



BSI Standards Publication

Internet of Things (IoT) — Reference architecture

National foreword

This British Standard is the UK implementation of ISO/IEC 30141:2018, incorporating corrigendum December 2020.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by ISO/IEC corrigendum December 2020 is indicated in the text by AC1 AC1.

The UK participation in its preparation was entrusted to Technical Committee IOT/1, Internet of Things.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 16427 5

ICS 35.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2018.

Amendments/corrigenda issued since publication

Date	Text affected
31 January 2021	Implementation of ISO/IEC corrigendum December 2020



ISO/IEC 30141

Edition 1.0 2018-08

INTERNATIONAL STANDARD



Internet of Things (IoT) – Reference architecture

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.020

ISBN 978-2-8322-5972-6

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

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references	9
3 Terms and definitions	9
4 Abbreviated terms	9
5 Internet of Things Reference Architecture (IoT RA) conformance.....	10
6 IoT RA goals and objectives	10
6.1 General.....	10
6.2 Characteristics.....	11
6.3 Conceptual Model	11
6.4 Reference Model and architecture views	11
7 Characteristics of IoT systems.....	12
7.1 General.....	12
7.2 IoT system trustworthiness characteristics	13
7.2.1 General	13
7.2.2 Availability	14
7.2.3 Confidentiality.....	14
7.2.4 Integrity	15
7.2.5 Protection of personally identifiable information (PII)	15
7.2.6 Reliability.....	16
7.2.7 Resilience.....	17
7.2.8 Safety	17
7.3 IoT system architecture characteristics	18
7.3.1 Composability.....	18
7.3.2 Functional and management capability separation	18
7.3.3 Heterogeneity	19
7.3.4 Highly distributed systems	20
7.3.5 Legacy support.....	20
7.3.6 Modularity.....	21
7.3.7 Network connectivity.....	21
7.3.8 Scalability.....	22
7.3.9 Shareability	22
7.3.10 Unique identification	23
7.3.11 Well-defined components.....	23
7.4 IoT system functional characteristics	24
7.4.1 Accuracy	24
7.4.2 Auto-configuration	25
7.4.3 Compliance	25
7.4.4 Content-awareness.....	26
7.4.5 Context-awareness.....	26
7.4.6 Data characteristics – volume, velocity, veracity, variability and variety	27
7.4.7 Discoverability	27
7.4.8 Flexibility	28
7.4.9 Manageability	29
7.4.10 Network communication.....	29

7.4.11	Network management and operation.....	30
7.4.12	Real-time capability	31
7.4.13	Self-description	31
7.4.14	Service subscription	32
8	IoT Conceptual Model (CM)	32
8.1	Main purpose	32
8.2	Concepts in the IoT CM	33
8.2.1	IoT entities and domains.....	33
8.2.2	Identity	35
8.2.3	Services, network, IoT device and IoT gateway	36
8.2.4	IoT-User	38
8.2.5	Virtual entity, Physical Entity and IoT device.....	39
8.3	High level view of CM	41
9	IoT Reference Model (RM).....	42
9.1	The IoT Reference Model context	42
9.2	IoT RMs	42
9.2.1	Entity-based RM	42
9.2.2	Domain-based RM	44
9.2.3	Relation between entity-based RM and domain-based RM.....	46
10	IoT Reference Architecture (RA) views	46
10.1	General description.....	46
10.2	IoT RA functional view	47
10.2.1	General	47
10.2.2	Intra-domain functional components	47
10.2.3	Cross-domain capabilities.....	50
10.3	IoT RA system deployment view	51
10.3.1	General	51
10.3.2	Systems/sub-systems in Physical Entity Domain (PED)	52
10.3.3	Systems/sub-systems in Sensing & Controlling Domain (SCD)	52
10.3.4	Systems/sub-systems in Application & Service Domain (ASD)	52
10.3.5	Systems/sub-systems in Operation & Management Domain (OMD).....	53
10.3.6	Systems/sub-systems in User Domain (UD).....	53
10.3.7	Systems/sub-systems in Resource Access & Interchange Domain (RAID)	53
10.4	IoT RA networking view	54
10.4.1	Communications networks	54
10.4.2	Communication networks implementation	55
10.5	IoT RA usage view.....	56
10.5.1	General description	56
10.5.2	Description of the roles, sub-roles and related activities	56
10.5.3	Mapping activities, roles and IoT systems in domains	61
11	IoT trustworthiness	64
11.1	General.....	64
11.2	Safety	65
11.3	Security	66
11.3.1	General	66
11.3.2	IoT system Information Security Management System (ISMS)	66
11.3.3	IoT system & product Security Life Cycle Reference Model	68
11.4	Privacy and PII Protection.....	69

11.5	Reliability	72
11.6	Resilience	73
11.7	Trustworthiness and the Reference Architecture	74
Annex A (informative)	Interpreting UML Class diagram for Conceptual Model	76
Annex B (informative)	Entity relationship tables for the CM	77
B.1	IoT entities and domains	77
B.2	Identity	78
B.3	Services, network, IoT device and IoT gateway	78
B.4	IoT-User	79
B.5	Virtual entity, Physical Entity and IoT device	80
Annex C (informative)	Relation between CM, RMs and RAs	81
Bibliography		83
Figure 1	– From generic Reference Architecture to context specific architecture	8
Figure 2	– IoT RA structure	11
Figure 3	– RM and architecture views	12
Figure 4	– Entity and domain concepts of the CM	33
Figure 5	– Domain interactions of the CM	34
Figure 6	– Identity concept of the CM	35
Figure 7	– Service, network, IoT device and IoT gateway concepts of the CM	36
Figure 8	– IoT-User concepts of the CM	38
Figure 9	– Virtual entity, Physical Entity, and IoT device concepts of the CM	39
Figure 10	– High level view of CM	41
Figure 11	– Entity-based IoT RM	42
Figure 12	– Domain and entity relationship, and representative conceptual entities in IoT systems	44
Figure 13	– Domain-based IoT RM	44
Figure 14	– Relation between entity-based RM and domain-based RM	46
Figure 15	– IoT RA functional view –decomposition of IoT RA functional components	47
Figure 16	– IoT RA system deployment view	52
Figure 17	– IoT RA networking view	54
Figure 18	– Roles present when the system is in use	57
Figure 19	– IoT service provider sub-roles and activities	59
Figure 20	– IoT service developer sub-roles and activities	60
Figure 21	– IoT-User sub-roles and activities	61
Figure 22	– Activities of device and application development	63
Figure 23	– Using device data for security-related analytics and operations	64
Figure 24	– IoT product Security Life Cycle Reference Model	69
Figure A.1	– Generalization	76
Figure A.2	– Association	76
Figure C.1	– Relation between IoT CM, RM, and RA	82
Table 1	– Characteristics of IoT systems	13
Table 2	– Overview of activities and roles	62

Table B.1 – Entity	77
Table B.2 – Domain	77
Table B.3 – Digital Entity	77
Table B.4 – Physical Entity	77
Table B.5 – IoT-User.....	77
Table B.6 – Network	78
Table B.7 – Identifier	78
Table B.8 – Endpoint	78
Table B.9 – IoT gateway	78
Table B.10 – IoT device	79
Table B.11 – Service.....	79
Table B.12 – Human user	79
Table B.13 – Digital user.....	79
Table B.14 – Application	80
Table B.15 – Sensor	80
Table B.16 – Actuator	80
Table B.17 – Virtual entity.....	80

INTERNET OF THINGS (IoT) – REFERENCE ARCHITECTURE

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.
- 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 National Committees and ISO member bodies.
- 3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or 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 National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.
- 5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC 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 publication.
- 7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member 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 of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.
- 8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 30141 was prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC joint technical committee 1: Information technology.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

IoT has a broad use in industry and society today and it will continue to develop for many years to come. Various IoT applications and services have adopted IoT techniques to provide capabilities that were not possible a few years ago. IoT is one of the most dynamic and exciting areas of ICT. It involves the connecting of Physical Entities (“things”) with IT systems through networks. Foundational to IoT are the electronic devices that interact with the physical world. Sensors collect the information about the physical world, while actuators can act upon Physical Entities. Both sensors and actuators can be in many forms such as thermometers, accelerometers, video cameras, microphones, relays, heaters or industrial equipment for manufacturing or process controlling. Mobile technology, cloud computing, big data and deep analytics (predictive, cognitive, real-time and contextual) play important roles by gathering and processing data to achieve the final result of controlling Physical Entities by providing contextual, real-time and predictive information which has an impact on physical and virtual entities.

IoT can be integrated into existing technologies. Real-time measurements generated by adding sensors to existing technology can improve its functionality and lower the cost of operations (e.g. smart traffic signals can adapt to traffic conditions, lowering congestion and air pollution). The data generated by IoT sensors can support new business models and tailor products and services to the tastes and needs of the customer. In addition to the applications, the technology needs to support supervision and adaptation of the IoT system itself.

Several forecasts indicate that IoT will connect 50 billion devices worldwide by the year 2020. There are a number of possible application areas, such as smart city, smart grid, smart home/building, digital agriculture, smart manufacturing, intelligent transport system, e-Health. IoT is an enabling technology that consists of many supporting technologies, for example, different types of communication networking technologies, information technologies, sensing and control technologies, software technologies, device/hardware technologies. This document is based on widely used enabling technologies that are defined in standards from several organizations such as ISO, IEC, ITU, IETF, IEEE, ETSI, 3GPP, W3C, etc.

Trustworthiness is recognized as an area of importance, and IoT can leverage current and future best practice. For example, monitoring and analysing deployed IoT systems is essential to maintain reliability and safety and security. Measures such as controlled access can ensure the security of the system.

This document provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practices. It uses a top down approach, beginning with collecting the most important characteristics of IoT, abstracting those into a generic IoT Conceptual Model, deriving a high level system based reference with subsequent dissection of that model into the four architecture views (functional view, system view, networking view and usage view) from different perspectives.

This document serves as a base from which to develop (specify) context specific IoT architectures and thence actual systems. ^[AC1] The contexts can be of different kinds including the business context, the regulatory context and the technological context, e.g. industry verticals, technological requirements and/or nation-specific requirement sets. ^[AC1] For more information, see Figure 1.

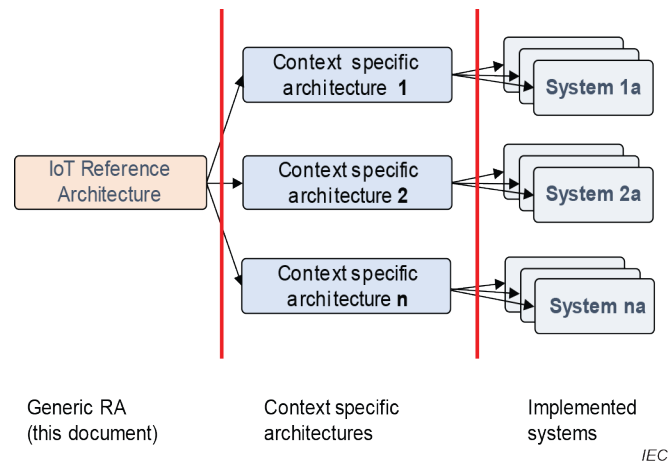


Figure 1 – From generic Reference Architecture to context specific architecture

INTERNET OF THINGS (IoT) – REFERENCE ARCHITECTURE

1 Scope

This document specifies a general IoT Reference Architecture in terms of defining system characteristics, a Conceptual Model, a Reference Model and architecture views for IoT.

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.

ISO/IEC 20924, *Internet of Things (IoT) – Definition and vocabulary*¹

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20924 apply.

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

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

4 Abbreviated terms

5Vs	volume, velocity, veracity, variability, and variety
API	application programming interface
ASD	Application & Service Domain
BSS	business support systems
CM	Conceptual Model
FQDN	fully qualified domain name
HMI	human machine interface
HTTP	Hypertext Transfer Protocol
HVAC	heating, ventilation and air conditioning
IaaS	infrastructure as a service
ICT	information and communication technologies
IoT	Internet of Things
IoT RA	Internet of Things Reference Architecture
LAN	local area network

¹ Under preparation. Stage at time of publication: ISO/IEC CDV 20924:2018.

LOB	line of business
OMD	Operation & Management Domain
OSS	operational support systems
PaaS	platform as a service
PED	Physical Entity Domain
PII	personally identifiable information
QoS	quality of service
RA	Reference Architecture
RAID	Resource Access & Interchange Domain
RFID	radio-frequency identification
RM	Reference Model
SaaS	software as a service
SCD	Sensing & Controlling Domain
UML	Universal Modelling Language
UD	User Domain
URI	uniform resource identifier
UUID	universally unique identifier

5 Internet of Things Reference Architecture (IoT RA) conformance

To claim conformance, the description of a concrete system architecture as provided by a vendor or system integrator should use the terminology and modelling concepts defined in this document, within the scope of their specific use case.

NOTE A separate conformity guide can be developed that can provide specific guidance to meeting and evaluating conformity to ISO/IEC 30141 to a broader set of entities beyond actual system descriptions.

6 IoT RA goals and objectives

6.1 General

The IoT Reference Architecture (IoT RA) represented in this document describes generic IoT system characteristics, a Conceptual Model, a Reference Model and a number of architectural views aligned with the architecture descriptions defined in ISO/IEC/IEEE 42010. [AC1] The IoT RA outlines the overall structured approach for the construction of IoT systems by providing an architectural structure framework. [AC1] In short, the IoT RA provides guidance for the architect developing an IoT system and aims to give a better understanding of IoT systems to the stakeholders of such systems, including device manufacturers, application developers, customers and users.

This document has the following descriptions:

- 1) the generic characteristics of IoT systems, outlining the characteristics expected from an IoT system;
- 2) the Conceptual Model (CM), describing the key concepts characterizing an IoT system;
- 3) the Reference Model (RM), providing the overall structure of the elements of the architecture;
- 4) a set of relevant architecture views, describing the architecture from a number of perspectives.

This document supports the following important standardization objectives:

- a) to enable the production of a coherent set of standards for IoT;
- b) to provide a technology-neutral reference point for defining standards for IoT; and
- c) to encourage openness and transparency in the development of a target IoT RA and in the implementation of IoT systems.

Figure 2 illustrates how the IoT RA is derived from a Conceptual Model and a set of characteristics that define a Reference Model and one or more architectural views.

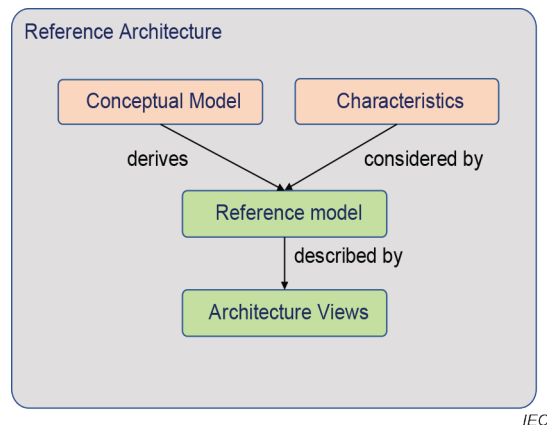


Figure 2 – IoT RA structure

Subclauses 6.2, 6.3 and 6.4 provide a summary of the characteristics, Conceptual Model and Reference Model, respectively.

6.2 Characteristics

The generic characteristics are described in Clause 7, which focuses on a number of key properties that an IoT system typically exhibits. Different application specializations can differ in terms of the actual quantification of these properties, but it is important for an IoT architect to consider how important the respective categories are for the particular system being designed. There are no characteristics that are required of any particular IoT system.

6.3 Conceptual Model

The Conceptual Model (CM) contains a number of vital concepts and describes how they relate to each other logically. Together with the generic characteristics, it provides the background and motivation for the architectural elements discussed in the architectural views in Clause 10. CM is described in Clause 8.

6.4 Reference Model and architecture views

RM is described in Clause 9. The RM and architecture views contain the parts as illustrated in Figure 3.

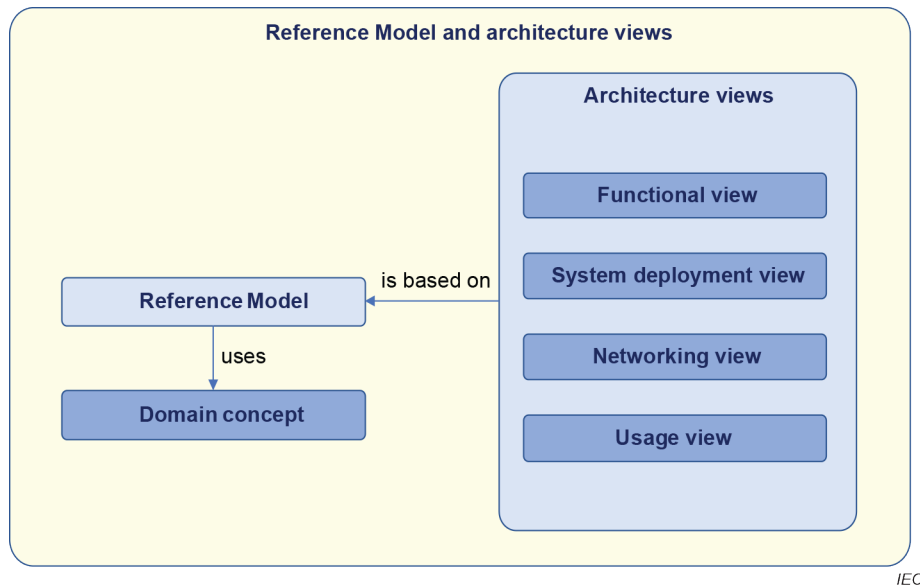


Figure 3 – RM and architecture views

Figure 3 above illustrates the relations between architecture views, Reference Model and domain concept. The domain concept is described in the CM in 8.2.1.1 and 8.2.1.3. Additionally, the RM is founded on the domain concept. A detailed description of domain based RM can be found in Clause 9.2.2.

The respective views are described in Clause 10.

7 Characteristics of IoT systems

7.1 General

Clause 7 provides characteristics of IoT systems. Functions based on all or a part of these characteristics can be implemented in IoT systems. Some of these characteristics are functional, such as network connectivity, while others are non-functional, such as availability and compliance. The characteristics are grouped and summarized in Table 1 and individually explained in 7.2 to 7.4.

Table 1 – Characteristics of IoT systems

Categories	Related characteristics
7.2 IoT system trustworthiness characteristics	7.2.2 Availability
	7.2.3 Confidentiality
	7.2.4 Integrity
	7.2.5 Protection of personally identifiable information
	7.2.6 Reliability
	7.2.7 Resilience
	7.2.8 Safety
7.3 IoT system architecture characteristics	7.3.1 Composability
	7.3.2 Functional and management capability separation
	7.3.3 Heterogeneity
	7.3.4 Highly distributed systems
	7.3.5 Legacy support
	7.3.6 Modularity
	7.3.7 Network connectivity
	7.3.8 Scalability
	7.3.9 Shareability
	7.3.10 Unique identification
	7.3.11 Well-defined components
7.4 IoT system functional characteristics	7.4.1 Accuracy
	7.4.2 Auto-configuration
	7.4.3 Compliance
	7.4.4 Content-awareness
	7.4.5 Context-awareness
	7.4.6 Data characteristics – volume, velocity, veracity, variability and variety
	7.4.7 Discoverability
	7.4.8 Flexibility
	7.4.9 Manageability
	7.4.10 Network communication
	7.4.11 Network management and operation
	7.4.12 Real-time capability
	7.4.13 Self-description
	7.4.14 Service subscription

7.2 IoT system trustworthiness characteristics

7.2.1 General

Trustworthiness is defined in ISO/IEC 20924 as follows:

"degree of confidence a stakeholder has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disruptions, human errors, system faults and attacks."

Within the scope of this document, security is defined as the combination of availability, confidentiality, and integrity.

7.2.2 Availability

7.2.2.1 Description

Availability is the property of being accessible and usable on demand by an authorized entity.² IoT systems can include both human users and service components as "authorized entities".

7.2.2.2 Relevance to IoT systems

In IoT systems, availability can be considered as a characteristic of devices, data and services. Availability of a device is related both to its inherent properties of operating correctly over time and to the network connectivity of the device. Availability of data is related to the ability of the system to get the requested data to and from a system component. Availability of services is related to the ability of the system to provide the requested service to users with a pre-defined QoS.

7.2.2.3 Examples

In some critical applications, e.g. health monitoring or intrusion detection, devices and data have to be highly available so that alarms can be sent to the system immediately when raised. In these cases, it is important that system design take into account potential failure modes and provide means of continuing operations, such as power supply backups, redundant devices, and multiple instances of a service.

7.2.3 Confidentiality

7.2.3.1 Description

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.³

7.2.3.2 Relevance to IoT systems

In an IoT system, confidentiality protection policies and mechanisms are responsible for prohibiting people or systems from reading data or control messages when they are not authorized to do so.

Confidentiality is a pre-requisite for secure operation, especially when the data to be transmitted contains secret tokens, e.g. for access control. Confidentiality is also required to protect sensitive data, which can include PII, e.g. personal health and financial information.

7.2.3.3 Examples

Data flowing through an IoT system could be considered confidential. Confidential data need to be protected from being used for criminal activities, and the inappropriate use of personal data needs to be prevented. For example, IoT motion detection sensors could reveal whether a property is occupied or not, allowing intruders to target the property.

Similar concerns relate to IoT smart meters, where the frequency of messages transmitted should not depend on the rate of electricity use, since this could reveal whether a property is occupied or not.

² Source: ISO/IEC 27000:2018, 3.7.

³ Source: ISO/IEC 27000:2018, 3.10.

7.2.4 Integrity

7.2.4.1 Description

Integrity is the property of accuracy and completeness,⁴ usually applied to information within a system.

7.2.4.2 Relevance to IoT systems

Integrity is vital for IoT systems to ensure that the data used for decision-making processes in the system and executable software have not been altered by faulty or unauthorized devices, by malicious actors, or by environmental causes.

7.2.4.3 Examples

In IoT deployments there is a risk that an intermediate device can alter the data and this can have impact on the functioning of the system. For example, an intermediate node can increase the value of the temperature of a room but air-conditioning system can rely on the given setting and not an altered setting from an anomaly.

7.2.5 Protection of personally identifiable information (PII)

7.2.5.1 Description

The concept of privacy overlaps, but does not completely coincide with, the concept of protection of PII. For IoT systems, pertinent entities can include people, technology and processes.

The term PII is used by various policies, rules, laws, and regulations that have their own scope and interpretation of the term. This document uses term PII as defined by ISO/IEC 27018:2014, 3.2:

"any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal"

Protection of PII is a legal or regulatory requirement in most jurisdictions whenever an IoT system involves personally identifiable information anywhere in its operation. Sensitivity extends to all PII from which sensitive PII can be derived, whether through aggregation, analysis or other means. Protection of PII is governed by a number of principles including, but not limited to, consent and choice; purpose legitimacy and specification; collection limitation; and data minimization. The principle of data minimization requires that organizations process only the minimally necessary PII for the identified purposes. PII should be securely deleted when no longer required.

Protection of PII is a general requirement and is governed by a series of principles which are described in ISO/IEC 29100:

- 1) consent and choice;
- 2) purpose legitimacy and specification;
- 3) collection limitation;
- 4) data minimization;
- 5) use, retention and disclosure limitation;
- 6) accuracy and quality;
- 7) openness, transparency and notice;

⁴ Source: ISO/IEC 27000:2018, 3.36.

- 8) individual participation and access;
- 9) accountability;
- 10) information security;
- 11) privacy compliance.

It is important that these principles are applied in any IoT system that is processing PII.

NOTE ISO/IEC 29100:2011, Clause 5 provides a more detailed discussion of these principles.

7.2.5.2 Relevance to IoT systems

Any IoT system which does collect, receive, process and/or exchange PII needs to ensure that such IoT systems and their interactions with other IoT systems (or IT systems in general) are in full compliance with privacy protection requirements of applicable jurisdictions. Situations where a user or person can be identified by data analysis or derived by machine learning mechanisms also need to be considered for protection. System owners in many jurisdictions are required to disclose a data breach. In the event of a compromise, it is important to ensure that they can identify the data that was compromised and report to local agencies.

7.2.5.3 Examples

Independent of the IoT application (e.g. wearables, healthcare monitoring, factory and building systems, automotive, energy, or smart home), the IoT system owner and operator acts as the PII controller. In this role, it is important to ensure the necessary access and data protection controls are identified and implemented for the IoT system. This includes ensuring adherence to local laws and regulatory requirements for data collection and destruction, seeking permission for collection of PII, and the creation of processes to notify users and officials of compromises to this information.

7.2.6 Reliability

7.2.6.1 Description

Reliability is a property of consistent, intended behaviour and results.⁵ An appropriate level of reliability in capabilities such as communication, service and data management is important to meet system requirements.

The desired level of reliability should always be seen in relation to the risk associated with the IoT system. Therefore, before changing an IoT system, the designer should evaluate the risk introduced by doing so. This can be handled through a risk management process as outlined in ISO 31010.

7.2.6.2 Relevance to IoT systems

An appropriate level of reliability is essential in diverse IoT system deployments and applications. Reliability can be highly critical in some applications, e.g. for specific health related applications, industrial manufacturing operations and time-critical applications.

7.2.6.3 Examples

Reliability of data is of great importance for the decision-making processes of many IoT systems. The absence of data or data corruption can lead to incorrect decisions or the failure to make decisions. Reliability of communication networks is important for ensuring the

⁵ Source: ISO/IEC 27000:2018, 3.55

availability and correct operation of IoT systems, particularly in mission-critical use cases or applications.

Medical devices are one potential IoT application area where the specifications for mean time between failures might be quite stringent, due to the possibility of injury or death if an IoT device, application or system providing medical capability were to fail while a patient is being treated.

7.2.7 Resilience

7.2.7.1 Description

Resilience is the ability of an IoT system or its components to adapt and continue to perform their required functions flexibly in the presence of faults and failures and other ad hoc changes without loss of operation and performance level.

7.2.7.2 Relevance to IoT systems

Communication, device or software component failures are to be expected in IoT systems, and without appropriate design they can escalate quickly causing global failure of the system. IoT systems need to be designed for resilience, incorporating self-monitoring and self-healing techniques to improve the system resilience.

7.2.7.3 Examples

An IoT system has to be resilient to gateway failures to ensure continuing communications paths between software components and IoT devices.

One approach to resiliency is to adopt a master–slave design where if the master unit fails, a redundant device is available to assume the master role. Industrial control devices and networks are a typical example of this resiliency approach.

For networks, a mesh network design is resilient to the failure of one link or one node – data can still flow from source to sink through an alternative route.

The resilience can be compared to a failsafe mode of a computer, or a limp home mode of a car. The essential functions can still be performed, but full functionality will not be possible.

7.2.8 Safety

7.2.8.1 Description

Safety is the state in which the risk of harm (to persons) or damage is limited to an acceptable level.⁶ Risk is the probability of the occurrence of harm combined with the severity of that harm. Harm includes injury or damage to the health of people, or damage to property or the environment. Harm can be due to malfunction, failure, or accident. While prior traits describe the desired behaviour of the system when operating correctly, safety includes the consideration of failure modes with the intent of preventing, reducing or mitigating the potential for undesired outcomes; specifically, damage, harm or loss.

7.2.8.2 Relevance to IoT systems

Many IoT systems are deployed in contexts or operational environments where damage, loss, injury or death might result if failure modes are not adequately addressed. In many operational contexts, approval to operate or connect will not be granted if safety requirements have not been met.

⁶ Source: ISO 21101:2014, 3.34

Even in contexts where compliance with safety standards is optional or voluntary rather than mandatory, proper consideration of safety factors can have significant impact on aspects such as continuity of operations, reduction of loss, prevention of injury or death, insurance premiums, torts and liability, and other issues.

7.2.8.3 Examples

IoT contexts where safety standards or requirements might need to be considered include medical or health care applications, transport such as aviation and automotive applications, consumer products, buildings, and environment monitoring. Many countries will have regulations for specific applications such as fire safety, national border safety, and radiation damage monitoring for systems commonly found in hospitals and atomic research centres.

7.3 IoT system architecture characteristics

7.3.1 Composability

7.3.1.1 Description

Composability is the ability to combine discrete IoT components into an IoT system to achieve a set of goals and objectives.

7.3.1.2 Relevance to IoT systems

System integration, interoperability and composability specify how the functional components are assembled to form a complete IoT system, how the functional components connect to each other and which binding mechanisms are used (e.g. dynamic or static, agent-based or peer-to-peer). Interoperability and composability are important topics in both the cyber and physical spaces. Composability imposes more stringent requirements than interoperability, in that it requires components not only compatible in their interfaces, but exchangeable with other components of the same kind. At a minimum these components share similar construction and improved characteristics such as timing, performance, scalability and security. When a component is replaced by another of the same kind that is compatible, the overall system functions and characteristics should at a minimum remain unchanged, but consideration can be given to permitting improvements in system functions and characteristics.

7.3.1.3 Examples

One example of composability is a temperature sensor in a building office with well-defined capabilities and a standardized service interface. The temperature sensor can be composed into the building heating, ventilation and air conditioning (HVAC) system for use in controlling the room and building temperature. In the event of a fire emergency in the building, this sensor could also be composed into an emergency response system providing the first responders with data on rooms affected by fire.

A second level of composability (or possibly interoperability) might be an IoT controller that is vendor-specific at the interface between the IoT component and a physical process device being controlled (a valve, motor, switch, pump or fan, for example), but is still fully interchangeable at the interface between the IoT device and the rest of the IoT system. In this example, the IoT device would serve as a kind of “middleware” between the vendor-agnostic IoT infrastructure, and the vendor-specific physical devices or mechanisms being controlled.

7.3.2 Functional and management capability separation

7.3.2.1 Description

Separation of functional and management capabilities means that the functional interfaces and capabilities of an IoT component, such as an IoT device, are cleanly separated from the management interfaces and capabilities of that component. This typically means that the management interface is on a different endpoint from that of the functional interface and the

management capabilities are handled by different software components than the functional interfaces.

7.3.2.2 Relevance to IoT systems

Management capabilities and functional capabilities logically differ as follows:

- purposes (execution/action vs information/description);
- user roles (control and modify behaviour vs transfer or consume facts and information);
- classifications and types of data (technical or system-specific vs personal/sensitive/public);
- access (e.g. an operator can access system configuration, but not gathered personal data; while the user can access the personal data but not access and modify system configuration);
- protocols, formats and life cycles (e.g. support multiple control protocols vs metadata/structure of the transferred information, which is particularly important considering interoperability and co-existence of multiple versions and variants of management capabilities).

Usually, the differences in capabilities yield differences in risks and hence require distinct security (and other) controls, e.g. retention policy is applicable while dealing with functional data, but might not apply to management data, access control can be weaker for a user and stronger for an administrator).

Ubiquitous penetration of IoT into virtually all areas of life increases the attack surface, multiplying the number of potential attack targets and often rendering measures such as physical security controls ineffective. The key value of IoT – the connection of numerous edge components to each other and to IoT service components – increases security concerns, since adding a weak link makes the whole chain weak. Applications and systems previously running in well-protected data centres can become exposed to additional threats via connected IoT components.

Separation of management from functional capabilities enables or strengthens the ability to apply different authorization, authentication and protection mechanisms or constraints to management as opposed to functional capabilities. Broad sharing of data from an IoT system might be useful or desirable, and yet there are many circumstances where it is necessary to limit control of an IoT system or component to only a subset of the entities with which the data from that IoT system is shared.

7.3.2.3 Examples

If an IoT system is used to provide sensors and data for HVAC or other building management systems, it might be desirable to share data with other inter-related systems (alarms, access control, power management or auxiliary power, etc.), while still retaining management of the system to ensure system constraints are respected.

7.3.3 Heterogeneity

7.3.3.1 Description

A diverse set of components and Physical Entities of an IoT system that interact in various ways.

7.3.3.2 Relevance to IoT systems

IoT is typically cross-system, cross-product and cross-domain. Realizing the full potential of IoT requires interoperability between heterogeneous components and systems. This heterogeneity creates numerous challenges for the interconnected IoT systems.

7.3.3.3 Examples

A smart container using RFID tags for identity and related RFID sensors needs interworking of RFID systems and sensor network systems.

A second example of heterogeneity is a set of temperature sensors from different manufacturers and with different specifications, integrated into a single system.

There are various industrial communication technologies such as RAPIEnet, EtherCAT, EtherNet/IP, PROFINET, POWERLINK, CC-Link IE, Modbus/TCP, Fieldbus, Profibus, MTConnect, OPC, OPC-UA, OMG DDS, etc., which implies various heterogeneous combinations of communication in connected manufacturing equipment, monitoring, and control devices. A factory can consist of multiple production lines which are expanded as business revenues increase. This gradual expansion can increase the diversity of communication endpoints, and can ultimately increase the heterogeneity of the whole system.

7.3.4 Highly distributed systems

7.3.4.1 Description

Distributed systems are systems which, while being functionally integrated, consist of sub-systems which can be physically separated and remotely located from one another. These sub-systems are normally connected by a communication link (e.g. data bus).⁷

Note that the highly distributed systems are not necessarily stationary over time. Some systems, like RFID tracking, have a high degree of mobility for individual devices, leading to an ever-diversifying topology.

7.3.4.2 Relevance to IoT systems

IoT systems can span whole buildings, whole cities and even the globe. Wide distribution can also apply to data – which can be stored at the edge of the network, centrally, or both. Distribution can also apply to processing – some processing takes place centrally (in cloud services), but processing can also take place at the edge of the network, either in the IoT gateways or even within (more capable types of) sensors and actuators.

7.3.4.3 Examples

For Industry 4.0, production can comprise smart manufacturing systems with distributed assembly lines. These lines are stretched across multiple factories and closely integrated with remotely-located third party suppliers, logistics companies, market providers and customers, which is represented as horizontal integration.

7.3.5 Legacy support

7.3.5.1 Description

Legacy support is the concept that an IoT system might need to incorporate existing installed components, even where these components embody technologies that are no longer standard or approved. A service, protocol, device, system, component, technology, or standard that is outdated but which is still in current use can be incorporated into an IoT system.

7.3.5.2 Relevance to IoT systems

Support of legacy component integration and migration can be important, although when supporting legacy components, it is also important to ensure that the design of new

⁷ Source: ISO 3511-4:1985, 2.5.

components and systems does not unnecessarily limit future system evolution. To prevent prematurely stranding legacy investment, a plan for adaptation and migration of legacy systems is important. Care should be taken when integrating legacy components to ensure that security and other essential performance and functional requirements are met. Legacy components can increase risk and vulnerabilities. Since current technology becomes legacy technology in the future, it is important to have a process in place for managing legacy aspects of any given system. This is particularly crucial for IoT, where different connected devices can have very different life cycles and update schedules, often in concert with those of the physical and information systems they are integrated with.

7.3.5.3 Examples

One example of transition from legacy to future compatibility is the current slow rollover from IPv4 compliance to IPv6 compliance. The limits of the IPv4 address space and of the IPv4 protocol are known, and the transition to IPv6 is clearly the way of the future, but the varying pace of the transition, depending on the context, can be a complex topic. This transition is especially pertinent to IoT, given the enormous number of devices that are destined to be connected.

Many existing standards and application environments still assume and depend on IPv4; yet it is clear that continuing to use IPv4 forever is not a viable strategy. Contributing factors include the lack of sufficient address space, as well as the masquerading of multiple addresses behind a single IP address. The timing of a shift to IPv6 is organization-specific and depends on multiple factors.

7.3.6 Modularity

7.3.6.1 Description

Modularity is a property of components that can be combined to form larger systems of components. Modular components can be removed cleanly from a system and replaced with a module of similar size and with similar physical and logical interfaces.

7.3.6.2 Relevance to IoT systems

Modularity allows components to be combined in different configurations to form systems as needed. By focusing on standardized interfaces and not specifying the internal workings of each component, implementers have flexibility in the design of components and IoT systems.

7.3.6.3 Examples

An example of modularity in an IoT system might be a smart thermostat. Because the interface to an HVAC system and the interface to a larger IoT infrastructure could both be defined in compliance with open interface standards, there is nothing to prevent a thermostat from vendor A being replaced by one from vendor B. Furthermore, it is not important how the functionality of the device is implemented. Vendor A might provide the capability in the form of an application-specific integrated circuit (ASIC)-based state machine, while vendor B's design might be based on a microcontroller. As long as both devices perform the same functions in response to the same inputs, and they are both compliant with open standard interfaces without imposing any proprietary constraints, there is nothing to prevent one from being replaced by the other.

7.3.7 Network connectivity

7.3.7.1 Description

The concept of IoT entities having the capability of communicating with many other entities over a communications network is a core concept of IoT. This many-to-many relationship enables other IoT characteristics including composability, resilience, shareability, scalability, and discoverability while creating challenges in the areas of security, reliability, manageability, accuracy, real-time capability, privacy, and safety. In IoT systems, components communicate

with each other across network links. The connections between components are established using either wired or wireless media. Networked IoT devices that originate, route and terminate communications are described as (network) nodes. Endpoint network devices are the source or destination of all information in transit. Any IoT related networking communications protocol is layered onto more specific or more general communications protocols, down to the physical layer that directly deals with the transmission media at every network node.

7.3.7.2 Relevance to IoT systems

IoT systems rely on the ability to exchange information in a structured manner based upon multiple different but inter-networked connections – all within a physical, wired or wireless network. IoT devices are considered “networked” when one device is able to exchange information with other devices whether or not they have a direct connection to each other. IoT network structure can be static or dynamic and can have capabilities such as quality of service (QoS), resilience, encryption, authentication and authorization.

7.3.7.3 Examples

The scale of an IoT network can vary substantially, from local proximity networks connecting a handful of devices over a limited distance, to global scale networks operating at Internet scale and connecting very large numbers of devices and service components.

It is typical for the networks in IoT systems to be heterogeneous and connected to each other via gateways or equivalent components.

7.3.8 Scalability

7.3.8.1 Description

Scalability is the characteristic of a system to continue to work effectively as the size of the system, its complexity or the volume of work performed by the system is increased.

7.3.8.2 Relevance to IoT systems

IoT systems involve various elements such as devices, networks, services, applications, users, stored data, data traffic, and event reports. The amount of each of these elements can change over time and it is important that the IoT system continues to function effectively when the amounts increase.

7.3.8.3 Examples

One example of scalability is an increase in the number of sensor devices attached to an IoT system over a specific period of time. If a system changes from monitoring temperature sensors in a single building to monitoring temperature sensors on all buildings in a city there will be a significant increase in the volume of sensor data flowing in the system, in the volume of data being stored in databases, in the number of devices handled by the management system, and in the number of temperature readings processed by services and applications.

7.3.9 Shareability

7.3.9.1 Description

Shareability is the capacity of an individual component to be accessed and its resources allocated communally between multiple interconnected systems.

7.3.9.2 Relevance to IoT systems

Many IoT components are underutilized since a single system often uses only a fraction of a component's capabilities. Resources can be used more efficiently if functionality or outputs of components can be shared among multiple systems.

7.3.9.3 Examples

The motion detection capabilities of a lighting control system could be leveraged by the security system to increase the security systems capability.

Temperature sensing for heating control could be used by the security system for fire detection.

7.3.10 Unique identification

7.3.10.1 Description

Unique identification is the characteristic of an IoT system to unambiguously and repeatably associate the entities within the system with an individual name, code, symbol, or number, and to interact with the entities, or trace or control their activities, by referencing that name, code, symbol or number. These entities include the components of the IoT system itself, such as software components, sensors, actuators, and network components.

7.3.10.2 Relevance to IoT systems

It is essential that the entities in an IoT system can be distinguished from each other. This enables interoperability and global services across heterogeneous IoT systems. It is important for entities to be uniquely identifiable within a given context so that IoT systems can appropriately monitor and communicate with specific entities. Some devices can be hidden behind IoT gateways, or information consolidated to protect privacy (e.g. see ISO/IEC 15045-1). A variety of identification schemes can be supported in specific implementations of IoT systems to meet the application requirements.

7.3.10.3 Examples

IPv4 address, IPv6 address, MAC address, URI, and FQDNs are used as unique, unambiguous identification of network endpoints in Internet applications. Individual hardware devices, software, and other entities can have unique manufacturer's IDs, object identifiers, universally unique identifiers (OIDs, UUIDs) or other identifiers which similarly allow unique, unambiguous identification.

Physical Entities are often given labels in the form of radio frequency identification (RFID) tags, barcodes and their equivalents. These carriers can contain encoded identifiers that can be sensed by an IoT device. For humans, biometric information can be used to provide unique identification.

7.3.11 Well-defined components

7.3.11.1 Description

IoT entities are considered to be well-defined when an accurate description of their capabilities and characteristics is available, including any associated uncertainties. Capability information includes not only information about the specific component functionality, but configuration, communication, security, reliability and other relevant information.

7.3.11.2 Relevance to IoT systems

Many components are used to assemble an IoT system. They are typically discovered through an information system interface and the metadata associated with the component cannot be available because the component does not follow established standards or is incapable of storing metadata. Without understanding the capabilities of each component that will be used within a system it is difficult to understand whether the system meets its design goals.

7.3.11.3 Examples

An example of implementation of a well-defined component is: A particular IoT component is available with varying amounts of memory or support for various RF frequencies, waveforms and protocols. Such a device has a baseline information interface which all the variants make use of to inform other IoT components of the list of capabilities offered by the device. Once the devices' respective configurations have been exchanged, each device's software or applications can then self-adjust to take into account the capabilities of the other devices.

7.4 IoT system functional characteristics

7.4.1 Accuracy

7.4.1.1 Description

Accuracy is a characteristic of various elements in an IoT system:

Sensors make measurements on properties of the physical world. Accuracy of these sensors is the closeness of agreement between the measured values and the actual values of those properties.

Software services can make calculations based on input data. Consider some automated image processing software – examples include number plate recognition for vehicles or facial recognition to establish the identity of people in a scene. Such software can be said to have an accuracy expressed as a percentage with which the recognized number plate text matches the actual number plate text, or the percentage with which the recognized identity of an individual matches the actual identity of the person in the scene.

Actuators operating on the physical world translate digital commands into actions, and accuracy for actuators can be described in terms of the closeness of the actual physical world actions to those intended by the digital command. An example might be a robot arm, where a digital command intends to move the tip of the robot arm to a particular location in 3D space. Accuracy can be expressed by how closely the position of the actual tip of the robot arm matches that of the digital command.

Therefore, in some cases, accuracy can be expressed in terms of the deviation of a continuous quantity in the digital world from its value in the physical world. In other cases it can be expressed as the percentage of instances in which the digital output of a discrete value correctly matches the expected value (i.e. the percentage of correct values).

7.4.1.2 Relevance to IoT systems

An appropriate level of accuracy is essential to IoT system deployments and applications. Depending on the context, differing degrees of accuracy might be required.

7.4.1.3 Examples

In a medical or manufacturing context, it might be critical for an IoT device, application or system providing temperature information or control to be accurate to within a tenth of a degree, while in a home HVAC context, accuracy to plus or minus two degrees might be adequate.

7.4.2 Auto-configuration

7.4.2.1 Description

Auto-configuration is the automatic configuration of devices based on the interworking of predefined rules (associated algorithms based on data inputs). Auto-configuration includes automatic networking, automatic service provisioning and plug & play. Auto-configuration allows an IoT system to react to conditions and the addition and removal of components such as devices and networks. Auto-configuration needs security and authentication mechanisms to ensure that only authorized components can be auto-configured into the system. Security mechanisms need to be organized appropriately for each market segment.

7.4.2.2 Relevance to IoT systems

Auto-configuration is useful for large-scale IoT systems whose configurations change dynamically over time. Auto-configuration's promotion of faulty component elimination and timely maintenance greatly benefits users with demanding reliability requirements.

7.4.2.3 Examples

Examples of auto-configuring devices and protocols include Dynamic Host Configuration Protocol (DHCP), Zero Configuration Networking (Zeroconf™), Bonjour™, UPnP™ (ISO/IEC 29341 series), etc.⁸

7.4.3 Compliance

7.4.3.1 Description

Compliance is the characteristic of conforming to rules, such as those defined by a law, a regulation, a standard or a policy. IoT systems, services, components and applications can be deployed in circumstances which require adherence to a variety of laws, policies or regulations. Such support might be inherent in the IoT device or system, or might require specific configuration, programming, modification or extension to ensure compliance.

Additionally, there can be a range of varying granularity or levels of abstraction at which the regulations are applied or enforced.

7.4.3.2 Relevance to IoT systems

Regulations of relevance to IoT systems can take many forms, including regulations to assure interoperability, to mandate or constrain functionality or capability, to assess the ability of the IoT device or system to function in a certain usage context without causing damage, and to impose at least minimal balance between contribution to the collective good and self-interest on the part of system owners or operators.

7.4.3.3 Examples

Regulations which might apply to an IoT context include one or more of the following categories.

- 1) Safety regulations – These might include flight safety standards for IoT devices operating in aircraft, regulations covering the manufacture and sale of devices intended for consumer use in the home, regulations for automotive systems, or regulations for devices or systems used in a medical context.

⁸ Trademarks are given for the convenience of users of this document and do not constitute an endorsement by ISO or IEC.