ISO/IEC 30147

Edition 1.0 2021-05

INTERNATIONAL STANDARD

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

ISO/IEC 30147:2021-05(en)

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

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

ISO/IEC 30147

Edition 1.0 2021-05

INTERNATIONAL STANDARD

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.020; 35.030

ISBN 978-2-8322-9808-4

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

CONTENTS

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

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.

3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this document.

7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.

8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.

9) Attention is drawn to the possibility that some of the elements of this ISO/IEC document may be the subject of patent rights. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

1 Scope

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

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

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

ISO 31000, *Risk management – Guidelines*

3 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.7
integrity
property of accuracy and completeness

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

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

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

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

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

3.10
IoT system
system providing functionalities of IoT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4 Abbreviated terms

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

5 IoT systems/services and IoT trustworthiness

5.1 Characteristics specific to IoT systems and services

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

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

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

Activities and tasks in each process to realize IoT trustworthiness are included in those for the IoT system by which the IoT service is provided. Descriptions of activities and tasks are represented by those for an IoT system, unless otherwise specified. When applied to an IoT service, choose activities and tasks that are applicable.

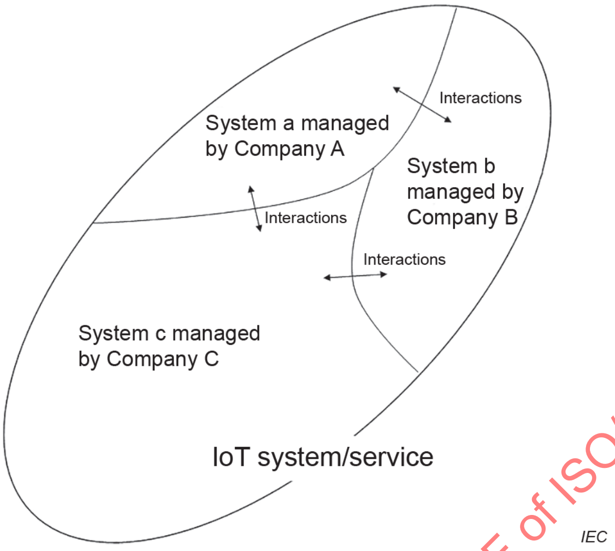
Interactions
System a managed by Company A
System b managed by Company B
Interactions
Interactions
System c managed by Company C
IoT system/service
IEC

Figure 1 – An IoT system, a system of systems

A Thing in an IoT system might be the following status or might have the following issues.

1) Compromised Thing

An intruder could have taken control of the Thing-of-interest and provided data, command and controls with the intent of disrupting the entire IoT setup resulting in the loss of trust of the Thing. This results in hacking of flights or automobiles, for example.

2) Incorrectly configured Thing

Because of some fault in command and control, the configuration of the Thing-of-interest could have exhibited a state that is neither expected nor detected, resulting in loss of IoT trustworthiness of the Thing. An example of this issue is CO_2 and SO sensors incorrectly configured in a gas turbine.

3) Damaged Thing

Because of some operational conditions, the Thing-of-interest could have become damaged, resulting in a situation or state that the Thing-of-interest is not trustworthy. This can cause a disaster if it is an altitude, speed, or flap sensor in an airplane.

4) Incorrect interactions because of poor interfaces

The interfaces between the Thing-of-interest and other Things could have lost the compatibility because of various factors (upgrades, incorrect patches, wrong configuration and so on), resulting in the Thing-of-interest ceasing to be trustworthy. For example, patches not or incorrectly installed in medical devices can cause a serious healthcare problem.

5) Incompatibility because of incorrect configuration

The Thing-of-interest could be configured incorrectly (for example, units of measurement, size of data exchange, nature of data, and so on), resulting in a situation that the information received from the Thing-of-interest is not useful, which results in the Thing-of-interest ceasing to be trustworthy. An example is incorrect baud rate used for configuring the IoT devices.

6) Failure to respond

The Thing-of-interest may fail to respond in certain situations to other Things because of a variety of factors (not a known request, not configured to respond, and so on), resulting in the Thing-of-interest ceasing to be trustworthy from the point of view of the other Things. The Air France 447 case is considered an example of this.

7) Failure to recognize

The Thing-of-interest may generate a response which is not recognized as a meaningful interaction because of the incorrect configuration of other Things, resulting in the Thing-of-interest and the other Things losing mutual trust. For example, altimeter failure results in discrepancy between the displayed altitudes.

As Things in an IoT system are such as those in the above, IoT systems have specific conditions and characteristics which are very different from other existing IT systems, such as the following.

a) The extent and the degree of impacts of threats become very wide and big. The impacts may include damages to the lives and properties of individuals, leaking of confidential information of individuals.

b) The life time of IoT systems, especially in operation and maintenance, is sometimes very long. For example, the lifespan of an IIoT system is more than ten years in general.

c) There are cases where it is very difficult to monitor and manage IoT devices. Unmanaged IoT devices may connect to IoT systems. Users may not be aware of problems if they occur. For example, an IoT system suffers from security issues by not being updated or in relation with firmware issues.

d) It can be difficult for communication entities including IoT devices to sufficiently understand the environments of each other.

e) The functions and performances of IoT devices are restricted.

f) There are possibilities of connections in IoT systems which the developers did not expect. After an IoT device is connected to the Internet, the IoT system to which the IoT device provides data may change. The data owners and users of the IoT system may also change as time passes.

Because of the above conditions and characteristics, IoT system can have risks shown in Annex A. Annex B provides an overview of how the above issues are resolved with the processes in Clause 6.

5.2 IoT trustworthiness

The definition of IoT trustworthiness can apply to the entities within an IoT system if "an IoT system" in the definition is replaced appropriately. Note that IoT trustworthiness is realized if IoT trustworthiness of all the entities in the IoT system is achieved.

IoT trustworthiness, especially safety, is not realized only with ICT elements. Only ICT elements are dealt with in this document.

The concept of IoT trustworthiness is similar to that of dependability, which covers reliability, availability, maintainability and supportability and other related attributes such as durability, integrity, recoverability and robustness (see IEC 62853[9]). This document defines that security comprises integrity and availability as well as other attributes. Maintainability, supportability, durability, recoverability, and robustness themselves do not appear in the definition of IoT trustworthiness. However, they are attributes to achieve resilience and reliability of IoT trustworthiness.

The relative importance of each of safety, security, privacy, reliability and resilience depends on the nature and the context of the IoT system.

In addition to the five factors listed in the definition of IoT trustworthiness, the following factors can be also relevant to the IoT trustworthiness. In Clause 6, the five factors are mainly considered, but the following factors should also be considered in each process, if necessary.

a) Coherence

   The interaction between two or more Things-of-interest needs to be coherent and meaningful to the situation context.

b) Consistency

   The interaction between two or more Things-of-interest across different instances needs to be consistent and in accordance with the expectations defined earlier.

c) Flexibility

   The Thing-of-interest needs to be able to adapt to the different conditions that it encounters because of the change in environment, change in relationships, change in situation context, change in responses and so on.

d) Robustness

   The Thing-of-interest needs to be strong and not be vulnerable to changes introduced into the environment or the Internet either intentionally or non-intentionally.

e) Cohesion

   The Thing-of-interest needs to compose the Internet of Things together and function seamlessly as a cohesive whole.

f) Recoverability

   The Thing-of-interest needs to be able to maintain and preserve a specified level of operations and quality, even in the event of failure, in a specific context of use.

g) Scalability

   Adding a Thing-of-interest (or even a new feature to the Thing) needs to not escalate the need for upgrading existing working methodology, but rather accommodate, maintain, and preserve the potential of growth of the system.

6 Processes for realizing IoT trustworthiness

6.1 General

For each process, there is no change from "Purpose" and "Outcomes" in ISO/IEC/IEEE 15288:2015. Therefore, this document describes only the supplements to "Activities and tasks" in ISO/IEC/IEEE 15288:2015. Follow ISO/IEC/IEEE 15288:2015 at each process unless otherwise specified.

6.2 Agreement processes

6.2.1 Acquisition process

In addition to the contents in 6.1.1.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), include the selection criteria.

   NOTE The selection criteria include, for example:

   i) management systems properly established and operated, help desks and support systems well prepared, and service management efficiently and effectively operated;

   ii) requirements when the contract with the supplier is finished (e.g. expiration of contract period, end of support).

b) In a) 2), include in the request requirements for IoT trustworthiness appropriate to the processes and IoT system-of-interest that the product or service will be used for, especially continuous improvement of the standard measures, related procedures, and others on IoT trustworthiness. Note that the request identifies the privacy principles, which meet those of the IoT system-of-interest, such as consent and choice, transparency, and individual participation (see ISO/IEC 29134:2017) if the product or service handles personal identifiable information of users of the IoT system-of-interest.

c) In e) 1), confirm that the delivered product or service satisfies the requirements on IoT trustworthiness in the agreement, if any.

6.2.2 Supply process

In addition to the contents in 6.1.2.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 2):

   1) Include requirements when the contract with the acquirer is finished (e.g. expiration of contract period, end of support) in the criteria.

   2) Consider the importance of the to-be-supplied system or service in the acquirer's system or service in defining a supply strategy.

b) In c) 1), include the scope of the responsibilities on IoT trustworthiness throughout the life cycle in the acceptance criteria of the agreement.

c) In e) 2), improve continuously the standard measures, related procedures, and others on IoT trustworthiness.

6.3 Organizational project-enabling processes

6.3.1 Life cycle model management process

In addition to the contents in 6.2.1.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 5):

   1) Consider each of the five factors of IoT trustworthiness. If a factor requires a specific life cycle model different from other factors, take this fact into consideration. Address any conflicts arising from different life cycle models according to the priorities of factors which are set up by the IoT trustworthiness policy.

6.3.2 Infrastructure management process

There is no supplement to this process.

6.3.3 Portfolio management process

There is no supplement to this process.

6.3.4 Human resource management process

In order to realize IoT trustworthiness of the IoT system-of-interest, conduct activities and tasks written in 6.2.4.3 of ISO/IEC/IEEE 15288:2015 for IoT trustworthiness because the technologies in IoT are updated rapidly.

6.3.5 Quality management process

In order to realize IoT trustworthiness of the IoT system-of-interest, conduct activities and tasks written in 6.2.5.3 of ISO/IEC/IEEE 15288:2015 for IoT trustworthiness. This is done by replacing "quality" with "IoT trustworthiness" in the activities and tasks for "Quality Management process" in ISO/IEC/IEEE 15288:2015.

6.3.6 Knowledge management process

In order to realize IoT trustworthiness of the IoT system-of-interest, conduct activities and tasks written in 6.2.6.3 of ISO/IEC/IEEE 15288:2015 for IoT trustworthiness because the technologies in IoT are updated rapidly.

6.4 Technical management processes

6.4.1 Project planning process

In addition to the contents in 6.3.1.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), identify also the policy on IoT trustworthiness. In this task, identify each interaction (input/output) with other interrelated IoT systems and their data protection policies. At a second step, identify which factors of IoT trustworthiness relate to each interaction and prioritize the factors at each interaction. Considering all these, determine the policy on IoT trustworthiness including business continuity of the IoT system-of-interest.

b) In b) 4):

   1) Define roles and responsibilities throughout the life cycle separately for each factor of IoT trustworthiness – security, privacy, reliability, resilience, and safety – after recognizing roles and responsibilities of other related systems or services. Define also a role to control and be responsible for the whole IoT trustworthiness. Contain multiple members in the role, say IoT trustworthiness team, and assign the chief responsible for the IoT trustworthiness of the IoT system-of-interest. In addition, assign a chief to each team of the five factors. Demonstrate top management's commitment to IoT trustworthiness.

   2) Define communication channels between the IoT trustworthiness team and each of the teams of the five factors, and also those between relevant organizations responsible for other related systems or services.

c) In b) 6), plan the acquisition of materials and enabling system services supplied from outside the project, especially from other systems in the IoT system, which are interrelated to the IoT system-of-interest.

6.4.2 Project assessment and control process

In addition to the contents in 6.3.2.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), identify activities for the acquired products or systems that are not compliant to contractual requirements found in technical management processes and technical processes.

b) In b) 7):

   1) Conduct required management and technical reviews when internal and external incidents on IoT trustworthiness occur and when the IoT system-of-interest connects to new IoT devices/systems.

   2) Check the impacts caused by internal and external incidents on IoT trustworthiness to the production by the IoT system-of-interest, if applicable.

c) In c) 1):

   1) Include continuous improvements of the activities and tasks for IoT trustworthiness in the related processes.

      NOTE The improvements include detection of security incidents, contingency plans, and so forth.

   2) Choose actions that minimize damages and mitigate the impacts caused by future incidents on IoT trustworthiness.

   3) Include necessary actions for the production by the IoT system-of-interest in order to keep the quality of the products, if applicable.

6.4.3 Decision management process

In addition to the contents in 6.3.3.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 3), involve especially the relevant parties on the IoT devices/systems which are interrelated to the IoT system-of-interest in the decision-making in order to draw on experience and knowledge, if appropriate.

b) In b) 2), include certainties and risks in measurable selection criteria.

6.4.4 Risk management process

In addition to the contents in 6.3.4.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) Conduct activities for risk management in alignment with ISO 31000 or conduct those separately and in parallel for each factor of IoT trustworthiness in alignment with the existing International Standards: ISO/IEC 27005:2018 for security, ISO/IEC 29134:2017 for privacy, ISO/IEC 27031 for resilience, and ISO/IEC Guide 51, IEC 61508 (all parts) and many industry specific standards for safety, for example. Ensure that physical risks against safety are taken into consideration. Study relevant accidents and incidents which have already occurred in these activities.

b) In a) 1), consider when and under what conditions risk assessment should be undertaken and how often risks and their treatments should be reviewed. This is because the risks and the acceptable risks of the IoT system-of-interest may change as time passes.

c) In a) 2):

   1) Identify the assets and processing of the IoT system-of-interest.

   2) Prioritize them in each of the five factors of IoT trustworthiness, where priority levels are defined independent of the five factors and approved by the IoT trustworthiness team.

d) In b) 1), define criteria by which the significance of risk will be decided. This may be based on state of risk (consequences and their likelihood) or other factors and may differ for each of the categories of IoT trustworthiness (e.g. decisions about whether to treat a safety risk may be based on criteria of risks being reduced so far as is reasonably practicable).

e) In c), record the results from each task.

f) In c) 1), consider:

   1) risks which may be caused by other IoT systems which connect to the IoT system-of-interest, risks which may be caused by other IoT systems, which may connect to the IoT system-of-interest in the future including replacements of IoT devices/systems, and also the case where the IoT system-of-interest receives contradicting requests from multiple entities, between which there are no relations at all, as a risk because they may cause an incident of the IoT system-of-interest;

   2) risks of the IoT system-of-interest which may influence other IoT systems;

   3) risks caused by internal fraud, mistakes in operation, and unawareness of users on specifications of the IoT devices/system.

g) When d) 2) for each factor has finished, assess proposed risk treatments to check that they do not introduce new risks to the IoT system-of-interest or to other factors of IoT trustworthiness. Iterate this task until all the factors get consistent results. If there are conflicts among the results from risk management process of the factors of IoT trustworthiness, cooperate to resolve the conflicts. If the conflicts are not resolved, the IoT trustworthiness team determines the priority among the risks and resolves the conflicts.

h) In d) 4), review and authorize the results of the whole risk management process activities where the resolved conflicts, if any, are reported clearly and in detail to the IoT trustworthiness team, and update document to reflect new risk treatments as existing controls.

6.4.5 Configuration management process

In addition to the contents in 6.3.5.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1):

   1) Manage automatic updates of configuration.

   2) Include the protection of configuration into the necessary baseline.

   3) Coordinate the configuration management strategy well across the organizations managing IoT systems, which are connected to the IoT system-of-interest, to cover the whole life cycle of the IoT system-of-interest or the extent of the contract, as appropriate.

b) In b) 4), consider well security risks caused by connection to the Internet and reflect the results to the baseline, especially to IoT devices/systems which have not been connected to the Internet.

c) In c), review configuration change management from the viewpoint of IoT trustworthiness.

6.4.6 Information management process

In addition to the contents in 6.3.6.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1):

   1) Define the strategy to meet the privacy principles if the IoT system-of-interest handles personal identifiable information.

   2) Define who collects from which resource and how to analyse relevant information on IoT trustworthiness continuously.

      NOTE 1 The information resources can include IoT device vendors, consultation companies, the national computer security incident response team, and so forth. The information includes recent countermeasures on IoT trustworthiness which need to be shared with stakeholders.

   3) Categorize the collected information and analysed information depending on importance and impact, and also categorize the stakeholders.

      NOTE 2 The categorization of the collected information can be the five factors of IoT trustworthiness. This will make it easy to disseminate the relevant information to relevant stakeholders to maintain the IoT trustworthiness of the IoT system-of-interest.

   4) Define urgent level of information.

   5) Define who disseminates which category of information to which category of stakeholders, how and how urgently when in the life cycle in order to maintain IoT trustworthiness of the IoT system-of-interest.

      NOTE 3 This includes communication with the top management and other stakeholders including external organizations on the responsibility of the IoT system-of-interest, recovery after a major incident, and so forth.

   6) Define rules regarding disclosure of information on incidents which occurred in the IoT system-of-interest.

b) In a) 4), define formats and structure for each category of stakeholders so that they do not misunderstand the disseminated information.

6.4.7 Measurement process

In order to realize IoT trustworthiness of the IoT system-of-interest, conduct activities and tasks written in 6.3.7.3 of ISO/IEC/IEEE 15288:2015 for IoT trustworthiness.

6.4.8 Quality assurance process

In order to realize IoT trustworthiness of the IoT system-of-interest, conduct activities and tasks written in 6.3.8.3 of ISO/IEC/IEEE 15288:2015 for trustworthiness. This is done by replacing "quality" with "IoT trustworthiness" in the activities and tasks in 6.3.8.3 of ISO/IEC/IEEE 15288:2015.

In addition to the contents in 6.3.8.3 on quality assurance process written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), consider the following reflecting the characteristics of the IoT system-of-interest:
   1) testing on security and privacy in which the behaviours and environments of users are reflected;
   2) testing on operation and maintenance functions which are to be used for a long time;
   3) testing in which a large amount of data and a lot of IoT devices are used;
   4) testing in which the IoT system is used in unexpected ways;
   5) testing of the cloud/edge where the IoT system-of-interest is implemented;
   6) regulations of the places where the IoT system-of-interest is to be used.

6.5 Technical processes

6.5.1 Business or mission analysis process

In addition to the contents in 6.4.1.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), consider also problems and opportunities concerning IoT trustworthiness.
b) In b) 2), define IoT trustworthiness of the IoT system-of-interest.

   NOTE This definition of IoT trustworthiness is examined in later processes if necessary.

c) In c) 1), consider preliminary operational concepts and other concepts also from the viewpoint of IoT trustworthiness.

6.5.2 Stakeholder needs and requirements definition process

In conducting stakeholder needs and requirements definition process, include the organizations which own/manage IoT systems connected to the IoT system-of-interest in the stakeholders.

In addition to the contents in 6.4.2.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 2), prioritize the stakeholder needs and requirements considering the importance in order to continue the business by the IoT system-of-interest.
b) In b) 1), include the viewpoints of IoT trustworthiness and consider the length of the life time of the IoT system-of-interest.
c) In b) 2), include also stakeholder needs on IoT trustworthiness.
d) In b) 3), consider relations, including conflicts, among five factors of IoT trustworthiness.
e) In c) 2), include the interaction between users and the system between to-be-connected IoT systems, if any.
f) In d) 3), include stakeholder requirements, consistent with life cycle concepts, scenarios, interactions, constraints, and critical quality characteristics on IoT trustworthiness.
g) In e) 1), consider carefully the priority among the five factors, if applicable.
h) In e) 2), consider measures on IoT trustworthiness, if applicable.

6.5.3 System requirements definition process

In conducting system requirements definition process, define also requirements for IoT trustworthiness to the IoT system-of-interest.

In addition to the contents in 6.4.3.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), take IoT trustworthiness into consideration.

b) In a) 2), clarify the existing requirements related to IoT devices and networks, which are the elements of the IoT system-of-interest, such as

   1) statutory and regulatory requirements,

   2) essential requirements not stated in 1), and

   3) additional requirements recognized as necessary in the relevant industries.

   NOTE IoT regulations can come from multiple sources and will differ across jurisdictions. Regulations that specifically address IoT are uncommon at the time of writing this document; however, regulations related to IoT trustworthiness, more explicitly cyber security, critical infrastructure protection, health and safety, environmental protection, and national security can all be in scope as regulatory requirements for IoT systems.

c) In b) 1), classify functions into administrative and non-administrative and define the relation to IoT trustworthiness, if necessary.

d) In b) 2), define necessary implementation constraints on IoT trustworthiness, in particular, considering the limited resources of IoT devices.

e) In b) 3), identify system requirements that relate to risks, criticality of the system, or critical quality characteristics on IoT trustworthiness.

   NOTE System requirements on IoT trustworthiness include the following.

   i) Appropriate initial settings and their checking.

   ii) Authorization of requests to the IoT system-of-interest.

   iii) Authentication of accesses and requests to the IoT system-of-interest:

   Authentication includes that for physical accesses, for example.

   Authentication methods, measures to multiple failures of authentication trials, and others need to be considered depending on the importance of the application and the risk of the accesses and requests. Multifactor authentication also needs to be considered.

   iv) Protection of functions and assets:

   Protection includes encryption and integrity checking for stored and communication data, invalid checking of communication data, and use of tamper-resistant hardware if applicable. When cryptography is used, the life cycle management of cryptographic keys needs to be also considered.

   v) Alerting against anomalies in advance, for example, judging from predictive information.

   vi) Proactive countermeasures against anomalies.

   vii) Monitoring, recording, and reporting of anomalies.

   viii) Acquiring logging data to identify the causes of anomalies.

   ix) Monitoring configurations of components in the IoT system-of-interest.

   x) Maintaining the operation even if anomalies occur:

   Assignment of sufficient resources is needed in order to maintain operation even if a denial of service or a natural disaster occurs to the IoT system-of-interest.

   xi) Recovering immediately after anomalies:

   For recovery, backup of appropriate system components and checking of the backup data are needed.

   xii) Autonomous halt and operation-suspending.

   xiii) Restricting installation of software after start of operation.

   xiv) Deletion of data.

   xv) Maintaining IoT trustworthiness even if time passes.

f) In b) 4), define system requirements and rationale on IoT trustworthiness.

g) In c) 1), analyse the complete set of system requirements from IoT trustworthiness aspects, especially whether it is consistent among the five factors of IoT trustworthiness.

h) In c) 2), define critical performance measures that enable the assessment of technical achievement on IoT trustworthiness, if necessary.

i) In d) 1), obtain explicit agreement on the system requirements from the chief of the IoT trustworthiness team.

6.5.4 Architecture definition process

In addition to the contents in 6.4.4.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 2), identify stakeholder concerns on IoT trustworthiness.

b) In a) 3), consider step-by-step and continuous approach because there may be changes in relevant regulations and technologies implemented in the IoT system caused by the technological innovation.

c) In a) 4), define evaluation criteria on IoT trustworthiness. In particular, consider

   1) architecture such that influences of anomalies in an architectural entity do not spread to other architectural entities, and

   2) architecture such that architectural entities can maintain IoT trustworthiness, even if an unspecified entity connects to the IoT system-of-interest.

d) In b) 1), take the layers of cloud, edge, and IoT devices into consideration.

e) In c) 1), consider IoT trustworthiness of interfaces and interactions with external entities.

f) In c) 2), identify appropriate architectural entities which realize each requirement of IoT trustworthiness considering the hardware resources and other constraints. This does not have to be done by an individual architectural entity but may be done by multiple architectural entities as a whole IoT system.

g) In c) 3), allocate those on IoT trustworthiness.

h) In d) 2), consider network segmentation between the system elements.

i) In e), assess architecture candidates also from the aspects of IoT trustworthiness.

j) In f) 1), allocate the chief of the IoT trustworthiness team for the governance.

k) In f) 2), obtain explicit acceptance of the architecture also by the chief of the IoT trustworthiness team.

6.5.5 Design definition process

In addition to the contents in 6.4.5.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 2), determine the necessary factors of IoT trustworthiness.

b) In a) 3), consider the five factors of IoT trustworthiness, in particular security which evolves very fast.

c) In a) 4), define evaluation criteria on IoT trustworthiness. In particular, consider

   1) design such that not only each system element can maintain IoT trustworthiness but also the entire system can maintain IoT trustworthiness,

   2) design such that influences of anomalies in a system element do not spread to other system elements,

   3) design such that consistency is achieved among the five factors of IoT trustworthiness,

   4) design such that system elements can maintain IoT trustworthiness, even if unspecified elements connect to the IoT system-of-interest,

   5) design such that stable parts and non-stable parts of functions are made separate considering the successive updates of IoT functions, and

   6) strategy of logging of the entire IoT-system-of-interest including the classification of priority, the retention period for each classified priority, timing, transmission, permission of access, and so forth.

d) In b) 1), allocate also system requirements to system elements on IoT trustworthiness (see 6.5.3).

e) In c) 2), assess each candidate non-developmental item and new design alternative from the viewpoints of IoT trustworthiness.

f) In d) 1), map the five factors of IoT trustworthiness.

6.5.6 System analysis process

In addition to the contents in 6.4.6.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), identify the problem or question that requires system analysis from the viewpoints of IoT trustworthiness.

b) In a) 2), include IoT trustworthiness team and teams of the five factors into stakeholders.

c) In a) 3),

   1) include analysis on incidents each of which is caused by a violation of one or more factors of the IoT trustworthiness,

   2) include impact analysis of these incidents to the IoT system-of-interest and the stakeholders, and

   3) obtain explicit agreement from the chief of the IoT trustworthiness team.

d) In a) 4),

   1) include correlation analysis of the events and comparative analysis with the incident information obtained from outside the IoT system-of-interest where the risk level of an event is determined with specified criteria,

   2) consider attackers' intention analysis for security incidents, and

   3) consider digital forensics for any type of incident (not only for security).

e) In a) 5), define the period for the review of system analysis method.

f) In b) 3), review the result on issues in which factors of IoT trustworthiness interrelate to each other.

g) In b) 5), categorize the results of the system analysis according to the impact, the relevant component and stakeholder impacted, and so forth.

6.5.7 Implementation process

In addition to the contents in 6.4.7.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), consider application of technologies depending on each layer (cloud, edge, or IoT device) of the IoT system-of-interest. Include the synchronization of the clocks used in logging.

b) In a) 2), consider the limited resources of IoT devices.

c) In b) 3), ensure that the IoT system-of-interest meets system requirements in which multiple factors of IoT trustworthiness interrelate to each other and record the objective evidence in detail according to the importance of the corresponding system requirement.

6.5.8 Integration process

In addition to the contents in 6.4.8.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), identify and define check points for the correct operation and integrity of the assembled interfaces and the selected system functions for initial settings.

b) In a) 2), define carefully when and under what conditions a network segment in the IoT system-of-interest is connected to other network segments.

6.5.9 Verification process

In addition to the contents in 6.4.9.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), consider

1) maximum values related to the IoT system-of-interest (maximum number of connected IoT devices, maximum amount of data, the life time of IoT devices, and the maximum connections of IoT devices, etc.),

2) variations of IoT devices and systems connected to the IoT system-of-interest (interoperability of functions and data, etc.),

3) variations of users, user behaviours, and user environments related to the IoT system-of-interest considering demographics of users and privacy protection of users, and so forth,

4) actions to system failures and exceptional events to the IoT system-of-interest (connection of unspecified IoT devices, handlings of unexpected data, failures of IoT devices or systems caused when they are connected to the IoT system-of-interest, communication failure, use of the IoT system-of-interest for a long period of time where resources are exhausted, contradicting requests from multiple external systems, etc.),

5) security measures without significant side effects on other factors of IoT trustworthiness (detection of vulnerabilities exploitation, connection to a system whose security policies are not consistent with those of the IoT system-of-interest, influence of security functions on other factors, data sanitization/deletion and restoring the initial configuration, if necessary, when an IoT device/system is transferred to another owner or disposed of), and

6) stable operation for a long period of time (failure analysis functions, update functions, etc.).

b) In a) 2), consider the items in a). Reflect the results to requirements, architecture, or design.

c) In a) 3), select those considering the items in a). Because there are massive verification cases, consider

1) improvements in efficiency,

2) reorganization and streamlining of verification,

3) reduction of verification man-hours, and

4) facilitation of recursive and compositional verification.

d) In a) 4), consider the construction of verification environment of large-scaled system and data and efficient verification.

NOTE The following items are taken into account:

i) connection of various kinds of IoT devices through the available interfaces,

ii) handling of large amount of data,

iii) handling of malformed data,

iv) handling of failures and exceptional events,

v) handling of security anomalies,

vi) verification cases where the real IoT system is used, those where a simulated system is used, or those where a combination of the real IoT system and a simulated system are used,

vii) reorganization and streamlining of verification,

viii) reduction of verification man-hours, and

ix) facilitation of recursive and compositional verification.

e) In a) 5), consider

1) functions for verification,

2) modularization of architecture, and

3) unification of interface used for verification, especially for control and monitoring.

f) In b) 1), include the checking procedure of connection to a running real IoT system, if necessary.

g) In c) 2), record operational incidents and problems with evidence including the reason of conclusion.

NOTE There can need to be explanation to stakeholders when troubles occur after start of operation. Preparing for such a case, record supplementary information including the reason of conclusion in verification activities in addition to the result success/failure. In particular, it is important for a case when the conclusion is success even if there were differences from the specification. Description to the manual needs to be considered, if applicable.

6.5.10 Transition process

In addition to the contents in 6.4.10.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In b) 2), ensure the initial settings.

b) In b) 4), demonstrate the proper initial settings including

   1) physical block of unnecessary ports of machines and IoT devices, and

   2) connection to real IoT systems, if necessary.

c) In b) 5), provide

   1) required actions to connect the IoT system-of-interest to the external network,

   2) change from the initial ID and password, and awareness of strength of password,

   3) necessity of maintenance of constituent components and report of maintenance status to the users,

   4) awareness of aged deterioration of security functions and necessity of the newest version of software as countermeasure against new vulnerabilities,

   5) reactions against failures, troubles, and incidents, and

   6) data sanitization/deletion and restoring the initial configuration, if necessary, when an IoT device/system is transferred to another owner or disposed of.

d) In c) 3), trace the transitioned system elements depending on the importance of the system elements in the IoT system-of-interest.

6.5.11 Validation process

In addition to the contents in 6.4.11.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), consider the validation scope and corresponding validation actions also from the viewpoint of IoT trustworthiness.

NOTE The following items are taken into account:

i) functions specific to IoT,

ii) accepted differences of performance of IoT devices from the specifications,

iii) variations of IoT devices and protocols used in communication with IoT devices,

iv) number of connections,

v) variations of data types and data sizes,

vi) measures to future extensions,

vii) user roles and behaviours,

viii) user environments and locations,

ix) feedbacks of status of use consistent with the privacy principle of the IoT system-of-interest and also conformant to relevant privacy regulations,

x) failures and troubles of IoT devices and their deterioration,

xi) countermeasures against threats and vulnerabilities,

xii) reactions to performance degradation and functional failure caused by system extension,

xiii) troubleshooting and incident handling of IoT devices and services used in the IoT system-of-interest,

xiv) monitoring system functioning for significant events, including failures and incidents, and

xv) replacement and termination of IoT devices and services used in the IoT system-of-interest.

b) In a) 2), identify the constraints considering the items in NOTE of a).

c) In a) 3), consider

1) use of validation scenario, and

2) use of stress testing tool, quasi failure generation tool, fuzzing tool, IoT device simulator, network simulator in order to validate IoT trustworthiness, and other tools intended for testing against threats and hazards to address IoT trustworthiness.

d) In a) 4), consider validation using validation scenario. Obtain agreement from the chief of the IoT trustworthiness team after review by the IoT trustworthiness team.

e) In b) 1), include the checking procedure of connection to running real IoT system if necessary.

f) In c) 2), record operational incidents and problems with evidence including the reason of conclusion.

NOTE Record supplementary information including the report of validation activities and execution log in addition to the result success/failure in order to achieve accountability. Record the evidence of explicit agreement from stakeholders.

6.5.12 Operation process

In addition to the contents in 6.4.12.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), define an operation strategy considering IoT trustworthiness.

NOTE Considering IoT trustworthiness, the operation strategy often includes

i) scope of responsibilities and collaboration with other organizations which operate other relevant systems,

ii) procedures to install IoT devices and software in order to check if they are genuine products,

iii) procedures to handle personal identifiable information to meet the privacy principles of the IoT system-of-interest and also conformant to relevant privacy regulations,

iv) separation of functions for system administrators and those for normal users,

v) appropriate procedures of life cycle management for users and other entities,

vi) physical access control as well as logical access control, including remote access, with an appropriate access control policy,

vii) preparation and support for most probable system behaviours of the IoT system-of-interest,

viii) scheduled backup and checking of appropriate components of the IoT system-of-interest,

ix) scope of logging and monitoring such as source/destination to/from special entities of the IoT system-of-interest, communication with external entities, and physical accesses to IoT devices and others, in compliance with applicable regulations, directives, industrial standards, and other rules,

x) procedures to update software, and

xi) operational monitoring activities including prioritization of anomalies and incidents.

b) In a) 5), include training on

1) connection of IoT devices,

2) user registration and accompanied actions,

3) handling of support-terminated products, and

4) deletion of data on appropriate timing.

c) In b) 3), pay attention to the influence of software update. Reconsider the update procedure if there are influences on the operation of the IoT system-of-interest or other relevant entities.

d) In b) 5), perform system contingency operations in alignment with the operation strategy.

e) In d) 1), provide information on IoT systems including risks in alignment with the strategy for information management.

6.5.13 Maintenance process

In addition to the contents in 6.4.13.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1), define a maintenance strategy under explicit agreement from the owner of the IoT system-of-interest.

NOTE Considering IoT trustworthiness, the maintenance strategy generally includes

i) prioritized maintenance strategy taking into account the importance of each component in the IoT system-of-interest, the impacts of events such as anomalies and incidents, and the most probable system behaviours caused by the anomalies and incidents, in compliance with applicable regulations, directives, industrial standards, and other rules,

ii) scope of responsibilities and collaboration, especially against incidents, with other organizations which maintain other relevant systems,

iii) procedures regarding remote maintenance including the permissions from relevant organizations,

iv) procedures to handle personal identifiable information to meet the privacy principles of the IoT system-of-interest and also conformant to relevant privacy regulations,

v) appropriate checking of logs, especially to those of communication with external entities and of physical accesses to IoT devices and others,

vi) reactions to the IoT system-of-interest (suspension/degeneracy) and to other systems (network disconnection) against failures, troubles, and incidents,

vii) procedures to recover the IoT system-of-interest in alignment with the policy of resilience,

viii) scheduled preventive maintenance actions such as updating of cryptographic keys, checking of vulnerabilities, and detection of security events, and

ix) skill to encounter incidents to maintain IoT trustworthiness of the IoT system-of-interest.

b) In a) 3), include information on IoT systems including risks in alignment with the strategy for information management.

c) In b) 5), include countermeasures against new vulnerabilities and deterioration of security functions. Pay attention to the influence of software update. Reconsider the update procedure if there are influences on the operation of the IoT system-of-interest or other relevant entities.

6.5.14 Disposal process

In addition to the contents in 6.4.14.3 written in ISO/IEC/IEEE 15288:2015, conduct the following.

a) In a) 1),

1) define procedures to dispose of personal identifiable information to meet the privacy principles of the IoT system-of-interest and also conformant to relevant privacy regulations,

2) let users of the IoT system-of-interest know relevant items in the disposal strategy.

Annex A
(informative)

Examples of risks specific to IoT systems

A.1 General

Risk is the effect of uncertainty on objectives where an effect is a deviation from the expected and objectives can have different aspects and can apply at different levels. Risks to IoT trustworthiness consist of risks to each factor (security, privacy, reliability, resilience, and safety) of trustworthiness and risks which arise from mutual dependence among the five factors.

A.2 Example 1: Security risk

There is a case in which criminals obtained a physical key to a maintenance door for an ATM, opened the ATM chassis, and withdrew cash from the ATM by connecting a cellphone, infecting the ATM with a virus, and so forth.

ATM specifications have become more standardized so that banks can procure ATMs from various suppliers as they like. This has made analysing a model of one manufacturer in order to attack an ATM of another manufacturer easier. As most ATMs in recent years run on a general-purpose OS, attackers can analyse the OS, prepare dedicated devices to attack the OS, and attack ATMs using them. For details, see [10].

A.3 Example 2: Reliability risk

There was an incident in which a defect in a pattern file of antivirus software made the performance of PCs decrease significantly. Because it happened on a Saturday, the damage to industries was limited to newspaper companies and transportation-related companies, etc., yet approximately 161 000 telephone enquiries were made from personal users and 13 000 from corporate users, of which only around 4 000 cases were responded to soon after the incident broke out. In IoT systems, not only PCs but also automobiles, home electrical appliances, and various other devices and systems are connected to the Internet. If they become unavailable all at once for any reason, as in the above case, impacts on daily life are significant. For software updates, sufficient consideration needs to be given so as not to affect reliability which allows users to use the systems whenever they want. For details, see [11].

A.4 Example 3: Safety risk

At a big event on information security, there was a demonstration of an in-vehicle device of a moving automobile that unauthorized hackers accessed remotely and controlled the engine and the steering wheel. The risk is high because human lives could be seriously injured by automobiles controlled remotely by invisible attackers. After the demonstration, 1,4 million vehicles of the model used in the demonstration were recalled.

The main cause of an attack such as the above is that the risk was not considered sufficiently in designing any of the composing elements including the mobile networks, the in-vehicle devices, the in-vehicle networks, and the vehicle information display services. This made possible a series of attacks in which the attackers entered from the mobile networks, got an unauthorized access to the in-vehicle devices, and altered the firmware on chips to send unauthorized instructions through the in-vehicle networks. Attacks need to be stopped somewhere within the composing elements in the vehicle system.

Conventional safety functions in general have not been implemented against intentional attacks because the systems-of-interest are not supposed to be connected to the Internet. In IoT systems, the attacks via the Internet against safety functions need to be considered and encountered. For details, see [12].

A.5 Example 4: Privacy risk

a) Smart cars integrate IoT devices to bring additional value to drivers and passengers. These devices communicate with each other and with the outside of the car (other cars, external services and so on). There are many documented cases of attacks on such automotive systems. Hackers can track a targeted automotive system, alter GPS coordinates, measure its speed, and drop pins on a map to trace its route as a result of which the privacy of the person travelling in the car is at risk. Another issue is that the sensors may not validate the subscriber of the information from the sensors resulting in sharing of personal information with third parties. Cellular connection of the automobile system may also have adverse impacts on privacy, for example in the case of remote tracking of the automobile by unknown people. It is also possible to create identity fraud by cloning the key fob wherein an intruder can misuse the identity of the user or another identity is used for communication with road infrastructures, manufacturer backend and so on. For details, see [13].

b) Healthcare data are considered to be private data. A patient may feel vulnerable if sensitive information like "a person p has certain disease d" gets revealed. Revelation of sensitive information not only affects the patient but also the family and society adversely. With increasing remote patient monitoring, it is but natural that health data from body sensors (wireless body area network – WBAN) of patients reaching the cloud (for access by doctors) is at risk of leakage. Measures should be taken to safeguard the privacy of a patient. This may be implemented through proper access control techniques. Access to patient data needs to be provided on a "need to know" basis and no user should be given more information than he or she needs. The data from WBAN is first passed to a local storage (smart device), which in turn connects to the cloud storage server. Measures need to be adopted at each such step since the smart device generally also acts as the data collection point for more than one patient. Finally, user authentication and authorization at the cloud storage will lead to data access by authorized user. For details, see [14], [15], and [16].

A.6 Example 5: Resilience risk

Smart public transportation systems use a plethora of integrated IoT devices to bring additional value to a city. These devices communicate with each other and with the operators and users for a variety of reasons and provide a variety of information. While the system as a whole is resilient to known failures due to specific causes or combinations of these, often the effect of cascading causes or combinations of causes on multiple fronts can be fatal. For example, electrical failure across the board, adverse weather conditions and communication network failure will result in the meltdown of the public transportation system especially in cases where the dependence on public transportation is significantly high. For details see [17] and [18].

A.7 Example 6: Risk arising from interconnected IoT trustworthiness factors

In the attack on the Ukrainian electricity supply chain in 2015, the telephone line was shut off by attackers and that facilitated the prolonged time of the compromise. The support only by telephone is not reliable, and the risk for the violation of this function is connected to increasing the risk for security and safety incidents.

Risks may also arise from conflicting situations. For example, for safety reasons it may be required to have the emergency access codes to the equipment. These codes disclosed to unauthorized people may lead to a security breach. At the same time, keeping the default codes secret or changing them with a password may lead to a situation where the safety hazard is not addressed in time.