

This is a preview - click here to buy the full publication



ISO/IEC 30141

Edition 1.0 2018-08

INTERNATIONAL STANDARD



Internet of Things (IoT) – Reference architecture

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.020

ISBN 978-2-8322-5972-6

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references	9
3 Terms and definitions	9
4 Abbreviated terms	9
5 Internet of Things Reference Architecture (IoT RA) conformance.....	10
6 IoT RA goals and objectives	10
6.1 General.....	10
6.2 Characteristics.....	11
6.3 Conceptual Model.....	11
6.4 Reference Model and architecture views.....	11
7 Characteristics of IoT systems.....	12
7.1 General.....	12
7.2 IoT system trustworthiness characteristics	13
7.2.1 General	13
7.2.2 Availability.....	14
7.2.3 Confidentiality.....	14
7.2.4 Integrity	15
7.2.5 Protection of personally identifiable information (PII)	15
7.2.6 Reliability.....	16
7.2.7 Resilience.....	17
7.2.8 Safety.....	17
7.3 IoT system architecture characteristics	18
7.3.1 Composability.....	18
7.3.2 Functional and management capability separation	18
7.3.3 Heterogeneity	19
7.3.4 Highly distributed systems	20
7.3.5 Legacy support.....	20
7.3.6 Modularity.....	21
7.3.7 Network connectivity.....	21
7.3.8 Scalability.....	22
7.3.9 Shareability	22
7.3.10 Unique identification	23
7.3.11 Well-defined components.....	23
7.4 IoT system functional characteristics	24
7.4.1 Accuracy	24
7.4.2 Auto-configuration	25
7.4.3 Compliance	25
7.4.4 Content-awareness.....	26
7.4.5 Context-awareness	26
7.4.6 Data characteristics – volume, velocity, veracity, variability and variety	27
7.4.7 Discoverability	27
7.4.8 Flexibility	28
7.4.9 Manageability	29
7.4.10 Network communication.....	29

7.4.11	Network management and operation.....	30
7.4.12	Real-time capability	31
7.4.13	Self-description	31
7.4.14	Service subscription	32
8	IoT Conceptual Model (CM).....	32
8.1	Main purpose	32
8.2	Concepts in the IoT CM	33
8.2.1	IoT entities and domains.....	33
8.2.2	Identity	35
8.2.3	Services, network, IoT device and IoT gateway	36
8.2.4	IoT-User	38
8.2.5	Virtual entity, Physical Entity and IoT device.....	39
8.3	High level view of CM	41
9	IoT Reference Model (RM).....	42
9.1	The IoT Reference Model context	42
9.2	IoT RMs	42
9.2.1	Entity-based RM	42
9.2.2	Domain-based RM	44
9.2.3	Relation between entity-based RM and domain-based RM.....	46
10	IoT Reference Architecture (RA) views	46
10.1	General description.....	46
10.2	IoT RA functional view	47
10.2.1	General	47
10.2.2	Intra-domain functional components	47
10.2.3	Cross-domain capabilities.....	50
10.3	IoT RA system deployment view	51
10.3.1	General	51
10.3.2	Systems/sub-systems in Physical Entity Domain (PED)	52
10.3.3	Systems/sub-systems in Sensing & Controlling Domain (SCD)	52
10.3.4	Systems/sub-systems in Application & Service Domain (ASD).....	52
10.3.5	Systems/sub-systems in Operation & Management Domain (OMD).....	53
10.3.6	Systems/sub-systems in User Domain (UD).....	53
10.3.7	Systems/sub-systems in Resource Access & Interchange Domain (RAID)	53
10.4	IoT RA networking view	54
10.4.1	Communications networks	54
10.4.2	Communication networks implementation	55
10.5	IoT RA usage view.....	56
10.5.1	General description	56
10.5.2	Description of the roles, sub-roles and related activities	56
10.5.3	Mapping activities, roles and IoT systems in domains	61
11	IoT trustworthiness	64
11.1	General.....	64
11.2	Safety	65
11.3	Security	66
11.3.1	General	66
11.3.2	IoT system Information Security Management System (ISMS)	66
11.3.3	IoT system & product Security Life Cycle Reference Model	68
11.4	Privacy and PII Protection.....	69

11.5	Reliability.....	72
11.6	Resilience.....	73
11.7	Trustworthiness and the Reference Architecture.....	74
Annex A (informative)	Interpreting UML Class diagram for Conceptual Model.....	76
Annex B (informative)	Entity relationship tables for the CM.....	77
B.1	IoT entities and domains.....	77
B.2	Identity.....	78
B.3	Services, network, IoT device and IoT gateway.....	78
B.4	IoT-User.....	79
B.5	Virtual entity, Physical Entity and IoT device.....	80
Annex C (informative)	Relation between CM, RMs and RAs.....	81
Bibliography.....		83
Figure 1	– From generic Reference Architecture to context specific architecture.....	8
Figure 2	– IoT RA structure.....	11
Figure 3	– RM and architecture views.....	12
Figure 4	– Entity and domain concepts of the CM.....	33
Figure 5	– Domain interactions of the CM.....	34
Figure 6	– Identity concept of the CM.....	35
Figure 7	– Service, network, IoT device and IoT gateway concepts of the CM.....	36
Figure 8	– IoT-User concepts of the CM.....	38
Figure 9	– Virtual entity, Physical Entity, and IoT device concepts of the CM.....	39
Figure 10	– High level view of CM.....	41
Figure 11	– Entity-based IoT RM.....	42
Figure 12	– Domain and entity relationship, and representative conceptual entities in IoT systems.....	44
Figure 13	– Domain-based IoT RM.....	44
Figure 14	– Relation between entity-based RM and domain-based RM.....	46
Figure 15	– IoT RA functional view –decomposition of IoT RA functional components.....	47
Figure 16	– IoT RA system deployment view.....	52
Figure 17	– IoT RA networking view.....	54
Figure 18	– Roles present when the system is in use.....	57
Figure 19	– IoT service provider sub-roles and activities.....	59
Figure 20	– IoT service developer sub-roles and activities.....	60
Figure 21	– IoT-User sub-roles and activities.....	61
Figure 22	– Activities of device and application development.....	63
Figure 23	– Using device data for security-related analytics and operations.....	64
Figure 24	– IoT product Security Life Cycle Reference Model.....	69
Figure A.1	– Generalization.....	76
Figure A.2	– Association.....	76
Figure C.1	– Relation between IoT CM, RM, and RA.....	82
Table 1	– Characteristics of IoT systems.....	13
Table 2	– Overview of activities and roles.....	62

Table B.1 – Entity	77
Table B.2 – Domain	77
Table B.3 – Digital Entity	77
Table B.4 – Physical Entity	77
Table B.5 – IoT-User.....	77
Table B.6 – Network	78
Table B.7 – Identifier	78
Table B.8 – Endpoint	78
Table B.9 – IoT gateway	78
Table B.10 – IoT device	79
Table B.11 – Service.....	79
Table B.12 – Human user	79
Table B.13 – Digital user.....	79
Table B.14 – Application	80
Table B.15 – Sensor	80
Table B.16 – Actuator	80
Table B.17 – Virtual entity.....	80

INTERNET OF THINGS (IoT) – REFERENCE ARCHITECTURE

FOREWORD

- 1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.
- 2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees and ISO member bodies.
- 3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.
- 5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.
- 8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 30141 was prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC joint technical committee 1: Information technology.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

IoT has a broad use in industry and society today and it will continue to develop for many years to come. Various IoT applications and services have adopted IoT techniques to provide capabilities that were not possible a few years ago. IoT is one of the most dynamic and exciting areas of ICT. It involves the connecting of Physical Entities (“things”) with IT systems through networks. Foundational to IoT are the electronic devices that interact with the physical world. Sensors collect the information about the physical world, while actuators can act upon Physical Entities. Both sensors and actuators can be in many forms such as thermometers, accelerometers, video cameras, microphones, relays, heaters or industrial equipment for manufacturing or process controlling. Mobile technology, cloud computing, big data and deep analytics (predictive, cognitive, real-time and contextual) play important roles by gathering and processing data to achieve the final result of controlling Physical Entities by providing contextual, real-time and predictive information which has an impact on physical and virtual entities.

IoT can be integrated into existing technologies. Real-time measurements generated by adding sensors to existing technology can improve its functionality and lower the cost of operations (e.g. smart traffic signals can adapt to traffic conditions, lowering congestion and air pollution). The data generated by IoT sensors can support new business models and tailor products and services to the tastes and needs of the customer. In addition to the applications, the technology needs to support supervision and adaptation of the IoT system itself.

Several forecasts indicate that IoT will connect 50 billion devices worldwide by the year 2020. There are a number of possible application areas, such as smart city, smart grid, smart home/building, digital agriculture, smart manufacturing, intelligent transport system, e-Health. IoT is an enabling technology that consists of many supporting technologies, for example, different types of communication networking technologies, information technologies, sensing and control technologies, software technologies, device/hardware technologies. This document is based on widely used enabling technologies that are defined in standards from several organizations such as ISO, IEC, ITU, IETF, IEEE, ETSI, 3GPP, W3C, etc.

Trustworthiness is recognized as an area of importance, and IoT can leverage current and future best practice. For example, monitoring and analysing deployed IoT systems is essential to maintain reliability and safety and security. Measures such as controlled access can ensure the security of the system.

This document provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practices. It uses a top down approach, beginning with collecting the most important characteristics of IoT, abstracting those into a generic IoT Conceptual Model, deriving a high level system based reference with subsequent dissection of that model into the four architecture views (functional view, system view, networking view and usage view) from different perspectives.

This document serves as a base from which to develop (specify) context specific IoT architectures and thence actual systems. The contexts can be of different kinds but shall include the business context, the regulatory context and the technological context, e.g. industry verticals, technological requirements and/or nation-specific requirement sets. For more information, see Figure 1.

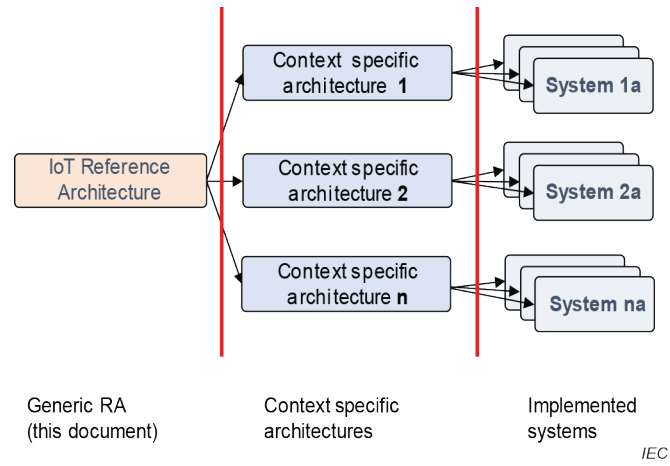


Figure 1 – From generic Reference Architecture to context specific architecture

INTERNET OF THINGS (IoT) – REFERENCE ARCHITECTURE

1 Scope

This document specifies a general IoT Reference Architecture in terms of defining system characteristics, a Conceptual Model, a Reference Model and architecture views for IoT.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 20924, *Internet of Things (IoT) – Definition and vocabulary*¹

¹ Under preparation. Stage at time of publication: ISO/IEC CDV 20924:2018.