ISO/IEC 30147

Edition 1.0 2021-05

INTERNATIONAL STANDARD

Internet of things (IoT) – Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes



ISO/IEC 30147:2021-05(en)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2021 ISO/IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

ISO/IEC 30147

Edition 1.0 2021-05

INTERNATIONAL STANDARD

Internet of things (IoT) – Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.020; 35.030

ISBN 978-2-8322-9808-4

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

CONTENTS

FOREWORD 4
INTRODUCTION 5
1 Scope 6
2 Normative references 6
3 Terms and definitions 6
4 Abbreviated terms 9
5 IoT systems/services and IoT trustworthiness 9
5.1 Characteristics specific to IoT systems and services 9
5.2 IoT trustworthiness 11
6 Processes for realizing IoT trustworthiness 12
6.1 General 12
6.2 Agreement processes 12
6.2.1 Acquisition process 12
6.2.2 Supply process 13
6.3 Organizational project-enabling processes 13
6.3.1 Life cycle model management process 13
6.3.2 Infrastructure management process 13
6.3.3 Portfolio management process 13
6.3.4 Human resource management process 13
6.3.5 Quality management process 13
6.3.6 Knowledge management process 14
6.4 Technical management processes 14
6.4.1 Project planning process 14
6.4.2 Project assessment and control process 14
6.4.3 Decision management process 15
6.4.4 Risk management process 15
6.4.5 Configuration management process 16
6.4.6 Information management process 16
6.4.7 Measurement process 16
6.4.8 Quality assurance process 17
6.5 Technical processes 17
6.5.1 Business or mission analysis process 17
6.5.2 Stakeholder needs and requirements definition process 17
6.5.3 System requirements definition process 18
6.5.4 Architecture definition process 19
6.5.5 Design definition process 19
6.5.6 System analysis process 20
6.5.7 Implementation process 20
6.5.8 Integration process 20
6.5.9 Verification process 21
6.5.10 Transition process 22
6.5.11 Validation process 22
6.5.12 Operation process 23
6.5.13 Maintenance process 24
6.5.14 Disposal process 24

Annex A (informative) Examples of risks specific to IoT systems 25
A.1 General 25
A.2 Example 1: Security risk 25
A.3 Example 2: Reliability risk 25
A.4 Example 3: Safety risk 25
A.5 Example 4: Privacy risk 26
A.6 Example 5: Resilience risk 26
A.7 Example 6: Risk arising from interconnected IoT trustworthiness factors 26
Annex B (informative) Overview of process and its application 27
B.1 Overview of approach toward process for IoT trustworthiness 27
B.2 Application of process to enhance IoT trustworthiness 29
Bibliography 30

Figure 1 – An IoT system, a system of systems 10

Table B.1 – Relations between typical characteristics of IoT systems and process bases 29

INTERNET OF THINGS (IoT) – INTEGRATION OF IoT TRUSTWORTHINESS ACTIVITIES IN ISO/IEC/IEEE 15288 SYSTEM ENGINEERING PROCESSES

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.
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 and ISO National bodies.
3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and 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 and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO 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 document.
7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National 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, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.
8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.
9) Attention is drawn to the possibility that some of the elements of this ISO/IEC document may be the subject of patent rights. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 30147 has been prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC joint technical committee 1: Information technology. It is an International Standard.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
JTC1-SC41/210/FDIS	JTC1-SC41/221/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1, available at www.iec.ch/members_experts/refdocs and www.iso.org/directives.

INTRODUCTION

In the Internet of Things (IoT), all IoT devices are mutually connected to each other and this is expected to bring new advantages to daily life. On the other hand, traditional system management devices (thermostats, lighting systems, traffic lights, etc.) which were not previously connected to the Internet are now being connected without regard to the level of IoT trustworthiness required by the system-of-interest. Many of these devices are being connected without the benefit of security controls and processes in place for servers, PCs, and smartphones. Flaws or failures in these devices caused by lack of IoT trustworthiness can have a deep impact on the users and system operation. This implies that there are conditions and characteristics specific to IoT systems and services which are different from those of other existing IT systems and services. Examples are as follows.

– The extent and the degree of impacts of threats are very wide and big.
– The life time of IoT systems and services, especially in operation and maintenance, is sometimes very long.
– It can be very difficult to monitor and manage some types of IoT devices.
– It can be difficult for communication entities including IoT devices to sufficiently know the environments of each other.
– The functions and performances of some IoT devices might be restricted technologically.
– In IoT systems and services, connections between entities can be made which the developers of the entities did not anticipate.

The purpose of this document is to provide guidance to realize IoT trustworthiness. This is because existing documents are targeted to each application area and do not necessarily cover all the challenges faced by the IoT system and service according to the above conditions and characteristics specific to IoT systems and services. This document provides system life cycle processes to realize IoT trustworthiness by applying and supplementing ISO/IEC/IEEE 15288:2015.

INTERNET OF THINGS (IoT) – INTEGRATION OF IoT TRUSTWORTHINESS ACTIVITIES IN ISO/IEC/IEEE 15288 SYSTEM ENGINEERING PROCESSES

1 Scope

This document provides system life cycle processes to implement and maintain trustworthiness in an IoT system or service by applying and supplementing ISO/IEC/IEEE 15288:2015. The system life cycle processes are applicable to IoT systems and services common to a wide range of application areas.

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.

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

ISO/IEC 27005:2018, *Information technology – Security techniques – Information security risk management*

ISO/IEC 27031:2011, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*

ISO/IEC 29134:2017, *Information technology – Security techniques – Guidelines for privacy impact assessment*

ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*

ISO 31000, *Risk management – Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC/IEEE 15288:2015, and the following apply.

NOTE The following terms are defined in ISO/IEC/IEEE 15288:2015:

acquirer, acquisition, activity, agreement, architecture, architecture viewpoint, asset, baseline, concept of operation, concern, customer, design (verb), design (noun), enabling system, environment, incident, information item, interface, life cycle, life cycle model, operational concept, operator, organization, party, problem, process, product, project, quality assurance, quality characteristic, quality management, requirement, resource, risk, stage, stakeholder, supplier, system, system element, system-of-interest, task, user, validation, verification.

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

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

3.1
asset
entity (3.6) that has value and is either owned by or under the custody of an individual, an organization, a government, or other groups

[SOURCE: ISO/IEC 20924:2021[1], 3.1.4]

3.2
availability
property of being accessible and usable on demand by an authorized entity (3.6)

Note 1 to entry: IoT systems can include both human users and service components as "authorized entities".

[SOURCE: ISO/IEC 27000:2018[2], 3.7]

3.3
characteristic
abstraction of a property of an entity (3.6) or of a set of entities

[SOURCE: ISO 18104:2014[3], 3.1.4]

3.4
component
modular, deployable, and replaceable part of a system that encapsulates implementation and exposes a set of interfaces

[SOURCE: ISO 14813-5:2010[4], B.1.31]

3.5
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities (3.6), or processes

[SOURCE: ISO/IEC 27000:2018[2], 3.10]

3.6
entity
thing (physical or non-physical) having a distinct existence

[SOURCE: ISO/IEC 15459-3:2014[5], 3.1, modified – In the definition, "anything" has been replaced by "thing".]

3.7
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018[2], 3.36]

3.8
Internet of Things
IoT
infrastructure of interconnected entities (3.6), people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world

[SOURCE: ISO/IEC 20924:2021[1], 3.2.4]

3.9
IoT device
entity (3.6) of an IoT system that interacts and communicates with the physical world through sensing or actuating

[SOURCE: ISO/IEC 20924:2021[1], 3.2.6]

3.10
IoT system
system providing functionalities of IoT

Note 1 to entry: An IoT system can include, but not be limited to, IoT devices, IoT gateways, sensors, and actuators.

[SOURCE: ISO/IEC 20924:2021[1], 3.2.9]

3.11
IoT trustworthiness
trustworthiness of an IoT system with characteristics including security, privacy, safety, reliability and resilience

Note 1 to entry: The term "trustworthiness" is defined at 3.1.34 in ISO/IEC 20924:2021 as the ability to meet stakeholder expectations in a demonstrable, verifiable and measurable way

Note 2 to entry: The relative importance of characteristics of IoT trustworthiness, including security, privacy, safety, reliability and resilience, depends on the nature and the context of the IoT system or service.

[SOURCE: ISO/IEC 20924:2021[1], 3.2.10, modified – Note 1 to entry and Note 2 to entry have been added.]

3.12
network
infrastructure that connects a set of endpoints, enabling communication of data between the digital entities (3.6) reachable through them

[SOURCE: ISO/IEC 20924:2021[1], 3.1.26]

3.13
reliability
ability of an item to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration may be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run, etc., and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

[SOURCE: IEC 60050-192:2015, 192-01-24]

3.14
resilience
tolerance of a system to malfunctions or capacity to recover functionality after stress

[SOURCE: ISO 18457:2016[6], 3.9]

3.15
security
protection against intentional subversion or forced failure, achieved by a composite of five attributes – confidentiality, integrity, availability, non-repudiation, and accountability – plus aspects of a sixth, usability, all of which have the related issue of their assurance

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.41, modified – In the definition, the attribute "non-repudiation" has been added.]

3.16
service
distinct functionality that is provided by an entity (3.6) through interfaces

[SOURCE: ISO/IEC 20924:2021[1], 3.1.30]

4 Abbreviated terms

ATM	automated teller machine
ICT	information and communication technology
IIoT	industrial IoT
OS	operating system
OT	operational technology
PC	personal computer
SoS	system of systems

5 IoT systems/services and IoT trustworthiness

5.1 Characteristics specific to IoT systems and services

An IoT service is a service provided by an IoT system which may be a system of systems (SoS), characterized as operationally and managerially independent of constituent systems (see 4.1 in ISO/IEC/IEEE 21839:2019[7][1], see also Figure 1). Note that there may be a case where no one is responsible for an IoT system which is an SoS. In such a case, it is a distinguishing feature of an IoT system that cooperation with other organizations, which operate and manage constituent systems of the IoT system, is necessary to achieve IoT trustworthiness. IoT trustworthiness is considered to be achieved if all the requirements of IoT trustworthiness are satisfied because IoT trustworthiness depends on each system. For details of IoT systems, a lot of examples are provided in ISO/IEC TR 22417:2017[8].

This document is targeted at users who are responsible for implementation and maintenance of IoT trustworthiness. When there is no entity responsible for the whole IoT system or service, this document applies to each constituent system or service for which there is an entity responsible regardless of whether it consists of multiple subsystems, part(s) of which may be operated and managed by another entity or entities.

---

1 Numbers in square brackets refer to the Bibliography.