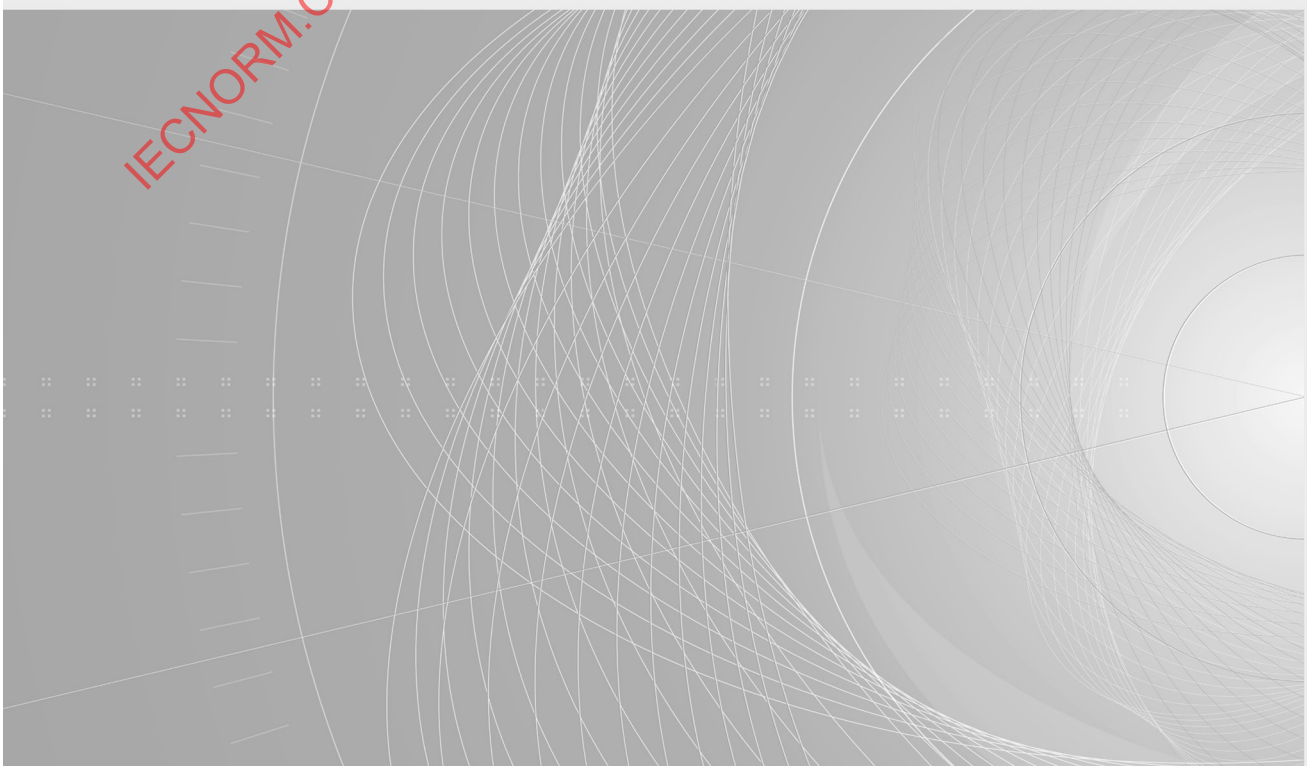
ISO/IEC TS 30149

Edition 1.0 2024-05

TECHNICAL SPECIFICATION

Internet of Things (IoT) – Trustworthiness principles



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

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 It also gives information on projects, replaced and withdrawn publications.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.

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

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

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

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.

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.

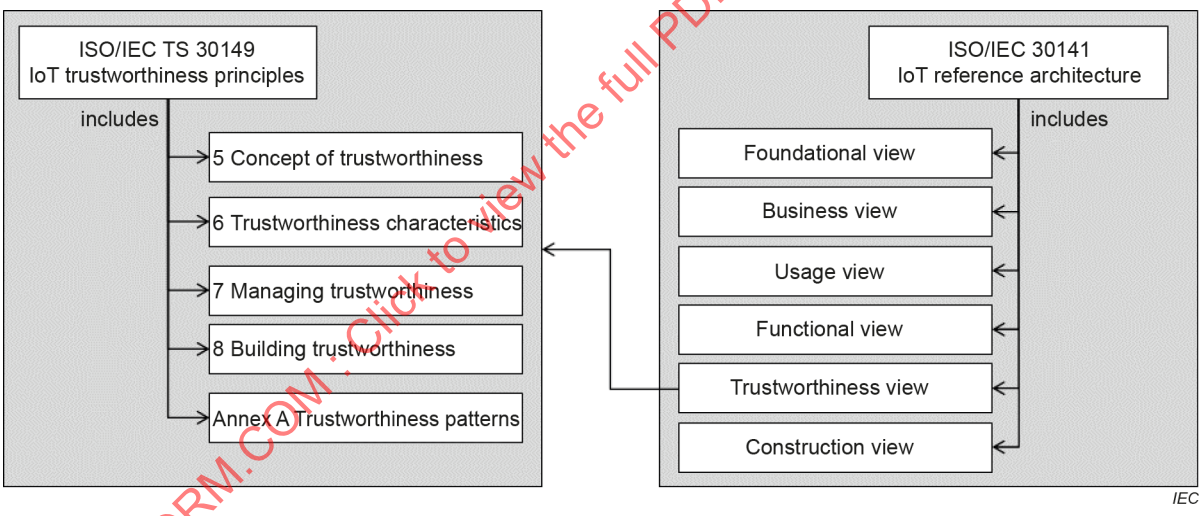


Figure 1 – Relationship between ISO/IEC TS 30149 and ISO/IEC 30141

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

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.]

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.

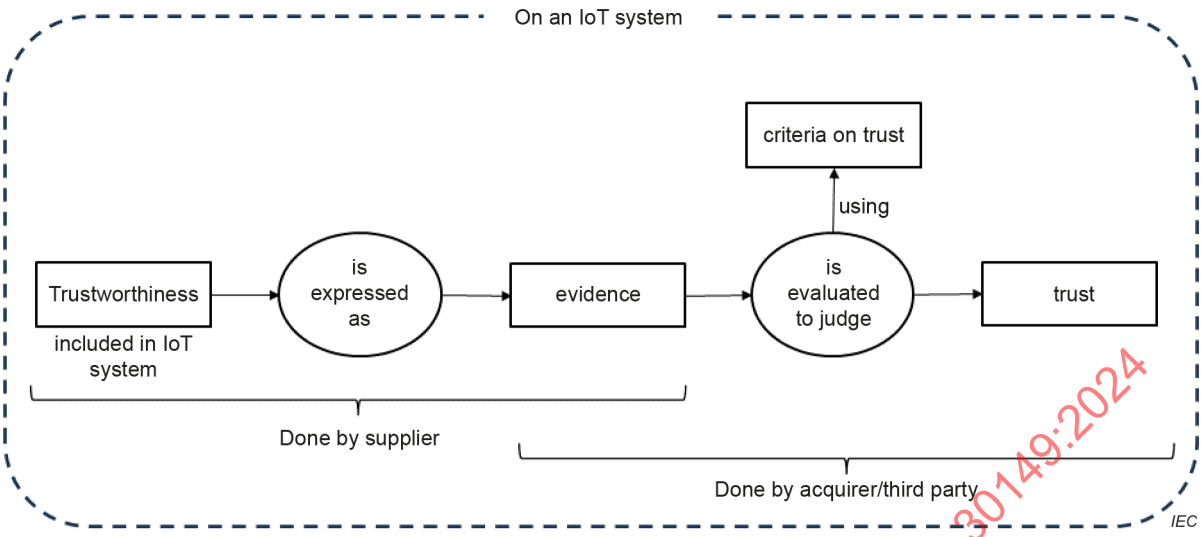


Figure 2 – Trustworthiness and trust

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.

5.3 Relation to characteristics, behaviour, assurance and confidence

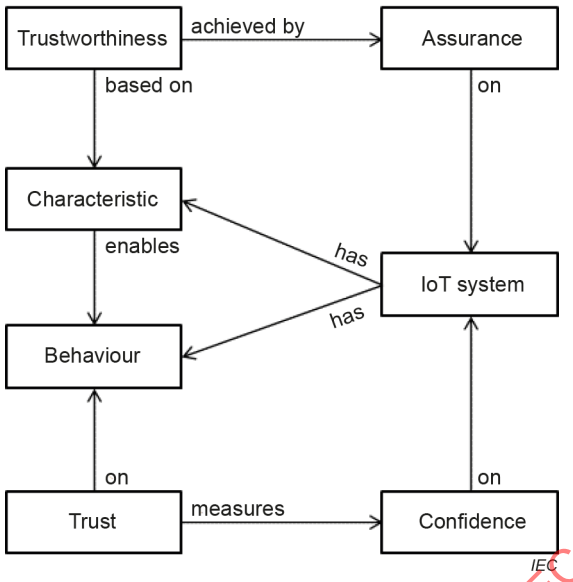


Figure 3 – Concepts of characteristics, behaviour, assurance and confidence

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.

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.

The distinctive characteristics of security objectives are the following:

– A security objective that is in scope should not change as the system evolves and changes within the boundaries described by the system specification.
– Security objectives of a subsystem can relate to the whole system. This means that the impact of the objective violation has the potential to spread across the whole system, not only its separate part.
– A security objective describes how the system behaves or how characteristics can change rather than how it does not behave or whether the characteristics cannot change.

The level of abstraction can vary from the generic reference to desirable behaviour of the system like "resilience to attacks" to the very concrete. For the system more concrete security objectives can be set. These security objectives usually reflect the system purpose and scenarios of its intended use. Examples are:

– maintaining privacy while working online;
– component security tolerance to reverse engineering;
– authenticity of the system software updates;
– authentication of the message source;
– authorization based on default-deny principle;
– safe execution of the security controls.

It is highly desirable to organize the process of identification of security objectives with involvement of system stakeholders (owners, users) and third-party OT experts and IT experts, led by security specialists.

Every security objective can be represented through a separate safety generic program property so they can be combined using the logical AND operation. Violation of each separate objective leads to the violation of the security of the system.

The statement of a security objective should be defined through positive statements.

EXAMPLE 1 "No data leak should happen during data transfer" is a negative statement variant.

EXAMPLE 2 "Data remains available only to authorized subjects" is a clearer variant. The last variant is clearer which can be operationalized into set of requirements.

6.2.3 Security assumptions

Security assumptions establish the base for the security of the system. All assumptions should be based on risks that have been identified as part of software development or similar lifecycle management approach. In some instances, it is not possible to make provision for protection against all potential threats: for example, in a case of compromised hardware, even the trustworthy software can be incapable of guaranteeing the required security level.

The clear definition of security assumptions contributes to determining the level of confidence in the security and helps to identify trusted (but not necessarily trustworthy) objects and processes.

For a threat model, definition of the security assumptions means that the appropriate threats are not considered in the scope of this model. Examples of security assumptions are:

– the hardware does not contain any undocumented features;
– trusted anchor (e.g. X.509 certificate) for the crypto mechanisms is trustworthy.

The general recommendation is the minimization of the impact of security assumptions.

6.2.4 Security design

Security by design is the concept of applying the methods of software development to minimize the security risks early in the design process and during the system implementation. This approach demonstrates the strong connection with a participative (stakeholder based) approach and relies on the threat model as the main artefact for elaborating the "secure by design system".

For the IoT system, the security for sensing the physical space is an essential issue to realize the IoT security, which is the base and core for the security design of the IoT system.

As deployment environments of IoT application systems are different and bring potential security risks, the impact of the surrounding environment on the security of IoT devices shall be considered by design, so appropriate security measures are adopted to reduce such risks.

6.2.5 Security assurance and control

As the excessively optimistic assumptions and human factor in software development and use pose additional risk on the system, even when developed according to "security by design" principles, the assurance for security is still required.

The assurance (and control) methods on security include but are not limited to:

– The responsible parties (person or organization) of each IoT subsystem should formulate and obey the security strategies for system operating.
– The security responsibility and conduct criterion for the responsible party of each IoT subsystem are clarified.
– The emergency response plan and policy are formulated to prevent the assurance of element being invalid.

Regular security assessments should be carried out for the assurance of the elements.

6.3 Privacy

6.3.1 Overview

Privacy is framed in ISO/IEC 29100:2011 [9]. It focuses on

– PII principals who provide their PII for processing to PII controllers and PII processors and, when it is not otherwise provided by applicable law, they give consent and determine their privacy preferences for how their PII should be processed;

NOTE ISO/IEC 29184:2020 [10], ISO/IEC TS 27560:2023 [11], and ISO/IEC 27556:2022 [12] provide further guidance on consent and privacy preferences

– PII controllers who determine why (purpose) and how (means) the processing of PII takes place, ensure adherence to the privacy principles of ISO/IEC 29100:2011 [9]; and
– PII processors who carry the processing of PII on behalf of a PII controller.

The privacy principles to adhere to are the following:

– consent and choice;
– purpose legitimacy and specification;
– collection limitation;
– data minimization;
– use, retention and disclosure limitation;
– accuracy and quality;
– openness, transparency, and notice;

– individual participation and access;
– accountability;
– information security;
– privacy compliance.

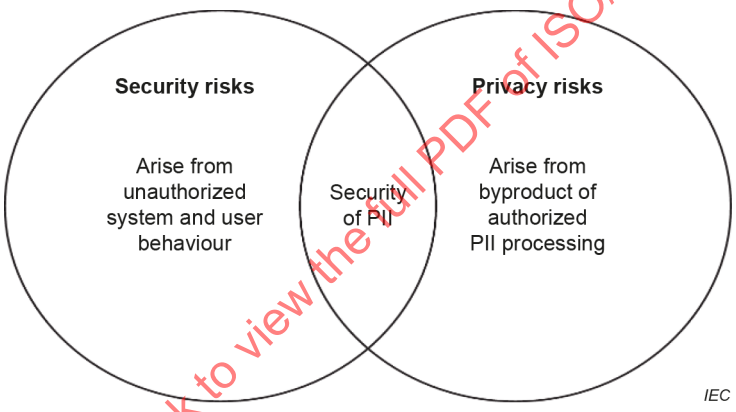
The nature of the privacy property is the following: privacy is a goal that depends on the PII principal and on the context.

EXAMPLE A picture at home can be shared within the family community but not externally.

Privacy can be defined by its nature [13] or by its harm [14]. Privacy is enforced through privacy management capability such as consent and privacy preference management through privacy controls resulting from a privacy risk assessment.

6.3.2 Privacy goals

From the system perspective, privacy is a prominent issue for IoT. IoT acquires real and real-time information of the physical objects, and the data are sensitive and private. As privacy can be interpreted as an aspect of security, Figure 4 illustrates how these two concepts interplay and differ.



SOURCE: Figure 2 of NISTIR 8062 [15]. Reproduced with permission of the US National Institute of Standards and Technology.

Figure 4 – Relationship between security and privacy

The role of privacy objectives is to ensure that developed systems provide capabilities for privacy protection. Privacy objectives and their relations with respect to security are shown in Figure 4 (see ISO/IEC TR 27550:2019 [16]):

– security risks arise from unauthorized system and user behaviour,
– privacy risks arise as a by-product of authorized PII processing, and
– some security risks are also privacy risks, for instance a lack of security of collected PII (e.g. health data, location data, etc.).

The following privacy protection goals are used.

– Unlinkability: it ensures that a PII principal can make multiple uses of resources or services without others being able to link these uses together. The objective is to minimize the risk to privacy created by the potential linking of separate sets of PII.
– Transparency: it ensures that an adequate level of clarity of the processes in privacy-relevant data processing is reached so that the processing of the information can be understood and reconstructed at any time. The objective is to allow involved parties (e.g. PII principals, PII controllers and PII processors) to know the risks to privacy (e.g. the processing of health data or location data) and have sufficient information on countermeasures, how to employ them and what limitations they have.
– Intervenability: it ensures that PII principals, PII controllers, PII processors and supervisory authorities can intervene in all privacy-relevant data processing.

NOTE There can be legislative or regulatory limitations on the extent to which a PII principal or supervisory authority can intervene in data processing.

6.3.3 Privacy assumptions

Assumptions are the following:

– availability of evidence on the application of ISO/IEC 29100 principles;
– availability of capabilities to enforce privacy policies;
– availability of a process to audit privacy controls.

6.3.4 Privacy design

The role and approaches to implementing privacy-by-design are the following:

– integration in the system lifecycle process, and
– integration in the ICT ecosystem.

Privacy integration in the system lifecycle process requires the integration of the goal-oriented activities and the risk-oriented activities:

– in the goal-oriented activities, each privacy principle is considered as a high-level concern that the system needs to fulfil. Each principle is then decomposed into a set of specific goals to meet the concern. Privacy control requirements are then identified to address the specific goals; and
– in the risk-oriented activities, the focus is on the identification of the threats to and vulnerabilities of the PII assets in the system, and the identification of the risks associated with PII processing that can compromise compliance with the privacy principles.

NOTE 1 ISO/IEC 27561 [17] provides guidance on the operationalization of privacy principles.

NOTE 2 ISO/IEC/IEEE 15288:2023 [18] provides guidance on system lifecycle processes.

NOTE 3 ISO/IEC TR 27550:2019 [16] provides guidance on the engineering of privacy.

NOTE 4 ISO 31700-1:2023 [19] lists requirements for the engineering of consumer goods and services.

Privacy integration requires collaboration between organizations in the ecosystem. ISO/IEC TS 27570 [20] describes five collaboration processes:

– governance process;
– risk management process;
– data management process;
– engineering process; and
– the citizen engagement process.

6.3.5 Privacy assurance and control

Privacy assurance requires

– demonstrating that processing meets data protection and privacy safeguarding requirements through periodic audits;

NOTE 1 In the case of information security, ISO/IEC 27701:2019 [21] and ISO/IEC TS 27006-2:2021 [22] can be used.

– having appropriate internal controls and independent supervision mechanisms to assure compliance with relevant privacy law and with their security, data protection and privacy policies and procedures; and

– developing and maintaining privacy risk assessments.

NOTE 2 ISO/IEC 29134:2017 [23] can be used.

The role of assurance and control for privacy is as follows: Privacy assurance focuses on verifying

– capabilities to meet the goals, and

– measures (controls) to treat the risks.

NOTE 3 ISO/IEC 27400 [7] provides a list of security and privacy controls for IoT systems.

It is important that both privacy controls and privacy assurance cover the case of ecosystems.

EXAMPLE 1 PII that is exchanged for data analytics within a smart city ecosystem can involve consent management and privacy preference management by many PII controllers or PII processors. The goal of having a functioning consent and privacy preference management involving the ecosystem can require a capability focusing on a collaborative consent and privacy preference management. Assurance on this collaboration capability is a requirement for trustworthiness.

EXAMPLE 2 PII that is exchanged for data analytics within a smart city ecosystem can involve many PII controllers or PII processors. The risk of having a privacy breach involving the ecosystem can require a privacy control focusing on collaborative incident management. Assurance on this collaboration measure is a requirement for trustworthiness.

Privacy assurance also covers IoT ecosystems or IoT system of systems, which consist of interacting individual systems which are independently managed and operated. This requires the provision of compliance schemes involving multiple organizations.

NOTE 4 ISO/IEC/IEEE 21839 [24] provides a definition of system of systems (SoS).

6.4 Resilience

Resilience is covered in ISO/IEC 9837-1:– [25]. Resilience is the element of a system that behaves in a manner to avoid, absorb and manage dynamic adversarial conditions while completing the assigned missions, and to reconstitute the operational capabilities after causalities:

– resilience expects system failure or unstable functioning due to some reason and provides support for recovery and continuous execution;

– resilience covers both intentional attacks and non-intentional system failures; and

– resilience addresses the uncertainty about expected system behaviour through redundancy, e.g. alternative functionality, implementations, configurations, locations or network segments that can have different weaknesses so the same threats and hazards are not as disruptive to the replacement capabilities.

Resilience is a generic "liveness property" as it implies the commitment to bring out the behaviour supporting the system mission under adversarial conditions.

6.5 Reliability

Reliability is covered in ISO/IEC 25010 [26]. Reliability can be characterized by the following aspects:

– a well-defined set of conditions under which the system is tested to demonstrate that the functions perform for a specified period of time;
– a constrained set of functions to which reliability requirements apply;
– a practically guaranteed period of time during which the functions from this set reliably perform; and
– usually reliability covers non-intentional system failures.

The factors affecting the reliability of IoT system are divided into external factors and internal factors. External factors include working environment, installation location and position, human operation, electromagnetic environment, packaging conditions, etc. Internal factors include system management, equipment quality, network structure, business requirements, mechanism strategies, etc.

7 Managing trustworthiness

7.1 General

An aggregation of characteristics is expected (see Figure 5), e.g. safety, security, privacy, resilience, reliability, governability. The list of characteristics depends on stakeholders concerns and on the environment.

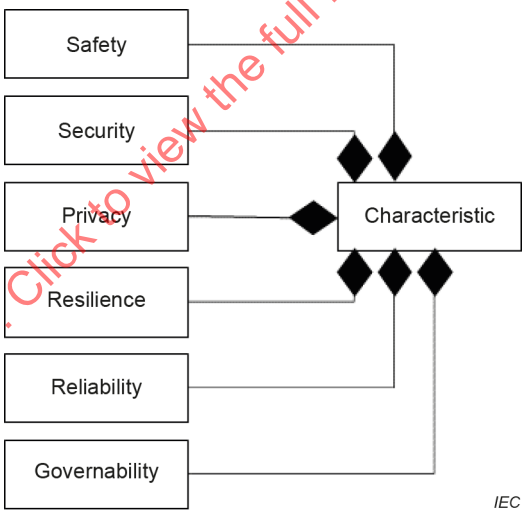


Figure 5 – Trustworthiness characteristics examples

Trustworthiness aspects are described in this document as system characteristics – or properties as they do not just manifest as specific functions. Trustworthiness of an entire system can be seen as a set of emergent characteristics derived from the trustworthiness of its sub-systems and from the overall architectural and functional design.

A system can exhibit these characteristics while operating.

Each characteristic can be associated with policies and regulation, with objectives, and with agreements (e.g. service level agreements (SLA) or service level objectives (SLO)), possibly involving contractual aspects. Such policies, objectives, agreements are in turn subject to measures, audits, and assurance procedures that involve metrics, key performance indicators (KPIs) and targets.

Even if components are considered trustworthy, the system can remain untrustworthy for two reasons:

– trustworthiness (the priorities of characteristics) is different for the system than for its separate components, and
– the way trustworthiness is achieved for some components can be not composable for other components.

7.2 Assumptions

Characteristics should be used to demonstrate how a target level of trust can be reached and maintained based on each characteristic and the given RA developed. These methods should be very specific to each characteristic and should enable the assessment of risks based on the use of a set of operational targets by each stakeholder.

The acceptance of the dependency between the identified risks and the set of assumptions is a measure of trust. An assumption that is wrong can lead to unjustified trust. Assumptions can involve different types of judgement:

– human factors (i.e. individual behaviour);
– operating environments;
– governance and business models;
– jurisdictions of operation;
– stakeholder reputation;
– awareness;
– intentions (good or bad);
– interest (absence or presence); or
– physical work constraints.

Assumptions can be objective or subjective.

EXAMPLE 1 Organization compliance is a subjective assumption.

EXAMPLE 2 Material yield strength physical property is an objective assumption.

7.3 Assurance

Assurance is based on evidence that risks are controlled to an acceptable degree. It can only be validated by using testing and evaluation techniques including risk assessments.

NOTE Risk assessment is based on evidence and not assumptions.

The following approaches can be used for assurance:

– Proving that system will always behave in a way that meets the criteria for trust over the given lifecycle of the product or solution. This can be accomplished by third party reviews, product documentation, design reviews, or other outputs of the development program.
– The following assurance approaches can be applied:
  - Providing a proof that the characteristic's objective is met.

    EXAMPLE 1 Probabilistic assessment.

    EXAMPLE 2 Formal specification and verification on model (model-checking).

- Testing if system can exhibit a behaviour that demonstrates that the characteristic's objective is not met.

  EXAMPLE 1 Testing and verification.

  EXAMPLE 2 Vulnerability assessment.

  EXAMPLE 3 RAM (reliability, availability and maintainability).

  These approaches can be provided as part of evaluations conducted both internal or external to the organization developing the solution.

- Analysis verification if a system can demonstrate behaviour that doesn't answer the criteria and reasoning that a target level is met or it wasn't possible. The following are examples of assurance methods.

  EXAMPLE 1 Testing and verification.

  EXAMPLE 2 Vulnerability assessment.

  EXAMPLE 3 Risk assessment.

– Decomposing the system into components, then applying the approaches mentioned above and justifying for the composition of components. As this is the combination of the approaches above, examples cover methodologies rather than separate methods. These methodologies can be bespoke for the concrete sets of security objectives, but some well-known methodologies also exist such as failure or fault analysis

7.4 Risks

Assurance claims depend on

– the correctness of assumptions, and

– the effectiveness of assurance methods.

Any uncertainty on assumptions and assurance method effectiveness create risk.

It can be noted that for every trustworthiness characteristic identified (e.g. security, safety) the risk can be defined differently. When talking about trustworthiness, the word "risk" should be used in conjunction with a concrete characteristic as this defines the interpretation of risk and determines the methods of risk assessment and further assurance on the separate trustworthiness characteristic.

7.5 Composition

System characteristics including security, safety, privacy, resilience, and reliability can be based on capabilities provided by individual components of the system. The process of ensuring that the resulting system is trustworthy is operationalized by the specification and validation of a trustworthiness composition model.

EXAMPLE 1 Trustworthiness of a gateway is enabled by the verification of an included hardware security module, both as an individual component and as part of the gateway.

The model should explain how assumptions, risks and operational behaviour are integrated.

There can be cases when no composition model is possible due to multiple different systems interconnecting and operated by different organizations. Due to defined lack of ownership or operational responsibility, it can lead to situation where operational aspects cannot be fully verified.

EXAMPLE 2 Composing a system with two components based on different levels of safety (one is fail-safe, the other is not) might not be possible.

For those systems which are already designed from components without any attention to composability from the trustworthiness perspective, the interaction between approaches to trustworthiness characteristics shall be assessed.

7.6 Trustworthiness profiles

There are models of security, safety and other characteristics which are widely known and adopted in several sectors. For example, "information security risk" is evaluated by "confidentiality, integrity and availability of the information". These models are useful but they are domain specific. They can be considered as specific trustworthiness profiles.

8 Building trustworthiness

8.1 General

Once trustworthiness objectives have been defined, they can be used as the basis to validate the overall implementation of the system. There are several ways to accomplish this:

– apply a goal-orientation approach by designing capabilities;
– apply a risk-orientation approach through a risk analysis and the identification of measures; and
– a combination.

The distinction between goal and risk is often of methodology or maturity origin:

– addressing a trustworthiness characteristic that is novel requires a risk-oriented approach, which involves the development of controls to treat identified risks;
– addressing a trustworthiness characteristic that has been treated in the past and is mature can sometimes involve a goal-oriented approach, which involves the development of capabilities to meet the goal.

EXAMPLE Privacy is a characteristic that has matured with the advent of regulatory frameworks such as GDPR. In the past, using PII without consent had to be considered as a risk. Since GDPR mandates consent management as an obligation, it now becomes a design goal.

8.2 Capability viewpoint

Figure 6 explains the relationship of trustworthiness with system goals:

– trustworthiness is based on the assurance that an IoT system has characteristics to enable the expected behaviour, based on capabilities that are included to achieve the goals of an IoT system;
– trust is about the confidence that an IoT system has the expected behaviour, based on assumptions that capabilities that are included to achieve the goals of IoT system are sufficient.

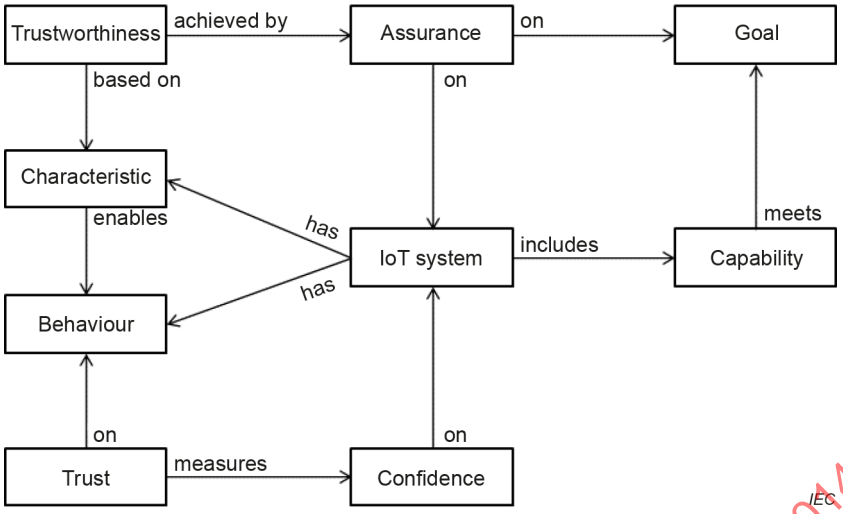


Figure 6 – Goal oriented trustworthiness

Table 1 shows examples of goals and capabilities that can be associated with characteristics.

NOTE Capabilities can be technical or organizational.

Table 1 – Example of goals and properties

Characteristic	Properties	Capabilities
Safety	Dependability, Liveness	Static redundancy, dynamic redundancy, system health monitoring
Security	Confidentiality, Integrity, Availability	Secure storage, Misbehaviour detection, hardware security module Identify, Protect, Detect, Respond, Recover [27]
Privacy	Unlinkability, Transparency, Intervenability, Compliance, Citizen empowerment,	Consent management [10], [11]; Privacy preference management [12] Identify-P, Govern-P, Control-P, Communicate-P, Protect-P [28] Operational capabilities: agreement, usage, validation, assurance, enforcement, security, interaction, access. See [17], [29]
Reliability	Function, Environment support, Durability, Performance	Predictive maintenance
Resilience	Asset manageability, Asset maintainability, Incident detectability, incident responsiveness, incident recoverability	Anticipation, withstanding, recovering, adapting [25], [30], [31]
Governability	Controllability, Manageability, Accountability, Policy enforceability, Usability of policy enforcement tools	Capabilities for evaluation, directing, monitoring [32] Example of monitoring capability: compliance dashboard See Cobit framework [33]

8.3 Risk viewpoint

A risk-oriented conceptual model of trustworthiness can be defined as well (Figure 7):

– an entity of interest includes controls to treat trustworthiness risks; and
– these controls treat risks related to trustworthiness.

EXAMPLE 1 Access management; application programming interface (API) sanitization for security; usage management for privacy.

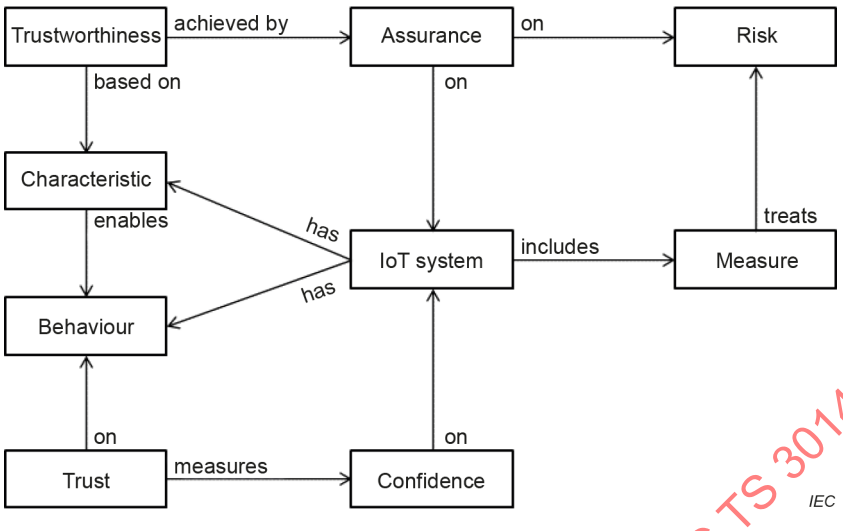


Figure 7 – Risk oriented trustworthiness

8.4 Assurance viewpoint

Assurance in the conceptual model can be defined as follows (Figure 8):

– in a goal-oriented model, assurance is achieved through claims based on arguments and evidence on a capability; and

– in a risk-oriented model, assurance is achieved through claims based on arguments and evidence on a measure.

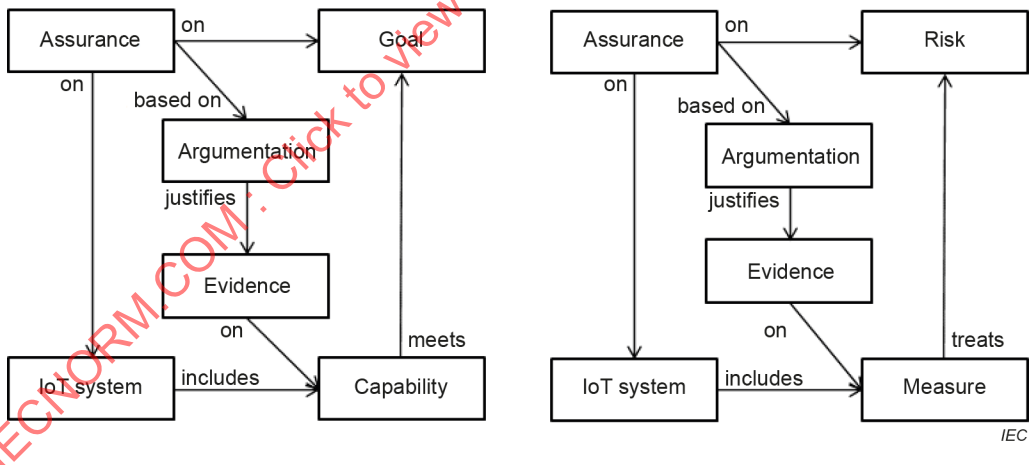


Figure 8 – Assurance based on claims, arguments, and evidence

8.5 Operationalization

A conceptual model for trustworthiness combining both the risk-oriented and goal-oriented views of trustworthiness can finally be defined (Figure 9).

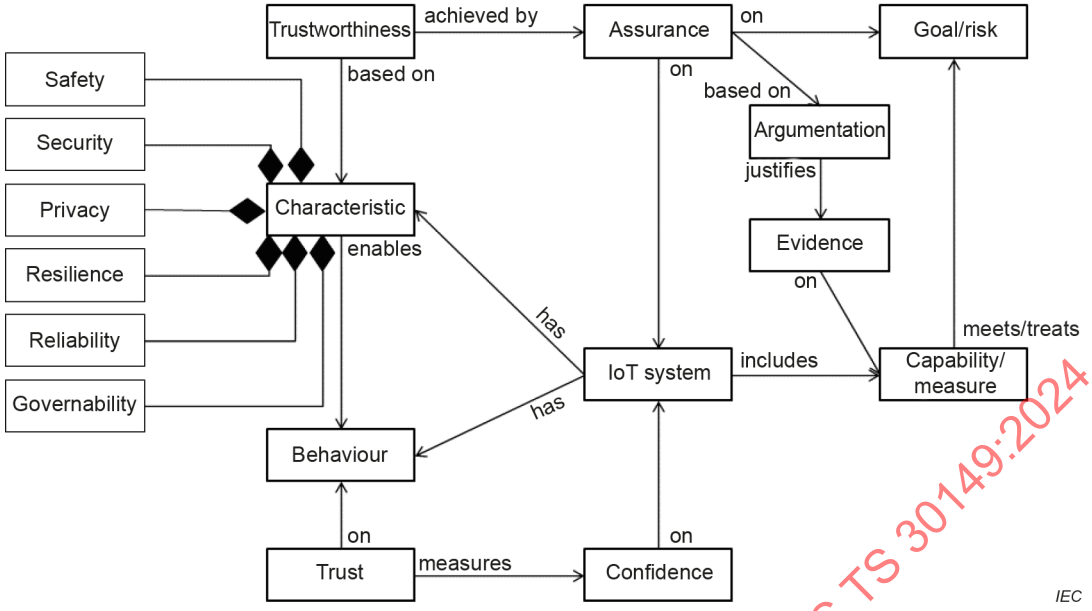


Figure 9 – Conceptual model for trustworthiness

NOTE From an overall conceptual model, statements such as "a control treats a trustworthiness risk" and "a capability meets a trustworthiness goal" can be used in parallel.

Operationalizing the conceptual model for trustworthiness involves the following activities:

– listing the characteristics and their dependencies;
– identifying goals and related capabilities;
– identifying risks and related treatments; and
– specifying assurance requirements in terms of claim, arguments and evidence.

Table 2 presents a list of principles for trustworthiness operationalization.

Table 2 – Principles for trustworthiness operationalization

Principle		Example
System and context	Relations that need trustworthiness depend on context	Hierarchical relations in public-key infrastructure (PKI)
	Dependencies between characteristics depend on context	Safety is a major concern in the automotive domain. Security analysis often focuses on its impact on safety. Privacy is a major concern in the health domain.
	Requirements on characteristics depend on context	In safety, fail-safe design could be required, i.e. the system's default behaviour keeps invariants even if new requirements are set for this system. In privacy, the minimization strategy could be required, i.e. data is not collected when possible.
	Context changes	The context of a system can change, new characteristics and new priorities can be introduced, as well as new methods.

Principle		Example
Process	Multi-stakeholder impact assessment	Determine risk factors of the system. This activity can include domain experts, safety, security and privacy experts, ethics experts.
	Multi-stakeholder architecture-based design	Participative (stakeholder-based) approach
	Independent assurance	Independent team, External organization
	Best practices including for composition	Established (standardized) protocols, procedures Examples of methods are rational (method-based) approach, normative (solution-based) approach, customized (attribute-based) approach.
	Continual improvement	Maturity of processes and practices increases over time. They are reflected in the processes of the company.
	Collaboration	Ecosystems require governance and collaboration

The operationalization of trustworthiness principles depends on the reference architecture that is used to build the system-of-interest. At an early stage of a project, such as design and concept, risk factors should be determined for a specific RA implementation. These are risk factors for each trustworthiness characteristic identified as an outcome to a proposed RA. These will serve as basis for the trustworthiness objectives.

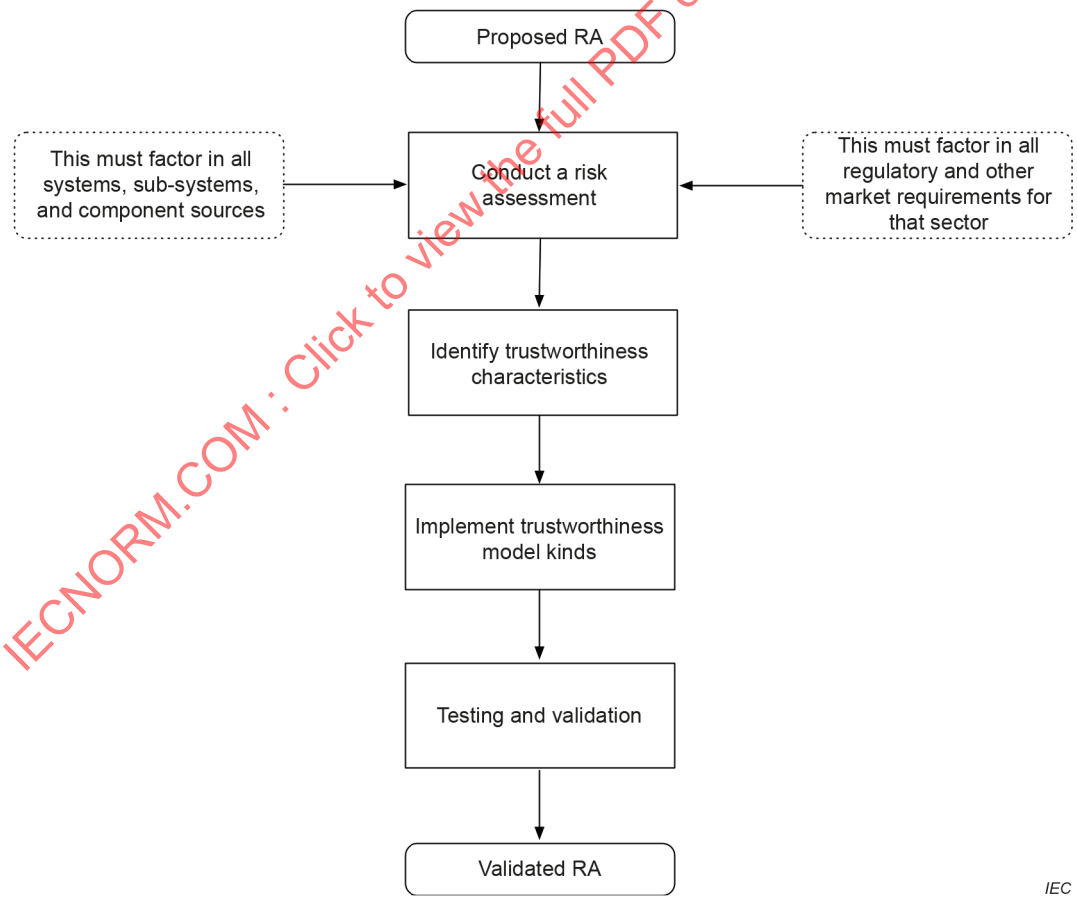


Figure 10 – Determining risk factors within an RA

Figure 10 describes the activities to determine risk factors. They are carried out in the context of the underlying reference architecture. These activities should not be an afterthought but part of a larger governance model within an organization. There should be ongoing processes and business practices that will allow for risk to be determined and mitigated by the vendor of these solutions. At a minimum a program should aim to complete the following.

– Conduct a risk assessment, factoring in all systems, sub-systems and components, regulatory and other market requirements.
– Identify and document characteristic's objectives.
– Implement trustworthiness capabilities, relying on suitable model kinds.
– Test and validate capabilities.

There are two aspects that all RAs should consider:

– all systems, subsystems, and component sources;
– all regulatory and other market factors where the target solution will be deployed.

The output of the "identify trustworthiness objectives" should include the following:

– definition of the characteristic objective;
– rationale on why the objective was identified;
– specification on how the objective can be verified.

The output of the "trustworthiness model kinds" should include the following:

– static models considered and how testing or evaluation results will result in any design modifications for the target RA;
– dynamic models considered and how testing or evaluation results will result in any design modifications for the target RA;
– interactive models considered and how testing or evaluation results will result in any design modifications for the target RA.

Testing and assessment should be conducted by both internal resources and validated as required by external third parties. This can include formal testing and evaluation that will lead to certification or other necessary assessments for a product within specific sectors in a market.

The details will be used to provide necessary assurance of the RA. This will include methods that were used for testing and validation for the products or services created as a result of this RA.

Annex A
(informative)

Best practices for IoT trustworthiness

A.1 Relation with ISO/IEC 30141

ISO/IEC 30141:– [1] addresses the following concerns for trustworthiness:

– how to build an implementation architecture with a level of confidence that meets trustworthiness goals;
– how to implement system assurance.

It specifies a trustworthiness view that covers

– concepts and relationship to IoT system assurance, and
– challenges with assuring IoT systems.

A.2 Concerns

Table A.1 lists the potential concerns in an IoT system architecture.

Table A.1 – Concerns for an implementation architecture

High level concern	Description	Detailed concerns
Characterization	What are the trustworthiness characteristics?	What are the risks of the concept of IoT? How can one evaluate and balance the cost of implementing a trusted and secure IoT system to benefit the market and users? How is trustworthiness implemented with minimal impact on system performance? How is trustworthiness implemented in compliance with regulations? How are the trustworthiness characteristics in an IoT system implementation determined? How can one assess the maturity of the trustworthiness model used in an IoT system implementation?
Impact	What is the impact of not addressing sufficiently a characteristic?	What impacts does trustworthiness of IoT components, IoT systems and IoT environment have on business and system ownership? How is or how was risk identified and quantified for each component in the IoT implementation? Was a secure development lifecycle used to determine that the appropriate test cases were used to validate the identified risks at design time? Was a risk determination performed at design time for the IoT implementation?
Measurement	What are the measurement means for trustworthiness?	How do you determine the level of trust for each component (system, software, or hardware) in the IoT implementation?

High level concern	Description	Detailed concerns
Capability	What are the capabilities to support a given trustworthiness characteristic?	How does the system of component provide safety? How does the system provide for authentication? How does the system provide for authorization? How does the system provide for privacy? How does the system provide for operational failure, including notifications? How does the system provide a means for detecting component and system operational state, failures and alerting?
Operation	What are the means to ensure trustworthiness during operation?	How does the system provide secure runtime operation? How are all components updated to ensure trust before and after the update? How would a potential compromise of a component be detected at runtime? How is trust ensured after a component is no longer supported or at the end of its service life? How is a component destroyed when not used or when it requires replacement? How are users or owners notified of a potential component breach? Including components provided by third parties?
Integration	What are the means for integration?	Does the test procedure verify every defined requirement? What third party access, components, and services are being used and how is each one prequalified to ensure operational trust?
Assurance	What are the means to verify trustworthiness?	What controls should be applied that will provide auditable means for validation for trust level? Is there an independent third party certification process (or self-certification regime)?

A.3 Patterns

A.3.1 General

The following patterns are defined in Clause A.3:

– trustworthiness characterization method;
– trustworthiness maturity model;
– trustworthiness impact assessment;
– trustworthiness engineering; and
– trustworthiness assurance.

A.3.2 Trustworthiness characterization method pattern

This pattern is described in Table A.2. It addresses the characterization concern of Table A.1.

Table A.2 – Trustworthiness characterization pattern

Information	Name	Trustworthiness characterization pattern
	Related patterns	–
Problem		It covers the following problems: – characteristics relationship, and – characteristics representation. As all IoT systems are different and the context of their use is different, the priorities of different trustworthiness aspects, their relevance to the system, the urgency of issues connected to them and approaches to risk mitigation will definitely vary. To reflect the particular priorities, approaches and rules, the characteristics relationship is dependent on the context policies.
Known Context	Specific context	
	Related context	
Solution	Architecture models	The characteristics relationship model kind covers the following expectation: specify the relationships between trustworthiness characteristics of the system-of-interest, and approaches to measure trustworthiness. It deals with so-called "-ilities". These include safety, security, privacy, reliability or resilience. These are non-functional requirements which set up the criteria for the solution, system, product, or environment according to the expectations about its functioning. The relationships allow for the understanding at the semantic level of the factors contributing to trust and their mutual influence. Thus, allowing for the prioritization of the aspects according to the industry or product constraints, regulations and other factors. The characteristics representation model kind covers the following expectation: specify the trustworthiness artefacts that are represented in the system-of-interest architecture.
	Examples	Example of characteristics relationship: trustworthiness in automotive system is constructed with safety (based on the ISO 26262 series) as the first characteristic. Security (based on ISO/SAE 21434) is then assessed according to the following criteria: safety, finance, operations, and privacy. Example of representation artefact: a trusted anchor can be used to provide specific security services (based on ISO/IEC TS 30168).
	Rationale for the pattern	The relationships depend on the context (specific document, or specific environment)
	Guidance	–

A.3.3 Trustworthiness maturity model pattern

This pattern is described in Table A.3. It addresses the characterization concern of Table A.1.

Table A.3 – Trustworthiness maturity model pattern

Information	Name	Trustworthiness maturity model pattern
	Related patterns	
Problem		The maturity model pattern covers the following expectation: Specify the system-of-interest maturity process.
Known Context	Specific context	
	Related context	
Solution	Architecture models[a]	Several models are possible: – OWASP Software Assurance Maturity Model (OWASP SAMM). – IIC IoT Security Maturity Model (IIC IoT SMM). – Capability Maturity Model Integration (CMMI®) – Automotive SPICE – Lockheed Martin Cyber Resilience Level® (CRL®) – Cyber Resilience Review methodology by the US Homeland Security – IEC 62740:2015, Root Cause Analysis (RCA)
	Examples	–
	Rationale for the pattern	
	Guidance	–

[a] Any trademarks that appear in this table are examples of suitable product(s) available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of these products.

A.3.4 Trustworthiness impact assessment pattern

This pattern is described in Table A.4. It addresses the impact and measurement concerns of Table A.1.

Table A.4 – Trustworthiness impact assessment pattern

Information	Name	Trustworthiness impact assessment pattern
	Related patterns	–
Problem		The impact assessment process covers the following expectation: specify the impact assessment process for trustworthiness of the system-of-interest. Business investment requires decisions that include trade-offs based on delivering functionality, addressing risks, ensuring business continuity, managing costs and reputation. The risks include security risks, safety risks, risks of non-compliance to privacy regulation, risks connected with unreliable systems behaviour. The choice or welfare correlation for the investments in mechanisms mitigating the risks in many cases is not clear, primarily due to the inconsistency of these risks and variability of the ways in which they are addressed. Thus, a trustworthiness framework includes impact assessment capabilities.