# ISO/IEC TS 30149

Edition 1.0 2024-05

# TECHNICAL SPECIFICATION

## Internet of Things (IoT) – Trustworthiness principles

ISO/IEC TS 30149:2024-05(en)

Documents
Document Sharing Hub

Full document details: ISO IEC TS 30149-2024

**THIS PUBLICATION IS COPYRIGHT PROTECTED**
**Copyright © 2024 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 Secretariat
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 It also gives information on projects, replaced and withdrawn publications.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 Products & Services Portal - products.iec.ch**
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. 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 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

Documents
Document Sharing Hub

Full document details: ISO IEC TS 30149-2024

# ISO/IEC TS 30149

Edition 1.0 2024-05

# TECHNICAL SPECIFICATION

## Internet of Things (IoT) – Trustworthiness principles

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.020; 35.030

ISBN 978-2-8322-8406-3

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

Documents
Document Sharing Hub

Full document details: ISO IEC TS 30149-2024

CONTENTS

FOREWORD ..... 4
INTRODUCTION ..... 5
1 Scope ..... 6
2 Normative references ..... 6
3 Terms and definitions ..... 6
4 Abbreviated terms ..... 7
5 Concept of trustworthiness ..... 7
5.1 Relation to trust ..... 7
5.2 Relation to context ..... 8
5.3 Relation to characteristics, behaviour, assurance and confidence ..... 9
6 Characteristics ..... 9
6.1 Safety ..... 9
6.1.1 General ..... 9
6.1.2 Safety goals ..... 10
6.1.3 Safety design ..... 10
6.1.4 Safety assurance and control ..... 10
6.2 Security ..... 10
6.2.1 General ..... 10
6.2.2 Security goals ..... 10
6.2.3 Security assumptions ..... 11
6.2.4 Security design ..... 12
6.2.5 Security assurance and control ..... 12
6.3 Privacy ..... 12
6.3.1 Overview ..... 12
6.3.2 Privacy goals ..... 13
6.3.3 Privacy assumptions ..... 14
6.3.4 Privacy design ..... 14
6.3.5 Privacy assurance and control ..... 15
6.4 Resilience ..... 15
6.5 Reliability ..... 16
7 Managing trustworthiness ..... 16
7.1 General ..... 16
7.2 Assumptions ..... 17
7.3 Assurance ..... 17
7.4 Risks ..... 18
7.5 Composition ..... 18
7.6 Trustworthiness profiles ..... 19
8 Building trustworthiness ..... 19
8.1 General ..... 19
8.2 Capability viewpoint ..... 19
8.3 Risk viewpoint ..... 20
8.4 Assurance viewpoint ..... 21
8.5 Operationalization ..... 21
Annex A (informative) Best practices for IoT trustworthiness ..... 25
A.1 Relation with ISO/IEC 30141 ..... 25
A.2 Concerns ..... 25

AVA Documents
Document Sharing Hub
Full document details: ISO IEC TS 30149-2024

A.3 Patterns ..... 26
A.3.1 General ..... 26
A.3.2 Trustworthiness characterization method pattern ..... 27
A.3.3 Trustworthiness maturity model pattern ..... 28
A.3.4 Trustworthiness impact assessment pattern ..... 28
A.3.5 Trustworthiness engineering pattern ..... 30
A.3.6 Trustworthiness assurance pattern ..... 32
Bibliography ..... 33

Figure 1 – Relationship between ISO/IEC TS 30149 and ISO/IEC 30141 ..... 5
Figure 2 – Trustworthiness and trust ..... 8
Figure 3 – Concepts of characteristics, behaviour, assurance and confidence ..... 9
Figure 4 – Relationship between security and privacy ..... 13
Figure 5 – Trustworthiness characteristics examples ..... 16
Figure 6 – Goal oriented trustworthiness ..... 20
Figure 7 – Risk oriented trustworthiness ..... 21
Figure 8 – Assurance based on claims, arguments, and evidence ..... 21
Figure 9 – Conceptual model for trustworthiness ..... 22
Figure 10 – Determining risk factors within an RA ..... 23

Table 1 – Example of goals and properties ..... 20
Table 2 – Principles for trustworthiness operationalization ..... 22
Table A.1 – Concerns for an implementation architecture ..... 25
Table A.2 – Trustworthiness characterization pattern ..... 27
Table A.3 – Trustworthiness maturity model pattern ..... 28
Table A.4 – Trustworthiness impact assessment pattern ..... 28
Table A.5 – Trustworthiness engineering pattern ..... 30
Table A.6 – Trustworthiness assurance pattern ..... 32

Documents
Document Sharing Hub

Full document details: ISO IEC TS 30149-2024

# INTERNET OF THINGS (IoT) – TRUSTWORTHINESS PRINCIPLES

## 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) IEC and ISO draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC and ISO take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC and ISO had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch and www.iso.org/patents. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 30149 has been prepared by subcommittee 41: Internet of Things and Digital Twin, of ISO/IEC joint technical committee 1: Information technology. It is a Technical Specification.

The text of this Technical Specification is based on the following documents:

| Draft | Report on voting |
|---|---|
| JTC1-SC41/390/DTS | JTC1-SC41/412/RVDTS |

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 Technical Specification is English.

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

Documents
Document Sharing Hub

Full document details: ISO IEC TS 30149-2024

# INTRODUCTION

With the complexity of many Internet of Things (IoT) solutions today, understanding the inherent risks of these products and solutions can be difficult without the correct context or technical understanding of the solution. Trust is a concept to ensure that all relevant stakeholders understand the specific trust elements of a solution and any potential risks to their given use case.

As potential vulnerabilities and attacks increase in complexity, they are only one aspect of the risk at hand. Design, components, and development techniques are some of the elements that can be considered during the creation, building and deployment of an IoT solution. Ensuring trust elements are identified at each stage of development for each component while considering all relevant stakeholders will provide a means to demonstrate a level of trustworthiness.

Leveraging the system architecture-based approach to ensure alignment to products and services used in ISO/IEC 30141:–[1][1] will allow all stakeholders to implement trustworthiness for products and solutions.

Figure 1 shows the relationship with ISO/IEC 30141.

– This document specializes the trustworthiness view of the IoT reference architecture.
– This document lists in Annex A a number of patterns that can be used in the construction view of the IoT reference architecture.

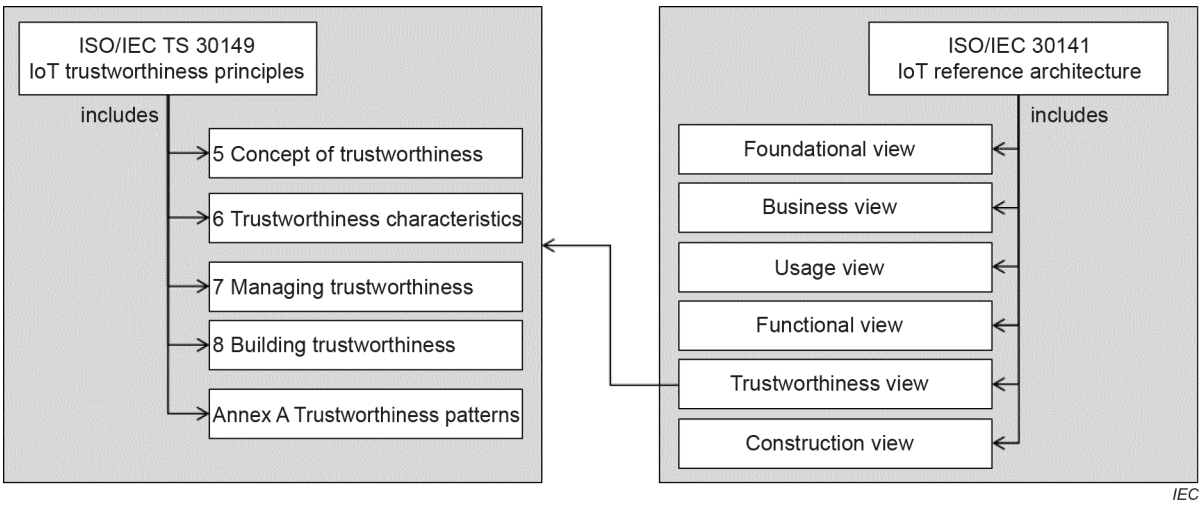


**Figure 1 – Relationship between ISO/IEC TS 30149 and ISO/IEC 30141**

[1] Numbers in square brackets refer to the Bibliography.

Documents
Document Sharing Hub
Full document details: ISO IEC TS 30149-2024

# INTERNET OF THINGS (IoT) – TRUSTWORTHINESS PRINCIPLES

## 1 Scope

This document provides elements of IoT trustworthiness based on the IoT reference architecture specified in ISO/IEC 30141.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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**
**assurance**
grounds for justified confidence that a claim has been or will be achieved

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.1]

**3.2**
**composability**
ability to assemble components logically and physically (without need for adaptation of the components or additional interfacing work)

Note 1 to entry: While ‘integration’ generally implies significant effort, ‘composition’ generally implies limited to no effort

EXAMPLE composition of a hardware security component and a data storage component to create a secure data storage component

[SOURCE: ISO 22166-1:2021, 3.3.1, modified – In the definition, "modules" has been replaced by "components" and "using various combinations into new modules" has been deleted from the end of the definition. Note 1 to entry and the example have been added.]

Documents
Document Sharing Hub

Full document details: ISO IEC TS 30149-2024

**3.3**
**trustworthiness**
ability to meet stakeholders' expectations in a verifiable way

Note 1 to entry: Depending on the context or sector, and also on the specific product or service, data, technology and process used, different characteristics apply and need verification to ensure stakeholders' expectations are met.

Note 2 to entry: Characteristics of trustworthiness include, for instance, accountability, accuracy, authenticity, availability, controllability, integrity, privacy, quality, reliability, resilience, robustness, safety, security, transparency and usability.

Note 3 to entry: Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as to organizations.

Note 4 to entry: Verifiability includes measurability and demonstrability by means of objective evidence.

[SOURCE: ISO/IEC TS 5723:2022, 3.1.1]

**3.4**
**claim**
proposition representing a requirement of the IoT system that enables the IoT system to achieve tolerable risk if it were met

[SOURCE: ISO/IEC 15026-3:2015, 3.2, modified – In the definition, "system-of-interest" has been replaced by "IoT system". Notes 1 and 2 to entry have been deleted.]

**3.5**
**ecosystem**
infrastructure and services based on a network of organizations and stakeholders

[SOURCE: ISO/IEC TS 27570:2021, 3.8, modified – Note 1 to entry has been deleted.]

**3.6**
**IoT system assumption**
condition concerning an IoT system that is accepted as true without proof of demonstration

**3.7**
**trust**
degree to which a user or other stakeholder has confidence that a product or system will behave as intended

[SOURCE: ISO/IEC 25010:2011, 4.1.3.2]

## 4 Abbreviated terms

IoT Internet of Things

PII personally identifiable information

RA reference architecture

## 5 Concept of trustworthiness

### 5.1 Relation to trust

Figure 2 depicts the relation between trustworthiness (3.3) and trust (3.7):

– a supplier provides an IoT system which includes trustworthiness, expressed through evidence; and

– evidence is evaluated to judge trust, based on criteria on trust.

Documents
Document Sharing Hub

Full document details: ISO IEC TS 30149-2024

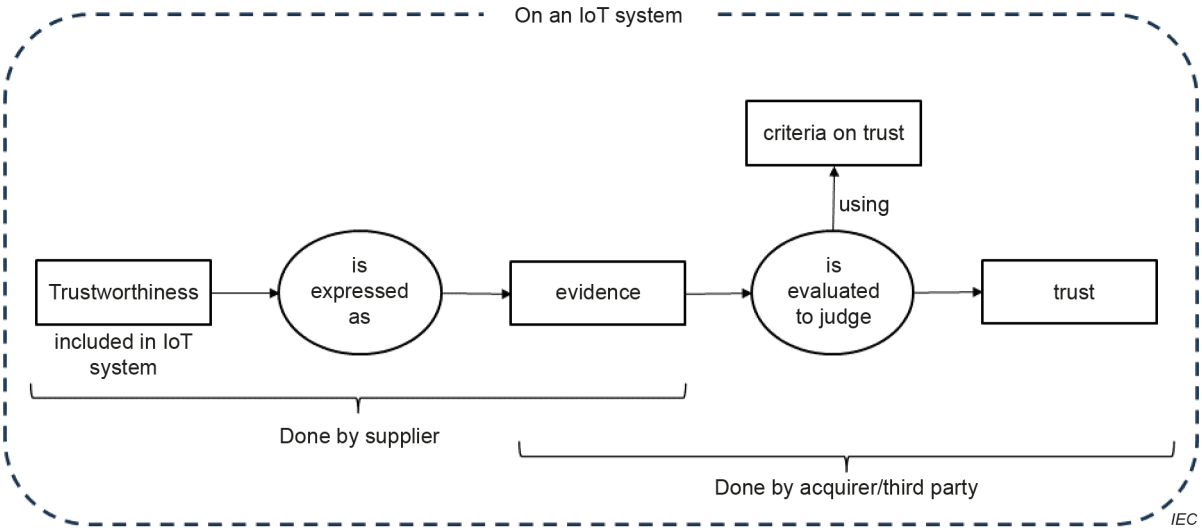


**Figure 2 – Trustworthiness and trust**

Trustworthiness is dependent on an IoT system reference architecture and its characteristics. Requirements to be verified are derived from the RA characteristics. Some requirements will be derived as a result of a risk management system in order to mitigate risks in the IoT system. Trustworthiness is then determined on the level of assurance as a result of the verification of the derived requirements. As such, trustworthiness is a deterministic characteristic of the IoT system based on verifiable evidence.

Trust is based on assumptions the user or stakeholder makes about the IoT system based on their past experience with the supplier, access to the verification evidence, or claims made by the supplier regarding the IoT system. Trust can extend to the entire IoT system or individually to each of the IoT system components.

NOTE ISO/IEC 15026-3:2015 [2] provides more information on establishing levels of trust.

## 5.2 Relation to context

Trust is the "acceptable dependence" related to the system in the context of the system use.

EXAMPLE 1 Smart traffic lights require safety of traffic regulation, authorized access for local and remote control and maintenance, resilience to weather conditions and vandal-proof implementation and deployment.

EXAMPLE 2 Online shopping for the customer requires a secure payment system. reliable delivery, and accurate shopping cart calculations (e.g. applying discounts, recalculating total when removing items from the cart, etc.).

EXAMPLE 3 Medical record systems require accuracy, security, and backup mechanisms.

Trustworthiness is validated evidence that the requirements of the system are met at a point of time.

NOTE Trustworthiness can be subjective as the criteria often depend on who set them for the system.

Documents
Document Sharing Hub
Full document details: ISO IEC TS 30149-2024

### 5.3 Relation to characteristics, behaviour, assurance and confidence

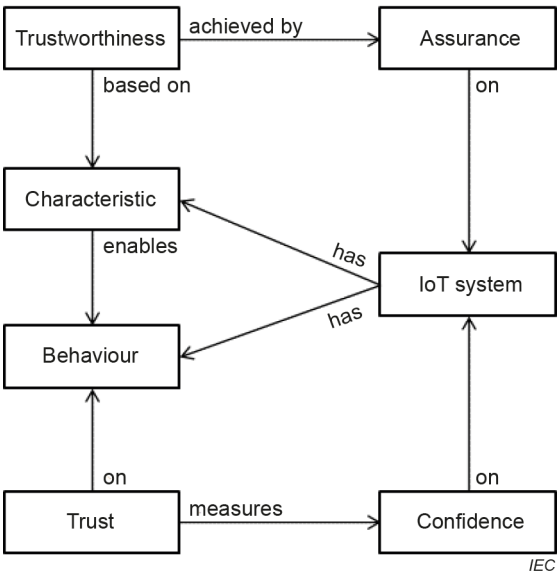


**Figure 3 – Concepts of characteristics, behaviour, assurance and confidence**

Figure 3 provides a conceptual viewpoint for trustworthiness, focusing on the relation to characteristics, behaviour, assurance and confidence:

– trustworthiness is associated with an entity of interest;

EXAMPLE Machine learning systems, autonomous systems, genomic processing systems are entities of interest.

NOTE The term "entity of interest" is defined in ISO/IEC/IEEE 42010 [3] as a generalization of the term "system of interest".

– trustworthiness is based on characteristics (e.g. safety, security) of an entity of interest;
– trustworthiness is verified by assurance on an entity of interest;
– characteristics enable the behaviour of an entity of interest; and
– trust measures confidence on an entity of interest.

## 6 Characteristics

### 6.1 Safety

#### 6.1.1 General

Some trustworthiness characteristics can be described through generic program properties, which are attributes of a program that is true for every possible execution of that program.

The safety generic program property asserts that nothing bad happens during execution, i.e. the program does not reach a bad state.

The liveness generic program property asserts that something good eventually happens, i.e. the program will eventually reach a good state.

Each safety objective can be described through safety generic program properties.

More descriptive details can be found in the IEC 61508 series [4] and the IEC 61511 series [5]. These should be referenced if the RA has safety characteristics that need to be considered. In some sectors, these aspects are mandatory and will have regulatory implications.

Documents
Document Sharing Hub
Full document details: ISO IEC TS 30149-2024

Safety is related to trustworthiness as follows:

– Safety is determined by a set of objectives. More descriptive details can be found in the IEC 61508 series [4] and the IEC 61511 series [5].
– Damage to the system itself can be included as damage to property or persons or not considered as a part of safety.
– Safety covers non-intentional system failures and negligence, not intentional behaviour.

### 6.1.2 Safety goals

Safety is determined through the set of safety goals. For the certification purposes these goals are very concrete.

### 6.1.3 Safety design

By design, a predictive analysis model for the IoT system shall be established to analyse the data of IoT devices and to perform the visual operations based on the predictive model. Meanwhile, the behaviour patterns of device failures are learned and predicted, and then the optimized solutions or improved design are provided.

### 6.1.4 Safety assurance and control

Assurance of safety goals endeavours to eliminate both systematic and probabilistic failures. Traditional operational technology (OT) safety-assessment techniques focus on physical items and processes, then combine empirically derived component failure probabilities into total system risk. Risk analysis to identify hazards intends to prevent faulty operations and improve system resilience to unexpected events.

## 6.2 Security

### 6.2.1 General

Security in the context of trustworthiness is the assurance that a security measure is effective relative to an actual or perceived threat. A threat can be either intentional or unintentional. An intentional attack can involve targeting IoT to stage an attack by an adversary. An unintentional attack can involve a worm that proliferates and infects IoT and non-IoT systems beyond its intended target. The adversary is as important as mitigating unintentional attacks through basic security fundamentals.

NOTE A threat model is the main artefact from risk assessment. It will lead to the development of countermeasures for identified threats.

More information about specific security aspects can be found in the IEC 62443 series [6], ISO/IEC 27400 [7], and ISO/IEC 27402 [8].

### 6.2.2 Security goals

Security objectives say what security controls exist for the particular solution (device, component, etc.). Identification of the security objectives, which are very high-level security requirements, is a crucial step towards the description of relevant threats for the particular system or solution. CIA (confidentiality, integrity, and availability) triad is the simplest example of security objectives for general informational resources. Other characteristics of trustworthiness can also represent the general security objectives, including safety, resources integrity, fail-safety, privacy, attack resilience, etc. These factors will depend solely on the proposed or implemented RA.

Documents
Document Sharing Hub
Full document details: ISO IEC TS 30149-2024