

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



ISO/IEC 30147

Edition 1.0 2021-02

PRE-RELEASE VERSION (FDIS)

**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

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



JTC1-SC41/210/FDIS

FINAL DRAFT INTERNATIONAL STANDARD (FDIS)

PROJECT NUMBER:

ISO/IEC 30147 ED1

DATE OF CIRCULATION:

2021-02-19

CLOSING DATE FOR VOTING:

2021-04-16

SUPERSEDES DOCUMENTS:

JTC1-SC41/162/CDV, JTC1-SC41/202/RVC

IEC ISO/IEC JTC 1/SC 41 : INTERNET OF THINGS AND DIGITAL TWIN

SECRETARIAT:

Korea, Republic of

SECRETARY:

Ms Jooran Lee

OF INTEREST TO THE FOLLOWING COMMITTEES:

HORIZONTAL STANDARD:

FUNCTIONS CONCERNED:

EMC

ENVIRONMENT

QUALITY ASSURANCE

SAFETY

SUBMITTED FOR CENELEC PARALLEL VOTING

NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is a draft distributed for approval. It may not be referred to as an International Standard until published as such.

In addition to their evaluation as being acceptable for industrial, technological, commercial and user purposes, Final Draft International Standards may on occasion have to be considered in the light of their potential to become standards to which reference may be made in national regulations.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

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

PROPOSED STABILITY DATE: 2026

NOTE FROM TC/SC OFFICERS:

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.....	28
B.1 Overview of approach toward process for IoT trustworthiness	28
B.2 Application of process to enhance IoT trustworthiness	30
Bibliography.....	31
Figure 1 – An IoT system, a system of systems	10
Table B.1 – Relations between typical characteristics of IoT systems and process bases.....	30

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:

Draft	Report on voting
JTC1-SC41/XX/FDIS	JTC1-SC41/XX/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*