AS ISO/IEC 30141:2021
ISO/IEC 30141:2018

Australian STANDARD®

STANDARDS Australia

Internet of Things (IoT) — Reference Architecture



AS ISO/IEC 30141:2021

This Australian Standard® was prepared by IT-042, Internet of Things and Related Technologies. It was approved on behalf of the Council of Standards Australia on 4 January 2021.

This Standard was published on 22 January 2021.

The following are represented on Committee IT-042:

Australian Academy of Technological Sciences and Engineering
Australian Communications and Media Authority
Australian Communications Consumer Action Network
Australian Industry Group
Australian Information Industry Association
Australian Smart Communities Association
Communications Alliance
Consumers Federation of Australia
CSIRO Data61
Engineers Australia
IoT Alliance Australia
NSW Data Analytics Centre
University of Technology Sydney
Water Services Association of Australia

This Standard was issued in draft form for comment as DR AS ISO/IEC 30141:2020.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76113 157 8

AS ISO/IEC 30141:2021
ISO/IEC 30141:2018

Internet of Things (IoT) — Reference Architecture

First published as AS ISO/IEC 30141:2021.

COPYRIGHT

© ISO/IEC 2021 — All rights reserved
© Standards Australia Limited 2021

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by the Standards Australia Committee IT-042, Internet of Things and Related Technologies.

The objective of this document is to specify a general IoT reference architecture in terms of defining system characteristics, a conceptual model, a reference model and architecture views for IoT.

This document is identical with, and has been reproduced from, ISO/IEC 30141:2018, *Internet of Things (loT) — Reference Architecture*.

As this document has been reproduced from an International Standard, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

© Standards Australia Limited 2021

Contents

Preface ii
FOREWORD v
INTRODUCTION vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviated terms 1
5 Internet of Things Reference Architecture (IoT RA) conformance 2
6 IoT RA goals and objectives 2
6.1 General 2
6.2 Characteristics 3
6.3 Conceptual Model 3
6.4 Reference Model and architecture views 3
7 Characteristics of IoT systems 4
7.1 General 4
7.2 IoT system trustworthiness characteristics 5
7.2.1 General 5
7.2.2 Availability 5
7.2.3 Confidentiality 6
7.2.4 Integrity 6
7.2.5 Protection of personally identifiable information (PII) 7
7.2.6 Reliability 8
7.2.7 Resilience 8
7.2.8 Safety 9
7.3 IoT system architecture characteristics 9
7.3.1 Composability 9
7.3.2 Functional and management capability separation 10
7.3.3 Heterogeneity 11
7.3.4 Highly distributed systems 11
7.3.5 Legacy support 12
7.3.6 Modularity 13
7.3.7 Network connectivity 13
7.3.8 Scalability 14
7.3.9 Shareability 14
7.3.10 Unique identification 14
7.3.11 Well-defined components 15
7.4 IoT system functional characteristics 15
7.4.1 Accuracy 15
7.4.2 Auto-configuration 16
7.4.3 Compliance 16
7.4.4 Content-awareness 17
7.4.5 Context-awareness 18
7.4.6 Data characteristics – volume, velocity, veracity, variability and variety 18
7.4.7 Discoverability 18
7.4.8 Flexibility 19
7.4.9 Manageability 20
7.4.10 Network communication 21
7.4.11 Network management and operation 21
7.4.12 Real-time capability 22
7.4.13 Self-description 22
7.4.14 Service subscription 23

8 IoT Conceptual Model (CM) 24
8.1 Main purpose 24
8.2 Concepts in the IoT CM 25
8.2.1 IoT entities and domains 25
8.2.2 Identity 27
8.2.3 Services, network, IoT device and IoT gateway 28
8.2.4 IoT-User 30
8.2.5 Virtual entity, Physical Entity and IoT device 31
8.3 High level view of CM 33

9 IoT Reference Model (RM) 34
9.1 The IoT Reference Model context 34
9.2 IoT RMs 34
9.2.1 Entity-based RM 34
9.2.2 Domain-based RM 36
9.2.3 Relation between entity-based RM and domain-based RM 38

10 IoT Reference Architecture (RA) views 39
10.1 General description 39
10.2 IoT RA functional view 39
10.2.1 General 39
10.2.2 Intra-domain functional components 39
10.2.3 Cross-domain capabilities 43
10.3 IoT RA system deployment view 44
10.3.1 General 44
10.3.2 Systems/sub-systems in Physical Entity Domain (PED) 45
10.3.3 Systems/sub-systems in Sensing & Controlling Domain (SCD) 45
10.3.4 Systems/sub-systems in Application & Service Domain (ASD) 45
10.3.5 Systems/sub-systems in Operation & Management Domain (OMD) 46
10.3.6 Systems/sub-systems in User Domain (UD) 46
10.3.7 Systems/sub-systems in Resource Access & Interchange Domain (RAID) 46
10.4 IoT RA networking view 46
10.4.1 Communications networks 46
10.4.2 Communication networks implementation 48
10.5 IoT RA usage view 49
10.5.1 General description 49
10.5.2 Description of the roles, sub-roles and related activities 49
10.5.3 Mapping activities, roles and IoT systems in domains 53

11 IoT trustworthiness 55
11.1 General 55
11.2 Safety 56
11.3 Security 57
11.3.1 General 57
11.3.2 IoT system Information Security Management System (ISMS) 57
11.3.3 IoT system & product Security Life Cycle Reference Model 59
11.4 Privacy and PII Protection 60
11.5 Reliability 62
11.6 Resilience 63
11.7 Trustworthiness and the Reference Architecture 65

Annex A (informative) **Interpreting UML Class diagram for Conceptual Model 66**

Annex B (informative) **Entity relationship tables for the CM 67**

Annex C (informative) **Relation between CM, RMs and RAs 71**

Bibliography 73

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.

© Standards Australia Limited 2021

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.

© Standards Australia Limited 2021

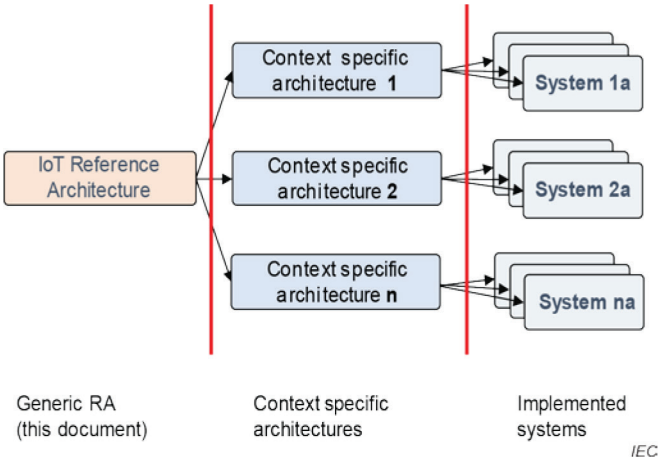


Figure 1 — From generic Reference Architecture to context specific architecture

© Standards Australia Limited 2021

NOTES

Australian Standard®

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)]

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20924 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

4 Abbreviated terms

5Vs	volume, velocity, veracity, variability, and variety
API	application programming interface
ASD	Application & Service Domain
BSS	business support systems
CMC	Conceptual Model
FQDN	fully qualified domain name
HMI	human machine interface
HTTP	Hypertext Transfer Protocol
HVAC	heating, ventilation and air conditioning
IaaS	infrastructure as a service
ICT	information and communication technologies
IoT	Internet of Things
IoT RA	Internet of Things Reference Architecture
LAN	local area network

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

© Standards Australia Limited 2021