): “Entities meaningfully treated as wholes are built up of smaller entities which are themselves, wholes. In a hierarchy, emergent properties denote the levels” (Whitney et al. [B146]). This proposition implies that emergent levels can be used when identifying hierarchy levels within an IoT system. Note that the hierarchy can be “flat,” for instance, for peer-to-peer systems.

Other relevant propositions are addressed in 6.6.2.4.3.3 and 6.6.2.4.3.4.

6.6.2.4.3.3 Operations

The following propositions shall be heeded when instantiating this model kind.

Boundary (contextual axiom): “The abstract, semi-permeable perimeter of the system defines the components that make up the system, segregating them from environmental factors and may prevent or permit entry of matter, energy and information.” (Whitney et al. [B146]). This proposition implies that the IoT architecture description shall define the system boundary. Note that this “physical” boundary is not the only one that can be defined for a system. Other boundaries can be drawn, for instance, for contingent parts of the system that can be accessed by users, for all parts information components that utilize encryption, etc.

Requisite parsimony (design axiom): “The capacity of human short-term recall is no greater than seven plus or minus two items.” (Whitney et al. [B146]). This limitation is relevant when compiling architecture descriptions that can readily be parsed by the stakeholders.

6.6.2.4.3.4 Correspondence rules

This model kind applies everywhere in the standard where the concept *system* is used.

The following propositions have implications for other model kinds in this viewpoint and also other viewpoints. These propositions are ordered by the system axioms.

Centrality axiom

Emergence: “Whole entities exhibit properties and patterns that are meaningful only when they are attributed to the whole, not its parts.” (Whitney et al. [B146]). This has, among others, implications for the sensors and actuators to be chosen (see 6.6.2.4.6) and for the information viewpoint. The implication for the latter is that meaning and thus knowledge is generated through synthesis. For instance, if an IoT system tracks the movement of cows on a pasture, one cannot infer whether a herd is in panic from the movement of a single cow. Rather, the IoT system needs to track the movement of several cows in order to infer this judgment. Interestingly, the fusion of different types of sensor data can enhance the reliability of this inference. In the cow herd example, the IoT system can, for instance, also record audio and listen for lowing.

Communication: “Communication is a transaction between the information source terminal and the destination terminal, with the sole aim of generation and reproduction of symbols. Information is transmitted as a selection along possible alternative states.” (Whitney et al. [B146]). This proposition implies a central role for communication in IoT systems. Communication is addressed in the communication viewpoint (see 6.6.5).

Contextual axiom

The choice of the system boundary has implications on the intent model kind (see 6.6.2.4.4). For instance, are the physical entities, which the IoT system interacts with, chosen to be part of the IoT system or not? This choice has repercussions for what constitutes the environment of the IoT system (see, for instance, the core conceptual model kind in 6.6.2.4.6).

The goal axiom

Purposeful behavior: “Purposeful behavior is meant to denote that the act or behavior may be interpreted as directed to the attainment of a goal—i.e., to a final condition in which the behaving object reaches a definite correlation in time or in space with respect to another object or event.” (Whitney et al. [B146]). This implies the centrality of the goal for the IoT system (see the “intent model kind” in 6.6.2.4.4).

The information axiom

Redundancy of potential command: “Effective action is achieved by an adequate concatenation of information.” (Whitney et al. [B146]). This implies that information synthesis is important for IoT systems and needs thus to be reflected in the information view of an IoT system. Note that information synthesis also plays a role for emergent properties (see the proposition *Emergence* above).

6.6.2.4.4 Intent model kind

6.6.2.4.4.1 Objective

The intent model kind links IoT stakeholder goals to IoT systems, as well as to the entities of interest with which the IoT system interacts. The importance of the system goal is implied by the purposive-behavior system proposition (see 6.6.2.4.3.4). A stakeholder's intent has implications for—among others—what is considered to be the entity of interest and what not (Floridi [B27]). For instance, for the user of an IoT-based fitness trainer that tracks pulse rate during training, the user itself is the entity of interest. For a person responsible for the maintenance of the fitness trainer, e.g., for calibration purposes, the IoT device itself, i.e., the fitness trainer, is the entity of interest.

6.6.2.4.4.2 Conventions

6.6.2.4.4.2.1 General

This model kind adopts the stakeholder concept promoted by ISO/IEC/IEEE 42010:2011 (see Clause 5). It also adopts the role concept promoted by TOGAF (The Open Group [B119]).

6.6.2.4.4.2.2 Model kind languages or notations

This model is presented in UML 2.2 [B94], particularly the class-diagram pattern. Other modeling languages that are capable of representing ontologies are also feasible, including natural languages.

6.6.2.4.4.2.3 Model kind meta-model

This model kind describes the properties and roles of humans and stakeholders and how they relate to IoT systems. The intermediate between the former and the latter is goals and intent. It is represented by two class diagrams (see Figure 13 and Figure 14).

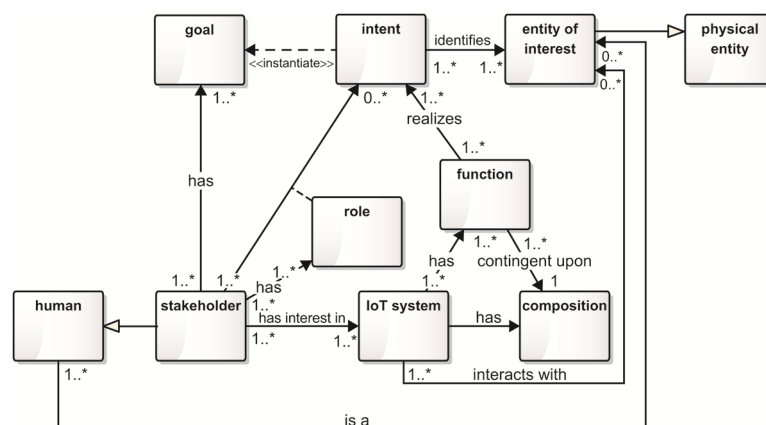


Figure 13—Class diagram of the intent model kind

A stakeholder is a human that has goals, which identify entities of interest. A human can be an entity of interest. An IoT system is a cyber-physical system, which interacts with the physical world through sensors