International Telecommunication Union

ITU-T Y.4552/Y.2078

(02/2016)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Services, applications, computation and data processing

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Next Generation Networks – Frameworks and functional architecture models

Application support models of the Internet of things

Recommendation ITU-T Y.4552/Y.2078

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	**Y.4550–Y.4699**
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4552/Y.2078

Application support models of the Internet of Things

Summary

Recommendation ITU-T Y.4552/Y.2078 provides application support models of the Internet of things (IoT). This Recommendation describes the basis of IoT application support models: the configurable application support model, the adaptable application support model and the reliable application support model. These three application support models are described in functional view, implementation view and deployment view, in order to identify, respectively, the configurable capabilities, the adaptable capabilities and the reliable capabilities for support of IoT applications having some characteristic requirements.

This Recommendation describes the IoT configurable capabilities that extend the IoT basic capabilities specified in Recommendation ITU-T Y.4401/Y.2068 in order to enable the IoT applications to configure the IoT capabilities based on their characteristic requirements.

This Recommendation describes the IoT adaptable capabilities that extend the IoT basic capabilities specified in Recommendation ITU-T Y.4401/Y.2068 in order to enable the IoT applications to adapt to the IoT capabilities based on their characteristic requirements.

This Recommendation describes the IoT reliable capabilities that extend the IoT basic capabilities specified in Recommendation ITU-T Y.4401/Y.2068 in order to support the IoT applications by the IoT capabilities with required degrees of reliability for fulfilling their characteristic requirements.

Use cases from the smart home environment provide examples about the usage of the IoT application support models.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4552/Y.2078	2016-02-13	13	11.1002/1000/12707

Keywords

Adaptable capability, application support model, configurable capability, deployment view, functional view, implementation view, Internet of things (IoT), reliable capability, requirements.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Basis of IoT application support models	3
6.1	Concepts and purpose of IoT application support models	3
6.2	Rationale for the selection of the IoT applications support models	4
6.3	The three views of IoT application support models	5
7	The configurable application support model	5
7.1	The description of the configurable application support model	5
7.2	The capabilities of the configurable application support model	8
8	The adaptable application support model	12
8.1	The description of the adaptable application support model	13
8.2	The capabilities of the adaptable application support model	15
9	The reliable application support model	17
9.1	The description of the high reliable application support model	17
9.2	The capabilities of the reliable application support model	19
10	Security considerations	23
Annex A – The list of configurable capabilities for support of IoT applications		24
Annex B – The list of adaptable capabilities for support of IoT applications		34
Annex C – The list of reliable capabilities for support of IoT applications		38
Appendix I – Use cases for the IoT applications support models from the smart home environment		45
I.1	Use case 1: Configurable remote monitoring in a smart home	45
I.2	Use case 2: Adaptable home energy management	46
I.3	Use case 3: Reliable health monitoring at home	47
Bibliography		48

Recommendation ITU-T Y.4552/Y.2078

Application support models of the Internet of Things

1 Scope

This Recommendation describes basis of application support models of the Internet of things (IoT) and specifies three application support models of the IoT: the configurable application support model, the adaptable application support model and the reliable application support model.

The three application support models are specified in functional view, implementation view and deployment view respectively.

The configurable capabilities, adaptable capabilities and reliable capabilities related, respectively, to each of the three models, are also identified and described.

The scope of this Recommendation includes:

- The basis of application support models;
- The functional view, the implementation view and the deployment view of the configurable application support model and related configurable capabilities that extend the IoT basic capabilities specified in [ITU-T Y.4401] to enable the IoT applications to configure the IoT capabilities based on their characteristic requirements;
- The functional view, the implementation view and the deployment view of the adaptable application support model and related adaptable capabilities that extend the IoT basic capabilities specified in [ITU-T Y.4401] to enable the IoT applications to adapt to the IoT capabilities based on their characteristic requirements;
- The functional view, the implementation view and the deployment view of the reliable application support model and related reliable capabilities that extend the IoT basic capabilities specified in [ITU-T Y.4401] to support the IoT applications by the IoT capabilities with required degrees of reliability for fulfilling their characteristic requirements.

All capabilities identified and specified in this Recommendation are numbered and summarized in the annexes.

Appendix I shows three use cases of the IoT application support models from the smart home environment.

NOTE – Only three IoT application support models are described and specified in this Recommendation. The specification of other application support models is outside the scope of this Recommendation and for further consideration.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things.*

[ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 application domain [ITU-T Y.4100]: An area of knowledge or activity applied for one specific economic, commercial, social or administrative scope.

NOTE – Transport application domain, health application domain and government application domain are examples of application domains.

3.1.3 device [ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.4 functional entity [b-ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.5 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.6 thing [ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IoT Internet of Things

M2M Machine-to-Machine

QoS Quality of Service

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Basis of IoT application support models

6.1 Concepts and purpose of IoT application support models

The IoT application support models refer to different sets of the IoT capabilities, including their relations, which can support IoT applications with some characteristic requirements, such as application adaptability, reliability and manageability.

NOTE 1 – The application characteristic requirements, as named in this Recommendation, are part of the common requirements as specified in [ITU-T Y.4100]. The application characteristic requirements refer to requirements related with some characteristics of IoT applications, such as the adaptability of M2M applications, the reliability of e-health applications and the configurability of smart city applications.

The IoT application support models are used to guide the design, implementation and deployment of the IoT capabilities to fulfil application characteristic requirements, in order to establish a common service platform [ITU-T Y.4401] for support of IoT applications across different application domains.

NOTE 2 – The service platform established by implementing and deploying capabilities of the IoT application support models may be used to shorten the time period and reduce the cost of developing the IoT applications with characteristic requirements, such as configurable, adaptable, or reliable requirements, by making usage of the capabilities of the service platform. Appendix I describes some use cases from the smart home environment showing examples about the usage of the IoT application support models.

In particular, the purposes of the IoT application support models are as follows: the first one is to specify groups of IoT capabilities in order to facilitate the selection of IoT capabilities [ITU-T Y.4401] for the support of IoT applications with some characteristic requirements; the second one is to derive, based on the selected IoT capabilities, other IoT capabilities, not explicitly identified in [ITU-T Y.4401], as necessary in order to facilitate the design, implementation and deployment of the IoT capabilities for support of IoT applications with some characteristic requirements.

In this Recommendation, the framework of the IoT application support models and three specific application support models: the adaptable application support model, the reliable application support model and the configurable application support model, are specified. Clause 6.2 provides the rationale for this classification of the IoT application support models.

NOTE 3 –This Recommendation specifies only three application support models. Because of different IoT application characteristic requirements, different IoT application support models could be specified. Other application support models are for further consideration with respect to other relevant characteristic requirements of IoT applications.

The configurable application support model refers to the set of IoT capabilities, including their relations, to support the IoT applications with the characteristic requirement of configurability. The

configurable application support model includes the IoT capabilities that can be configured by IoT applications, such as some service capabilities and communication capabilities that are related with the IoT applications.

The reliable application support model refers to the set of IoT capabilities, including their relations, to support the IoT applications with the required degrees of reliability. The reliable application support model includes the IoT capabilities that can enhance the reliability of IoT applications, such as reliable data communication capability.

The adaptable application support model refers to the set of IoT capabilities, including their relations, to support the IoT applications with the characteristic requirement of adaptability. The adaptable application support model includes the IoT capabilities that are adaptable to different application contexts, such as content awareness capability and context awareness capability.

6.2 Rationale for the selection of the IoT applications support models

Regarding the possible diverse classifications that can be considered for IoT applications, different classes for a given classification may require different application support models.

One possible classification of IoT applications is based on the characteristics of things, characteristics of IoT users and other functional characteristics of IoT.

The characteristics of things may include mobility, intelligent ability, etc. The characteristics of IoT users may include mobility, non-human operated, etc. Other functional characteristics of IoT may include content awareness, context awareness, etc.

NOTE 1 – For example, the IoT applications in support of things with mobility belong to the category of mobile thing applications of IoT; the IoT applications in support of things with intelligent ability belong to the category of smart thing applications of IoT; the IoT applications in support of non-human operated users of IoT belong to the category of IoT applications with non-human operators.

This classification of IoT applications may be too diverse to derive common application support models usable across different application domains. So this classification of IoT applications is not suitable as the basis to describe the IoT application support models.

Another classification of IoT applications is based on the non-functional requirements of IoT applications as specified in [ITU-T Y.4100], such as reliability, availability, manageability and adaptability. Based on this classification, IoT applications can be classified into reliable applications, manageable applications, adaptable applications, etc. Even if there are some differences among these non-functional requirements across different application domains, these differences consist in the absence of certain requirements in given application domain(s), or in the different strengths of certain requirements to be satisfied at the implementation and deployment level. So the application support models derived from this IoT application classification can be used across different application domains. This classification of IoT applications is suitable as the basis to describe the three IoT application support models specified in this Recommendation.

NOTE 2 – The three IoT application support models are related with several practical IoT applications, such as M2M applications, e-health applications and smart city applications. The configurable application support model specified in this Recommendation may be used to support smart city applications because these applications may address different application domains and require different configurations in these different domains. The adaptable application support model specified in this Recommendation may be used to support M2M applications because these applications usually require being able to adapt to different networking or application environments. The reliable application support model specified in this Recommendation may be used to support e-health applications because the e-health applications usually require high reliable networking and service provisioning.

6.3 The three views of IoT application support models

The three views of an IoT application support model consists of the functional view, the implementation view and the deployment view for support of the identified IoT applications with some characteristic requirements.

The functional view consists of the functional groups, including their relations, which support the identified applications.

NOTE 1 – This functional view is based on the functional view of the IoT framework that is specified in [ITU-T Y.4401].

The implementation view consists of the functional entities, including their relations, which support the identified applications.

NOTE 2 – This implementation view is based on the implementation view of the IoT framework that is specified in [ITU-T Y.4401].

The deployment view consists of the functional components, including their relations, which support the identified applications.

NOTE 3 – This deployment view is based on the deployment view of the IoT framework that is specified in [ITU-T Y.4401].

NOTE 4 – Based on the three views of the IoT application support models, some IoT application support capabilities can be derived for support of the IoT applications with some characteristic requirements.

NOTE 5 – The IoT application support capabilities derived from the three views of the IoT application support models are aligned with and extend the IoT capabilities specified in [ITU-T Y.4401] in order to fulfill some characteristic requirements of the IoT applications. The three views of the IoT application support models can identify the IoT application support capabilities required in the stages of designing, implementing and deploying the IoT applications.

7 The configurable application support model

The configurable application support model consists of the functional view, implementation view and deployment view and related capabilities.

NOTE – The three views of application support model can be used to derive and validate the capabilities for support of configurable applications of the IoT.

7.1 The description of the configurable application support model

7.1.1 The functional view of the configurable application support model

The functional view of the configurable application support model consists of a configurable management group, a configurable security and privacy protection group, a configurable data management group, a configurable service provision, a configurable communication group, a configurable connectivity group and a configurable application support group and the interactions among these groups as illustrated in Figure 7-1. Each functional group contains related capabilities for support of the IoT configurable applications.

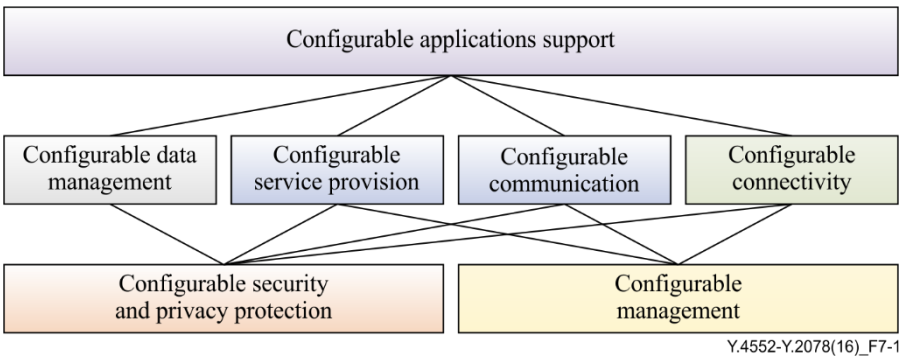

Figure 7-1 – The functional view of the configurable application support model

The configurable security and privacy protection group is related to the configurable data management group, the configurable service provision group, the configurable communication group and the configurable connectivity group, which refer to the fact that the other functional groups rely on the security and privacy protection capabilities specified in this functional group to protect their configurable capabilities for support of IoT applications.

The configurable management group is related to the configurable service provision group, the configurable communication group and the configurable connectivity group to provide required management capabilities.

The data management group has its own management capabilities, because configurable data management capabilities depend on data models. By ensuring the management of the data models by the data management group's own management capabilities, configuration management can be simplified.

The security and privacy protection group also has its own configurable management capabilities in order to prevent any possible intrusion or attack from external configuration management.

The configurable application support group is related to the configurable data management group, the configurable service provision group, the configurable communication group and the configurable connectivity group to allow the exposure of the configurable capabilities contained in these functional groups to IoT applications.

NOTE 1 – The functional view of the configurable application support model can be used to identify the functional groups related to the configurable capabilities for support of IoT applications.

NOTE 2 – In the functional view of the configurable application support model, there is no interaction among the configurable data management group, the configurable service provision group, the configurable communication group and the configurable connectivity group, because each of these functional groups does not need to interact with others to provide configurable capabilities.

7.1.2 The implementation view of the configurable application support model

The implementation view of the configurable application support model consists of a configurable management and identity management entity, a configurable IoT security and privacy protection entity, a configurable IoT gateway entity, a configurable end-user device entity, a configurable transport control entity, a configurable IoT transport control entity, a configurable service control entity, a configurable IoT service control entity, a configurable IoT data management entity and a configurable application support entity and the interactions among these entities as illustrated in Figure 7-2.

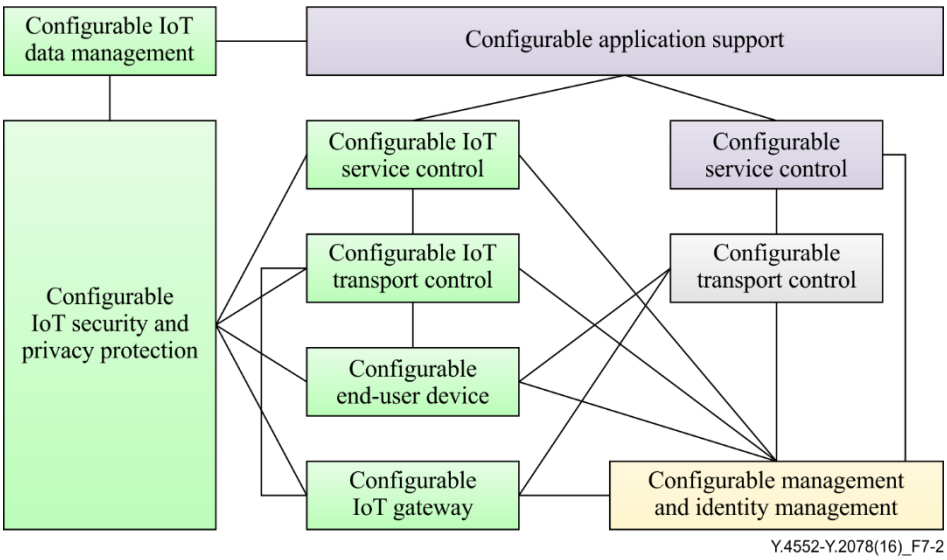

Figure 7-2 – The implementation view of the configurable application support model

The configurable management and identity management entity is related to the configurable IoT gateway entity, the configurable end-user device entity, the configurable transport control entity, the configurable IoT transport control entity, the configurable service control entity and the configurable IoT service control entity, in order to provide the required management capabilities for these functional entities.

The IoT security and privacy protection entity is related to the configurable IoT gateway entity, the configurable end-user device entity, the configurable IoT transport control entity, the configurable IoT service control entity and the configurable IoT data management entity, in order to provide the required IoT related security and privacy protection capabilities for these functional entities.

The configurable transport control entity is related to the configurable IoT gateway entity and the configurable end-user device entity in order to provide configurable transport capabilities for these functional entities. The configurable IoT transport control entity is related to the configurable IoT gateway entity and the configurable end-user device entity in order to provide configurable IoT related transport capabilities for these functional entities.

The configurable service control entity is related to the configurable transport control entity in order to expose the configurable transport control capabilities in the configurable service control entity. The configurable IoT service control entity is related to the configurable IoT transport control entity in order to allow the exposure of the configurable IoT related transport control capabilities in the configurable IoT service control entity.

The configurable application support entity is related to the configurable IoT data management entity, the configurable IoT service control entity and the configurable service control entity, in order to allow the exposure of all configurable capabilities specified in clause 7.2 by the application support entity specified in [ITU-T Y.4401].

7.1.3 The deployment view of the configurable application support model

The deployment view of the configurable application support model consists of the configurable device manager component, the configurable IoT gateway component, the configurable end-user device component, the configurable network manager component, the configurable IoT network controller component, the configurable service manager component, the configurable IoT service controller component, the configurable IoT data server component and the configurable service platform component and the interactions among these components as illustrated in Figure 7-3.

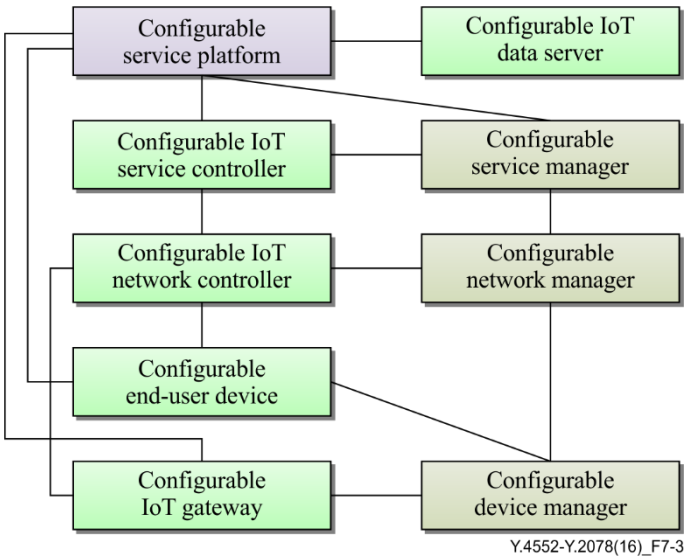

Figure 7-3 – The deployment view of the configurable application support model

The configurable service platform component is related to the configurable IoT data server component to enable the configurable capabilities for support of the IoT applications to be configured with different requirements on data of things. The configurable service platform component interacts with the configurable service manager component and the configurable IoT service controller component to enable the configurable capabilities for support of the IoT applications with different requirements of service provisioning, such as service creation or service customization.

The configurable service platform component is related to the configurable end-user device to enable the configurable capabilities for support of the IoT applications to be configured with different requirements of end-users. The configurable service platform component is related to the configurable IoT gateway component to enable the configurable capabilities for support of the IoT applications to be configured with different requirements of IoT devices, such as different ways of capturing and transferring data of things.

The configurable IoT network controller component is related to the configurable end-user device component and the configurable IoT gateway component to enable the configurable capabilities for support of the IoT applications with different network requirements.

The configurable network manager component is related to the configurable service manager component and the configurable device manager component to enable the configurable capabilities for support of the IoT applications to be configured across all functional layers of IoT, such capturing, buffering, transferring and analysing the data of things.

7.2 The capabilities of the configurable application support model

Based on the categories of the IoT basic capabilities specified in [ITU-T Y.4401] and the description of the configurable application support model specified in clause 7.1, the capabilities of the configurable application support model can be classified into the following groups: the configurable service provision capabilities, the configurable communication capabilities, the configurable data management capabilities, the configurable connectivity capabilities, the configurable management capabilities, the configurable application support capabilities and the configurable security and privacy protection capabilities.

The capabilities of the configurable application support model are specified from the perspective of configurable application support components as described in the deployment view of the

configurable application support model in clause 7.1.3 because these capabilities are implemented, deployed and used in these configurable application support components.

The following clauses describe, respectively, these capabilities of the configurable application support model. These same capabilities are numbered and summarized in Annex A.

NOTE – In the following clauses, the capability numbers, as shown in Annex A, are put between square brackets "[ ]" and inserted at the end of the description of the corresponding capability.

7.2.1 Configurable service provision capabilities

The configurable service provision capabilities extend the service provision capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to enable IoT applications to configure the IoT service provision capabilities based on their requirements.

The configurable service provision capabilities include the configurable service prioritization capability, the configurable service composition capability and the configurable location based and context-aware service capability.

The configurable service prioritization capability enables the IoT applications to configure services with different priorities, in order to provide differentiated services based on their requirements [A-1-1].

The configurable service composition capability enables the IoT applications to configure service creation or service customization based on their requirements [A-1-2].

The configurable location based and context-aware service capability enables the IoT applications to configure services that are provided both on the location information and related context and on the predefined rules or policies, in order to fulfil their requirements [A-1-3].

7.2.2 Configurable communication capabilities

The configurable communication capabilities extend the communication capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to enable IoT applications to configure the IoT communication capabilities based on their requirements.

The configurable communication capabilities include the configurable event-based communication capability, the configurable periodic communication capability, the configurable communication mode capability, the configurable quality of service (QoS) communication capability, the configurable content-aware communication capability and the configurable location based communication capability.

The configurable event-based communication capability enables the IoT applications to configure different events in order to initiate communication based on the requirements of the IoT applications [A-2-1].

The configurable periodic communication capability enables the IoT applications to configure the rules in order to periodically initiate communication based on the requirements of the IoT applications [A-2-2].

The configurable communication mode capability enables the IoT applications to configure different modes of communications in the transport network in order to transfer data from the source(s) to the destination(s) based on the requirements of the IoT applications [A-2-3].

The configurable quality of service communication capability enables the IoT applications to configure the related mechanisms in order to guarantee the QoS required for the delivery and processing of data (e.g., time-sensible data) based on the requirements of the IoT applications [A-2-4].

The configurable content-aware communication capability enables the IoT applications to configure the parameters related to the content and selected path for routing or blocking data transfer based on the requirements of the IoT applications [A-2-5].

The configurable location based communication capability enables the IoT applications to configure the parameters related to the locations and predefined rules in order to initiate communication based on the requirements of the IoT applications [A-2-6].

7.2.3 Configurable data management capabilities

The configurable data management capabilities extend configurable capabilities to the data management capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to enable IoT applications to configure the IoT data management capabilities based on their requirements.

The configurable data management capabilities include the configurable data storage capability, the configurable data processing capability, the configurable information exchange capability, the configurable semantic data operation capability and the configurable autonomic data operation capability.

The configurable data storage capability enables the IoT applications to configure the rules or the policies for storing data based on the requirements of the IoT applications [A-3-1].

The configurable data processing capability enables the IoT applications to configure the rules or the policies for processing data based on the requirements of the IoT applications [A-3-2].

The configurable information exchange capability enables the IoT applications to configure the parameters for sending data to or receiving data from external data sources, e.g., data centres and data servers outside the IoT based on the requirements of the IoT applications [A-3-3].

The configurable semantic data operation capability enables the IoT applications to configure the parameters for semantic annotating, semantic discovering, semantic storing and semantic composition of data of things based on the requirements of the IoT applications [A-3-4].

The configurable autonomic data operation capability enables IoT applications to configure the parameters for automatically collecting, aggregating, transferring, storing, analyzing data of things, as well as automatically managing these data operations based on the requirements of the IoT applications [A-3-5].

7.2.4 Configurable connectivity capabilities

The configurable connectivity capabilities extend the connectivity capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to enable IoT applications to configure the IoT communication capabilities based on their requirements.

The configurable connectivity capabilities include the configurable identification based connectivity capability, the configurable things' status notification capability, the configurable device mobility capability and the configurable and adaptable connectivity capability.

The configurable identification based connectivity capability enables the IoT applications to configure the parameters for connectivity establishment based on the identification of things and the requirements of the IoT applications [A-4-1].

The configurable things' status notification capability enables the IoT applications to configure the rules of automatic notification of the status of things and its changes based on the requirements of the IoT applications [A-4-2].

The configurable device mobility capability enables the IoT applications to configure the parameters for maintaining the connectivity with the IoT when end-user devices or IoT gateways are moving, based on the requirements of the IoT applications [A-4-3].

The configurable and adaptable connectivity capability enables the IoT applications to configure the parameters for extending connectivity configurations in order to connect with different types of devices of the IoT based on the requirements of the IoT applications, in order to be adaptable to different technologies in devices of IoT [A-4-4].

7.2.5 Configurable security and privacy protection capabilities

The configurable security and privacy protection capabilities extend the security and privacy protection capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to enable IoT applications to configure the IoT security and privacy protection capabilities based on their requirements.

The configurable security and privacy protection capabilities include the configurable communication security capability, the configurable data management security capability, the configurable service provision security capability, the configurable security integration capability and the configurable mutual authentication and authorization capability.

The configurable communication security capability enables IoT applications to configure the rules and policies for supporting secure, trusted and privacy protected communication based on the requirements of IoT applications [A-5-1].

The configurable data management security capability enables the IoT applications to configure the rules and policies for providing secure, trusted and privacy protected data management based on the requirements of the IoT applications [A-5-2].

The configurable service provision security capability enables the IoT applications to configure the rules and policies for providing secure, trusted and privacy protected service provision based on the requirements of the IoT applications [A-5-3].

The configurable security integration capability enables the IoT applications to configure the rules and policies for enabling integration of different security policies and techniques related to the IoT functional components based on the requirements of the IoT applications [A-5-4].

The configurable mutual authentication and authorization capability enables the IoT applications to configure the rules and policies for authenticating and authorizing IoT applications and devices before a device accesses IoT based on the requirements of the IoT applications [A-5-5].

7.2.6 Configurable application support capabilities

The configurable application support capabilities extend the application support capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to enable IoT applications to configure the IoT application support capabilities based on their requirements.

The configurable application support capabilities include the configurable group management capability, the configurable time synchronization capability, the configurable orchestration capability and the configurable application support operation acknowledgement capability.

The configurable group management capability enables the IoT applications to configure the parameters for creating, modifying, deleting and querying IoT groups, as well as adding, modifying, deleting and querying IoT group members, based on the requirements of the IoT applications [A-6-1].

The configurable time synchronization capability enables the IoT applications to configure the parameters for synchronizing the time among related functional components with different degrees of reliability, in order to support global or local time stamping for applications based on the different QoS requirements of the IoT applications [A-6-2].

The configurable orchestration capability enables the IoT applications to configure the parameters for automatic coordination of service provisioning or device operations based on the requirements of the IoT applications [A-6-3].

The configurable application support operation acknowledgement capability enables the IoT applications to configure the parameters for acknowledging the correct operations requested by applications in order to support reliable application operations in the IoT, based on the requirements of the IoT applications [A-6-4].

7.2.7 Configurable management capabilities

The configurable management capabilities enhance the management capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to enable IoT applications to configure the IoT management capabilities based on their requirements.

The configurable management capabilities include the configurable redundant deployment enablement capability, the configurable service integrity check capability, the configurable data integrity check capability, the configurable device integrity check capability, the configurable security integrity check capability and the configurable user profile integrity check capability.

The configurable redundant deployment enablement capability enables the IoT applications to configure deployment of redundant functional components of the IoT in order to provide different degrees of reliability required in communication, service provision and data management, based on the requirements of the IoT applications [A-7-1].

The configurable service integrity check capability enables the IoT applications to configure the parameters for checking the service lifetime, the available resources required to provide the service in order to provide different degrees of availability in service provisioning, based on the requirements of the IoT applications [A-7-2].

The configurable data integrity check capability enables the IoT applications to configure the parameters for checking the data lifetime, the available attributes of the data and the consistency of data in order to provide different degrees of availability in data management, based on the requirements of the IoT applications [A-7-3].

The configurable device integrity check capability enables the IoT applications to configure the parameters for checking the status of all device functions in order to provide different degrees of availability of IoT devices, based on the requirements of the IoT applications [A-7-4].

The configurable security integrity check capability enables the IoT applications to configure the parameters for checking the consistency of security policies deployed in all functional components of the IoT in order to provide different degrees of availability in security and privacy protection provisioning, based on the requirements of the IoT applications [A-7-5].

The configurable user profile integrity check capability enables the IoT applications to configure the parameters for checking the lifetime, subscription, privacy protection and availability of services subscribed by users in order to provide different degrees of availability in service provisioning and privacy protection for users, based on the requirements of the IoT applications [A-7-6].

8 The adaptable application support model

The adaptable application support model consists of the functional view, implementation view and deployment view and related capabilities.

NOTE 1 – The three views of the application support model can be used to derive and validate the capabilities for support of adaptable applications of the IoT.

NOTE 2 – "Adaptable" capabilities in this Recommendation refer to capabilities that can adjust themselves to make them suitable to their operating environment, including requirements of the IoT applications.

8.1 The description of the adaptable application support model

8.1.1 The functional view of the adaptable application support model

The functional view of the configurable application support model consists of the adaptable application support group, the adaptable data management group, the adaptable service provision group, the adaptable communication group, the adaptable connectivity group and the interactions among these groups as illustrated in Figure 8-1. Each functional group contains related capabilities for support of the IoT adaptable applications. Each functional group contains related capabilities for support of the IoT adaptable applications.

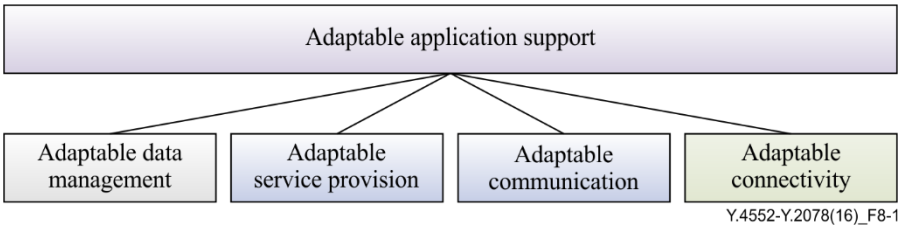

Figure 8-1 – The functional view of the adaptable application support model

The adaptable application support group is related to the adaptable data management group, the adaptable service provision group, the adaptable communication group and the adaptable connectivity group to expose their adaptable capabilities to the IoT applications.

NOTE – Neither the adaptable management group nor the adaptable security and privacy protection group are specified in the functional view of the adaptable application support model, because the functions both in management group and in security and privacy protection group are not adaptable. The management group contains capabilities that can manage the capabilities of the adaptable application support model based on policies or rules predefined by human operators, in order to make these adaptable capabilities controllable by humans, the adaptable application support model does not contain capabilities of the management group.

The security and privacy protection group contains capabilities that can secure the capabilities of the adaptable application support model and protect privacy in these adaptable capabilities based on the policies or rules predefined by human operators, in order to make these adaptable capabilities secured and privacy-protected strictly by humans, the adaptable application support model does not contain capabilities of the security and privacy protection group.

8.1.2 The implementation view of the adaptable application support model

The implementation view of the adaptable application support model consists of the adaptable IoT gateway entity, the adaptable end-user device entity, the adaptable transport control entity, the adaptable IoT transport control entity, the adaptable service control entity, the adaptable IoT service control entity, the adaptable IoT data management entity, the adaptable applications support entity and the interactions among these entities as illustrated in Figure 8-2.

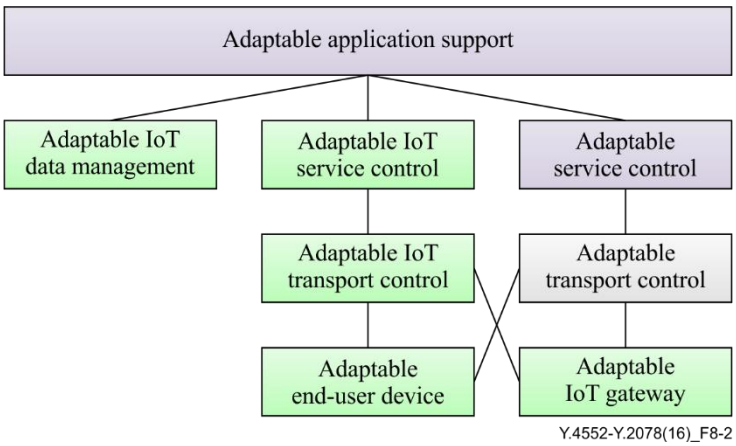

Figure 8-2 – The implementation view of the adaptable application support model

The adaptable application support entity is related to the adaptable IoT data management entity, the adaptable IoT service control entity and the adaptable service control entity, in order to allow exposure of their adaptable capabilities that can be accessed by IoT applications.

The adaptable IoT transport control entity is related to the adaptable end-user device entity and the adaptable IoT gateway entity in order to provide capabilities of adaptable communication and adaptable connectivity to fulfil adaptable requirements of IoT, such as adaptable event-based communication and adaptable identification-based connectivity.

The adaptable transport control entity is related to the adaptable end-user device entity and the adaptable IoT gateway entity in order to provide capabilities of adaptable communication and adaptable connectivity to fulfil general adaptable requirements, such as adaptable QoS enabling communication and adaptable device mobility.

The adaptable IoT transport control entity is related to the adaptable IoT service control entity in order to fulfil adaptable communication or connectivity requirements of IoT. The adaptable transport control entity is related to the adaptable service control entity in order to support IoT-independent adaptable communication or connectivity capabilities.

8.1.3 The deployment view of the adaptable application support model

The deployment view of the adaptable application support model consists of the adaptable IoT gateway component, the adaptable end-user device component, the adaptable IoT network controller component, the adaptable IoT service controller component, the adaptable IoT data server component, the adaptable service platform component and the interactions among these components as illustrated in Figure 8-3.

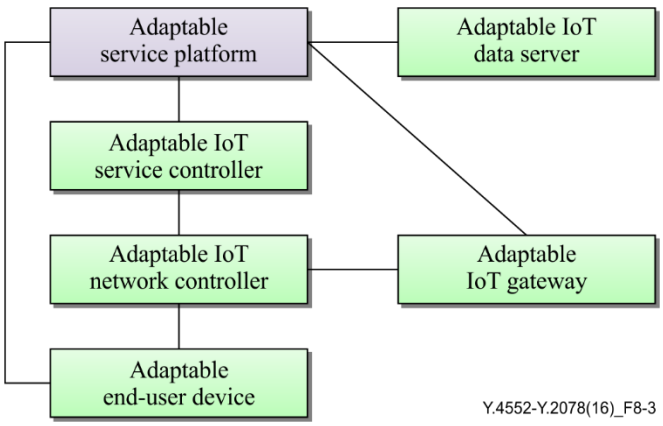

Figure 8-3 – The deployment view of the adaptable application support model

The adaptable service platform component is related to the adaptable end-user device component and the adaptable IoT gateway component in order to provide IoT-dependent adaptable application support capabilities, such as adaptable group management and adaptable orchestration capabilities.

NOTE – It is assumed that some capabilities contained in an adaptable service platform are deployed both in the adaptable end-user device component and in the adaptable IoT gateway component.

The adaptable service platform component is related to the adaptable IoT data server component in order to provide adaptable data management capabilities to IoT applications, such as the adaptable data processing capability.

The adaptable service platform component is related to the adaptable IoT service controller component in order to provide adaptable service provision capabilities to IoT applications, such as the adaptable service prioritization capability.

8.2 The capabilities of the adaptable application support model

Based on the categories of the IoT basic capabilities specified in [ITU-T Y.4401] and the functional view of the adaptable application support model specified in clause 8.1, the capabilities of the adaptable application support model can be classified into the following functional groups: adaptable service provision capabilities, adaptable communication capabilities, adaptable application support capabilities, adaptable data management capabilities and adaptable connectivity capabilities.

The capabilities of the adaptable application support model are specified from the perspective of the adaptable application support components as described in the deployment view of the adaptable application support model in clause 8.1.3, because these capabilities are implemented, deployed and used in these adaptable application support components.

NOTE 1 – IoT semantic capability is included in the capabilities of the adaptable application support model. IoT semantic capability facilitates the adaptable application support model's understanding of the meaning of IoT applications' service requests based on semantics.

NOTE 2 – The capability exposure capability is included in the capabilities of the adaptable application support model, specifically in the adaptable application support group. The capability exposure capability enables capabilities of the adaptable application support model to be discovered by IoT applications.

The following clauses describe, respectively, these capabilities of the adaptable application support model. These same capabilities are numbered and summarized in Annex B.

NOTE 3 – In the following clauses, the capability numbers, as shown in Annex B, are put between square brackets "[ ]" and inserted at the end of the description of the corresponding capability.

8.2.1 Adaptable service provision capabilities

The following IoT basic capabilities specified in [ITU-T Y.4401] provide adaptable service support abilities to IoT applications. They are part of the adaptable service provision capabilities of the IoT adaptable application support model. These capabilities include:

- Semantic based service capability, numbered as C-1-2 in [ITU-T Y.4401];
- Autonomic service capability, numbered as C-1-5 in [ITU-T Y.4401];
- Location based and context-aware service capability, numbered as C-1-6 in [ITU-T Y.4401]; and
- Adaptable service provision capability, numbered as C-1-11 in [ITU-T Y.4401].

In addition to the above capabilities, the following capabilities are part of the adaptable service provision capabilities.

The adaptable service prioritization capability enables the adaptable service platform and the adaptable IoT service controller to adjust services priorities, in order to adapt to differentiated services requirements from the IoT applications based on predefined rules [B-1-1].

The adaptable service composition capability enables the adaptable service platform and the adaptable service manager to adjust service creation or service customization based on the requirements of the IoT applications and predefined rules [B-1-2].

The adaptable mobility service capability enables the adaptable service platform and the adaptable service manager to adjust the mechanisms of remote service access, remote user authentication and remote service execution based on predefined rules [B-1-3].

8.2.2 Adaptable communication capabilities

The following IoT basic capabilities specified in [ITU-T Y.4401] provide adaptable communication abilities to IoT applications. They are part of the adaptable communication capabilities of the IoT adaptable application support model. These capabilities include:

- Content-aware communication, numbered as C-2-13 in [ITU-T Y.4401];
- Location-based communication, numbered as C-2-14 in [ITU-T Y.4401]; and
- Adaptable networking, numbered as C-2-16 in [ITU-T Y.4401].

In addition to the above capabilities, the following capabilities are part of the adaptable communication capabilities.

The adaptable event-based communication capability enables the adaptable service platform, the adaptable end-user devices and the adaptable IoT gateways to adjust the events for initiating communication based on predefined rules [B-2-1].

The adaptable quality of service enabling communication capability enables the adaptable network controller, the adaptable end-user devices and the adaptable IoT gateways to adjust the mechanisms according to current network status and predefined rules in order to guarantee the QoS required for the delivery and processing of data (e.g., time-sensible data) [B-2-2].

8.2.3 Adaptable application support capabilities

In addition to exposing the capabilities to IoT applications from other functional groups of the adaptable application support model, the following capabilities should be added in the adaptable application support capabilities.

The adaptable group management capability enables the adaptable service platform to create, modify, delete and query IoT groups, as well as to add, modify, delete and query IoT group members based on the requirements of the IoT applications and predefined rules [B-3-1].

The adaptable orchestration capability enables the adaptable service platform, the adaptable end-user devices and the adaptable IoT gateways to dynamically coordinate service provisioning based on the requirements of the IoT applications and predefined rules [B-3-2].

8.2.4 Adaptable data management capabilities

The following IoT basic capabilities specified in [ITU-T Y.4401] provide adaptable data management abilities to IoT applications. They are part of the adaptable data management capabilities of the IoT adaptable application support model. These capabilities include:

- Semantic data operation, numbered as C-4-6 in [ITU-T Y.4401]; and
- Autonomic data operation, numbered as C-4-7 in [ITU-T Y.4401].

In addition to the above capabilities, the following capabilities are part of the adaptable data management capabilities.

The adaptable data processing capability enables the adaptable IoT data server to adjust methods of data fusion and mining based on the IoT application requirements and predefined rules [B-4-1].

The adaptable information exchange capability enables the adaptable IoT data server to send data to or receive data from external data sources, e.g., data centres and data servers outside the IoT, based on the IoT application requirements and predefined rules [B-4-2].

8.2.5 Adaptable connectivity capabilities

The following IoT basic capability specified in [ITU-T Y.4401] provides adaptable connectivity abilities to IoT applications. The following capability is part of the adaptable connectivity capabilities of the IoT adaptable application support model:

− Adaptable connectivity, numbered as C-6-4 in [ITU-T Y.4401].

In addition to the above capability, the following capabilities are part of the adaptable connectivity capabilities:

The adaptable identification based connectivity capability enables the adaptable network manager, the adaptable end-user devices and the adaptable IoT gateways to dynamically choose the mechanisms for establishing the connectivity based on the identification of things and predefined rules [B-5-1].

The adaptable device mobility capability enables the adaptable network manager, the adaptable end-user devices and the adaptable IoT gateways to dynamically negotiate the mechanisms for keeping connectivity when the adaptable end-user devices or the adaptable IoT gateways are moving based on predefined rules [B-5-2].

9 The reliable application support model

The reliable application support model consists of the functional view, implementation view and deployment view of descriptions on the reliable application support model and related capabilities.

NOTE 1 – The three views of application support model can be used to derive and validate the capabilities for support of reliable applications of the IoT.

NOTE 2 – The degrees of reliability that may be realized in an IoT implementation will depend on application requirements and resource management. The definitions and specifications of the degrees of reliability are out of the scope of this Recommendation.

9.1 The description of the high reliable application support model

9.1.1 The functional view of the reliable application support model

The functional view of the reliable application support model consists of the reliable management group, the reliable data management group, the reliable service provision group, the reliable communication group, the reliable connectivity group, the reliable application support group and the interactions among these groups as illustrated in Figure 9-1. Each functional group contains related capabilities for support of the IoT reliable applications.

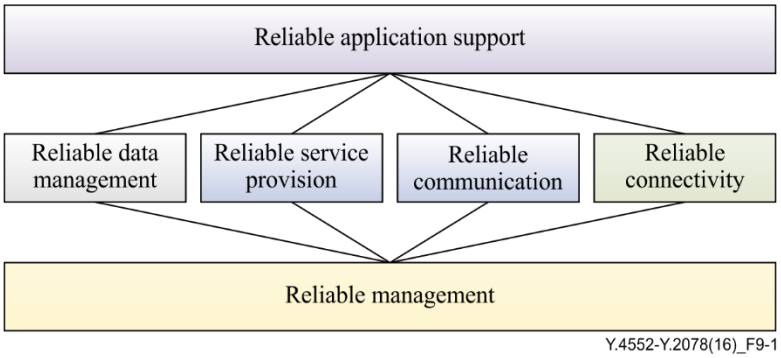

Figure 9-1 – The functional view of the reliable application support model

The reliable application support group is related to the reliable data management group, the reliable service provision group, the reliable communication group and the reliable connectivity group, in order to allow exposure of their reliable capabilities to IoT applications.

The reliable management group is related to the reliable data management group, the reliable service provision group, the reliable communication group and the reliable connectivity group, in order to provide management capabilities to support additional reliability requirements of IoT applications, such as reliable service integrity check capability and reliable data integrity check capability.

NOTE – The concepts of security and privacy protection are related to the concepts of reliability. In order to ensure that security and privacy protection are realized, some reliable support mechanisms are required for the implementation and deployment of the security and privacy protection capabilities. Based on the requirements that the security and privacy protection capability be isolated from other capabilities during implementation and deployment, these reliable support mechanisms are required to be implemented and deployed in self-sustained functional components. According to these considerations, the reliable application support model does not contain capabilities of the security and privacy protection group.

9.1.2 The implementation view of the reliable application support model

The implementation view of the reliable application support model consists of the reliable management and identity management entity, the reliable IoT gateway entity, the reliable end-user device entity, the reliable transport control entity, the reliable IoT transport control entity, the reliable service control entity, the reliable IoT service control entity, the reliable IoT data management entity, the reliable application support entity and the interactions among these entities as illustrated in Figure 9-2.

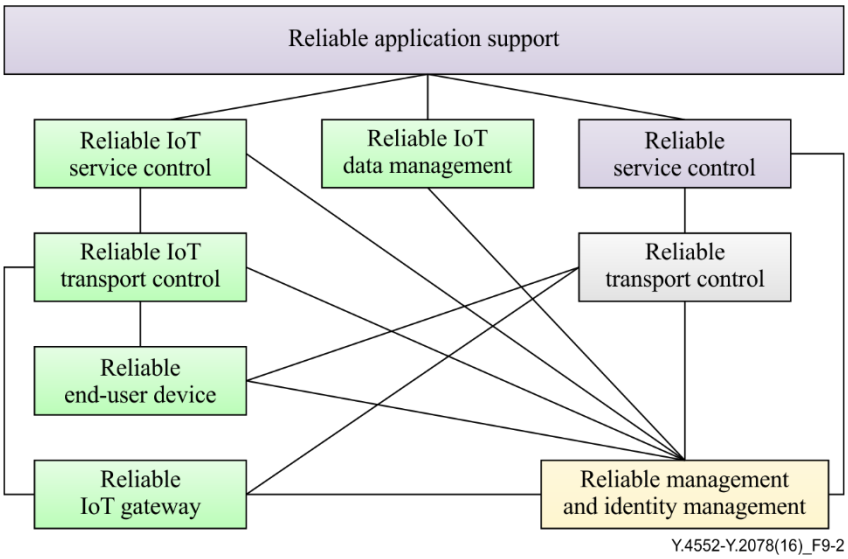

Figure 9-2 – The implementation view of the reliable application support model

The reliable application support entity is related to the reliable IoT data management entity, the reliable IoT service control entity and the reliable service control entity, in order to allow exposure of their reliable capabilities so that can be accessed by IoT applications, such as reliable programming interface capability.

The reliable management and identity management entity is related to the reliable IoT service control entity, the reliable IoT transport control entity, the reliable end-user device entity, the reliable IoT gateway entity, the reliable service control entity and the reliable transport control entity, in order to implement additional reliability features by management capabilities, such as the reliable distributed processing capability.

The reliable end-user device entity and reliable IoT gateway entity are related both to the reliable transport control entity and to the reliable IoT transport control entity, in order to implement reliable communication and connectivity capabilities, such as the reliable periodic communication capability and the reliable identification-based connectivity capability.

9.1.3 The deployment view of the reliable application support model

The deployment view of the reliable application support model consists of the reliable device manager component, the reliable IoT gateway component, the reliable end-user device component, the reliable network manager component, the reliable IoT network controller component, the reliable service manager component, the reliable IoT service controller component, the reliable IoT data server component, the reliable service platform component and the interactions among these components as illustrated in Figure 9-3.

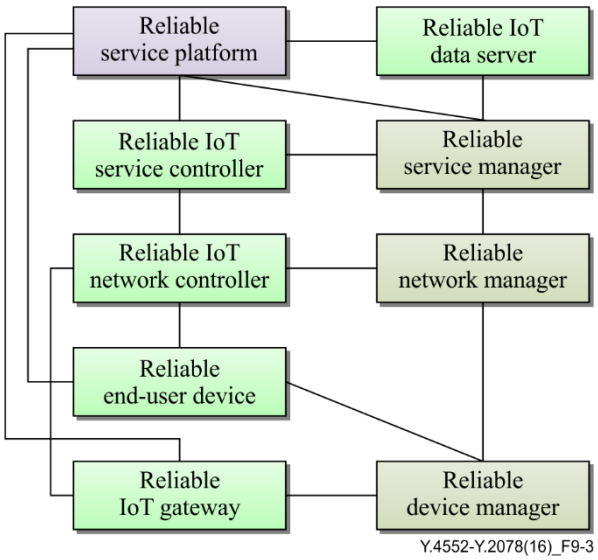

Figure 9-3 – The deployment view of the reliable application support model

The reliable service platform component is related to the reliable end-user device component and the reliable IoT gateway component to provide reliable application support capabilities, such as the reliable group management capability.

NOTE – It is assumed that IoT applications are required to be executed in the reliable end-user device component and the reliable IoT gateway component.

The reliable IoT data server component is related to the reliable service platform component in order to provide reliable data management capabilities, such as the reliable information exchange capability.

The reliable service platform component is related to the reliable service manager component, the reliable service manager component is related to the reliable network manager component and the reliable network manager component is related to the reliable device manager component, in order to provide integrated reliable management capabilities, such as the reliable management capability for multiple domains as defined in [ITU-T Y.4401].

9.2 The capabilities of the reliable application support model

Based on the categories of the IoT basic capabilities specified in [ITU-T Y.4401] and the functional view of the reliable application support model specified in clause 9.1, the capabilities of the reliable application support model can be classified into the following functional groups: reliable service provision capabilities, reliable communication capabilities, reliable application support capabilities,

reliable data management capabilities, reliable management capabilities and reliable connectivity capabilities.

The capabilities of the reliable application support model are specified from the perspective of reliable application support components as described in the deployment view of the reliable application support model in clause 9.1.3, because these capabilities are implemented, deployed and used in these reliable application support components.

The following clauses describe, respectively, these capabilities of the reliable application support model. These same capabilities are numbered and summarized in Annex C.

NOTE – In the following clauses, the capability numbers, as shown in Annex C, are put between square brackets "[ ]" and inserted at the end of the description of the corresponding capability.

9.2.1 Reliable service provision capabilities

The reliable service provision capabilities extend the service provision capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to support reliable service provisioning to the IoT applications.

The reliable service provision capabilities include the reliable service prioritization capability, the reliable service composition capability, the reliable mobility service capability, the reliable autonomic service capability and the reliable naming and addressing capability.

The reliable service prioritization capability enables the reliable service platform and the reliable IoT service controller to guarantee services priorities, in order to provide reliable differentiated services to the IoT applications [C-1-1].

The reliable service composition capability enables the reliable service platform and the reliable service manager to guarantee correct service creation or service customization based on the requirements of the IoT applications [C-1-2].

The reliable mobility service capability enables the reliable service platform and the reliable service manager to guarantee correct remote service access, remote user authentication and remote service execution based on the IoT application requirements [C-1-3].

The reliable autonomic service capability enables the reliable service platform, the reliable service manager and the reliable IoT service controller to guarantee automatic capturing, transferring and analyzing data of things and automatic provision of services in correct ways based on predefined rules [C-1-4].

The reliable naming and addressing capability enables the reliable service manager, the reliable network manager and the reliable device manager to guarantee creating, updating, deleting, querying names and addresses of users, devices and things in correct ways based on predefined rules [C-1-5].

In addition to the above capabilities, the service provision acknowledgement capability numbered as C-1-12 in [ITU-T Y.4401] is also part of reliable service provision capabilities.

9.2.2 Reliable communication capabilities

The reliable communication capabilities extend the communication capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to support reliable communication for the IoT applications.

The reliable communication capabilities include the reliable event-based communication capability, the reliable periodic communication capability and the reliable quality of service enabling communication capability.

The reliable event-based communication capability enables the reliable service platform, the reliable end-user devices and the reliable IoT gateways to guarantee correct ways of initiating communication based on predefined events and rules [C-2-1].

The reliable periodic communication capability enables the reliable service platform, the reliable end-user devices and the reliable IoT gateways to guarantee correct ways of periodically initiating communication based on predefined rules [C-2-2].

The reliable quality of service enabling communication capability enables the reliable network controller, the reliable end-user devices and the reliable IoT gateways to guarantee the QoS required for the delivery and processing of data (e.g., time-sensible data) in correct ways [C-2-3].

In addition to the above capabilities, the transport acknowledgement capability numbered as C-2-15 in [ITU-T Y.4401] is also part of reliable communication capabilities.

9.2.3 Reliable application support capabilities

The reliable application support capabilities extend the application support capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to provide reliable application support to the IoT applications.

The reliable application support capabilities include the reliable programmable interface provision capability, the reliable group management capability, the reliable time synchronization capability and the reliable user management capability.

The reliable programmable interface provision capability enables the reliable service platform to guarantee correct ways of providing or customizing services making use of existing capabilities based on the IoT application requirements [C-3-1].

The reliable group management capability enables the reliable service platform to guarantee correct ways of creating, modifying, deleting and querying IoT groups and of adding, modifying, deleting and querying IoT group members based on the requirements of the IoT applications and predefined rules [C-3-2].

The reliable time synchronization capability enables the reliable service platform to guarantee correct ways of synchronizing the time among related functional components, in order to support global or local time stamping for the IoT applications [C-3-3].

The reliable orchestration capability enables the reliable service platform, the reliable end-user devices and the reliable IoT gateways to guarantee correct ways of coordinating service provisioning based on the requirements of the IoT applications and predefined rules [C-3-4].

The reliable user management capability enables the reliable service platform to guarantee correct ways of creating, querying, updating and deleting IoT user profiles and of authenticating, authorizing, registering and auditing IoT users based on predefined rules [C-3-5].

In addition to the above capabilities, the application support operation acknowledgement capability numbered as C-3-6 in [ITU-T Y.4401], is also part of reliable application support capabilities.

9.2.4 Reliable data management capabilities

The reliable data management capabilities extend the data management capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to support reliable data management to the IoT applications.

The reliable data management capabilities include the reliable data processing capability, the reliable information exchange capability and the reliable autonomic data operation capability.

The reliable data processing capability enables the reliable IoT data server to guarantee trustable results of data fusion and mining based on the IoT application requirements and predefined rules [C-4-1].

The reliable information exchange capability enables the reliable IoT data server to guarantee correct ways of sending data to or receiving data from external data sources, e.g., data centres and data servers outside the IoT, based on the IoT application requirements and predefined rules [C-4-2].

The reliable autonomic data operation capability enables the reliable IoT data server, the reliable end-user devices and the reliable IoT gateways, to guarantee correct ways of automatically collecting, aggregating, transferring, storing, analyzing data of things, as well as automatically managing these data operations based on the IoT application requirements and predefined rules [C-4-3].

9.2.5 Reliable management capabilities

The reliable management capabilities extend the management capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to support reliable management to the IoT applications.

The reliable management capabilities include the reliable distributed processing management capability, the reliable multi-domain management capability, the reliable service integrity check capability, the reliable data integrity check capability, the reliable device integrity check capability, the reliable security integrity check capability and the reliable user profile integrity check capability.

The reliable distributed processing management capability enables the reliable IoT data server, the reliable service manager, the reliable network manager and the reliable device manager to guarantee correct ways of managing IoT functional components in a distributed way based on predefined rules [C-5-1].

The reliable multi-domain management capability enables the reliable IoT data server, the reliable service manager, the reliable network manager and the reliable device manager to guarantee correct ways of managing IoT functional components in multiple administrative domains [ITU-T Y.4401] based on predefined rules [C-5-2].

The reliable service integrity check capability enables the reliable service manager to guarantee trustable ways of checking service lifetime and available resources required to provide the service, in order to guarantee a certain degree of service provision availability based on the IoT application requirements [C-5-3].

The reliable data integrity check capability enables the reliable IoT data server to guarantee trustable ways of checking data lifetime, available attributes of data and consistency of data in order to guarantee a certain degree of availability of data management based on the IoT application requirements [C-5-4].

The reliable device integrity check capability enables the reliable device manager, the reliable IoT gateway and the reliable end-user device to guarantee trustable ways of checking the status of all device functionalities in order to guarantee a certain degree of device availability based on the IoT application requirements [C-5-5].

The reliable security integrity check capability enables the reliable service manager, the reliable network manager, the reliable device manager and the reliable IoT data server to guarantee trustable ways of checking the consistency of security policies deployed in all functional components of the IoT, in order to guarantee a certain degree of security availability in the IoT based on the IoT application requirements [C-5-6].

The reliable user profile integrity check capability enables the reliable service manager, the reliable network manager, the reliable device manager and the reliable IoT data server to guarantee trustable ways of checking lifetime, subscription, privacy protection and availability of services subscribed

by users, in order to guarantee a certain degree of availability of service provisioning and privacy protection for users based on the IoT application requirements [C-5-7].

In addition to the above capabilities, the redundant deployment enablement capability numbered by C-5-9 in [ITU-T Y.4401] is also part of reliable management capabilities.

9.2.6 Reliable connectivity capabilities

The reliable connectivity capabilities extend the connectivity capabilities of the IoT basic capabilities specified in [ITU-T Y.4401], in order to support reliable connectivity to the IoT applications.

The reliable connectivity capabilities include reliable identification based connectivity capability and reliable device mobility capability.

The reliable identification based connectivity capability enables the reliable network manager, the reliable end-user devices and the reliable IoT gateways to guarantee correct ways of establishing the connectivity based on the identification of things and predefined rules [C-6-1].

The reliable device mobility capability enables the reliable network manager, the reliable end-user devices and the reliable IoT gateways to guarantee correct ways of keeping the connectivity when the reliable end-user devices or the reliable IoT gateways are moving based on predefined rules [C-6-2].

10 Security considerations

Security is one of the fundamental aspects to be considered in the IoT application support models. This Recommendation considers the issues of security and privacy protection both from the perspective of the IoT application support models' description and of the capabilities of the IoT application support models' capabilities.

The issues of security and privacy protection from the perspective of the IoT application support models' description are considered, respectively, in clause 7.1 for the IoT configurable application support model, in clause 8.1 for the IoT adaptable application support model and in clause 9.1 for the IoT reliable application support model.

The issues of security and privacy protection from the perspective of the IoT configurable application support model capabilities are considered in clause 7.2.5. Concerning security and privacy protection with respect to the adaptable application support model and the reliable application support model, these issues are considered, respectively, in clauses 8.1.1 and 9.1.1.

Annex A

The list of configurable capabilities for support of IoT applications

(This annex forms an integral part of this Recommendation.)

The tables in this annex list and number the configurable capabilities identified in this Recommendation for support of IoT applications.

All tables in this annex have the following format:

– The first column of these tables is named as "capability number" and assigns a number to each IoT capability. The numbering rule for each IoT capability is as follows: A-<the sub-clause number of clause 7.2>-<the sequence number of each configurable capability in each sub-clause>. For example, the first configurable capability described in clause 7.2.1 is numbered as A-1-1.

– The second column of these tables is named as "capability name" and gives the name of each configurable capability.

– The third column of these tables is named as "capability summary" and briefly describes what the capability does.

– The fourth column of these tables is named as "related basic capabilities" and describes the IoT basic capabilities specified in [ITU-T Y.4401] that are related to the configurable capability.

NOTE 1 – One configurable capability may be related to one or several IoT basic capabilities.

The fifth column of these tables is named as "associated components" and lists the functional components of the deployment view of the configurable application support model described in clause 7.1 that are associated with the configurable capability. This column can be used to validate that the configurable capability can be implemented and deployed.

NOTE 2 – For the purpose of simplification, the prefixed "configurable" is omitted for the associated components naming in the tables.

Table A.1 shows the list of configurable service provision capabilities.

Table A.1 – List of configurable service provision capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-1-1	Configurable service prioritization	The configurable service prioritization capability enables the IoT applications to configure services in different priorities, in order to provide differentiated services based on their requirements.	Service prioritization numbered as C-1-1 in [ITU-T Y.4401]	Service platform, IoT service controller

Table A.1 – List of configurable service provision capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-1-2	Configurable service composition	The configurable service composition capability enables the IoT applications to configure service creation or service customization based on their requirements.	Service composition numbered as C-1-3 in [ITU-T Y.4401].	Service platform, service manager
A-1-3	Configurable location based and context aware service	The configurable location based and context-aware service capability enables the IoT applications to configure services that are provided both on the location information and related context, and on the predefined rules or policies, in order to fulfil their requirements.	Location based and context-aware service numbered as C-1-6 in [ITU-T Y.4401].	Service platform, service manager, IoT service controller

Table A.2 shows the list of configurable communication capabilities.

Table A.2 – List of configurable communication capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-2-1	Configurable event-based communication	The configurable event-based communication capability enables the IoT applications to configure different events in order to initiate communication based on the requirements of the IoT applications.	Event-based communication numbered as C-2-1 in [ITU-T Y.4401].	IoT gateway, end-user device, service platform
A-2-2	Configurable periodic communication	The configurable periodic communication capability enables the IoT applications to configure the rules in order to periodically initiate communication based on the requirements of the IoT applications.	Periodic communication numbered as C-2-2 in [ITU-T Y.4401].	IoT gateway, end-user device, service platform

Table A.2 – List of configurable communication capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-2-3	Configurable communication mode	The configurable communication mode capability enables the IoT applications to configure different modes of communications in transport network in order to transfer data from the source(s) to the destination(s) based on the requirements of the IoT applications.	Unicast communication numbered as C-2-3 in [ITU-T Y.4401]. Multicast communication numbered as C-2-4 in [ITU-T Y.4401]. Broadcast communication numbered as C-2-5 in [ITU-T Y.4401]. Anycast communication numbered as C-2-6 in [ITU-T Y.4401].	Network manager
A-2-4	Configurable Quality of Service communication	The configurable quality of service communication capability enables the IoT applications to configure the related mechanisms in order to guarantee the delivery and process the time-sensible data based on the requirements of the IoT applications.	Quality of service enabling communication numbered as C-2-8 in [ITU-T Y.4401].	IoT gateway, end-user device, IoT network controller
A-2-5	Configurable content-aware communication	The configurable content-aware communication capability enables the IoT applications to configure the parameters related with content and selected path for routing or blocking data transfer based on the requirements of the IoT applications.	Content-aware communication numbered as C-2-13 in [ITU-T Y.4401].	IoT gateway, end-user device, IoT network controller
A-2-6	Configurable location based communication	The configurable location based communication capability enables the IoT applications to configure the parameters related with locations and predefined rules in order to initiate communication based on the requirements of the IoT applications.	Location based communication numbered as C-2-14 in [ITU-T Y.4401].	IoT gateway, end-user device, IoT network controller

Table A.3 shows the list of configurable data management capabilities.

Table A.3 – List of configurable data management capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-3-1	Configurable data storage	The configurable data storage capability enables the IoT applications to configure rules or policies for storing data based on the requirements of the IoT applications.	Data storage numbered as C-4-1 in [ITU-T Y.4401].	IoT data server, IoT gateway
A-3-2	Configurable data processing	The configurable data processing capability enables the IoT applications to configure the rules or the policies for processing data based on the requirements of the IoT applications.	Data processing numbered as C-4-2 in [ITU-T Y.4401].	IoT data server
A-3-3	Configurable information exchange	The configurable information exchange capability enables the IoT applications to configure the parameters for sending data to or receiving data from external data sources, e.g., data centres and data servers outside the IoT based on the requirements of the IoT applications.	Open information exchange numbered as C-4-5 in [ITU-T Y.4401].	IoT data server
A-3-4	Configurable semantic data operation	The configurable semantic data operation capability enables the IoT applications to configure the parameters for semantic annotating, semantic discovering, semantic storing and semantic composition of data of things based on the requirements of the IoT applications.	Semantic data operation numbered as C-4-6 in [ITU-T Y.4401].	IoT data server, IoT gateway
A-3-5	Configurable autonomic data operation	The configurable autonomic data operation capability enables the IoT applications to configure the parameters for automatically collecting, aggregating, transferring, storing, analyzing data of things, as well as automatically managing these data operations based on the requirements of the IoT applications.	Autonomic data operation numbered as C-4-7 in [ITU-T Y.4401].	IoT gateway, end-user device, IoT data server

Table A.4 shows the list of configurable connectivity capabilities.

Table A.4 – List of configurable connectivity capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-4-1	Configurable identification based connectivity	The configurable identification based connectivity capability enables the IoT applications to configure the parameters for connectivity establishment based on the identification of things and the requirements of the IoT applications.	Identification based connectivity numbered as C-6-1 in [ITU-T Y.4401].	IoT gateway, end-user device, network manager
A-4-2	Configurable things' status notification	The configurable things' status notification capability enables the IoT applications to configure the rules of automatic notification of the status of things and its changes based on the requirements of the IoT applications.	Things' status notification numbered as C-6-2 in [ITU-T Y.4401].	IoT gateway, end-user device
A-4-3	Configurable device mobility	The configurable device mobility capability enables the IoT applications to configure the parameters for maintaining the connectivity with the IoT when end-user devices or IoT gateways are moving, based on the requirements of the IoT applications.	Device mobility numbered as C-6-3 in [ITU-T Y.4401].	IoT gateway, end-user device, network manager
A-4-4	Configurable and adaptable connectivity	The configurable and adaptable connectivity capability enables the IoT applications to configure the parameters for extending connectivity configurations to connect with different types of devices of the IoT based on the requirements of the IoT applications, in order to be adaptable to different technologies in devices of IoT.	Adaptable connectivity numbered as C-6-4 in [ITU-T Y.4401].	IoT gateway, end-user device, device manager

Table A.5 shows the list of configurable communication capabilities.

Table A.5 – List of configurable communication capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-5-1	Configurable communication security	The configurable communication security capability enables the IoT applications to configure the rules and policies for supporting secure, trusted and privacy protected communication based on the requirements of the IoT applications.	Communication security numbered as C-7-1 in [ITU-T Y.4401].	IoT gateway, end-user device, device manager, network manager, enhanced transport network
A-5-2	Configurable data management security	The configurable data management security capability enables the IoT applications to configure the rules and policies for providing secure, trusted and privacy protected data management based on the requirements of the IoT applications.	Data management security numbered as C-7-2 in [ITU-T Y.4401].	IoT data server, IoT gateway
A-5-3	Configurable service provision security	The configurable service provision security capability enables the IoT applications to configure the rules and policies for providing secure, trusted and privacy protected service provision based on the requirements of the IoT applications.	Service provision security numbered as C-7-3 in [ITU-T Y.4401].	Service platform, service manger
A-5-4	Configurable security integration	The configurable security integration capability enables the IoT applications to configure the rules and policies for enabling integration of different security policies and techniques related to IoT functional components based on the requirements of the IoT applications.	Security integration numbered as C-7-4 in [ITU-T Y.4401].	Device manager, network manager, service manager

Table A.5 – List of configurable communication capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-5-5	Configurable mutual authentication and authorization	The configurable mutual authentication and authorization capability enables the IoT applications to configure the rules and policies for authenticating and authorizing IoT applications and devices before a device accesses IoT based on the requirements of the IoT applications.	Mutual authentication and authorization numbered as C-7-5 in [ITU-T Y.4401].	Device manager, network manager

Table A.6 shows the list of configurable application support capabilities.

Table A.6 – List of configurable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-6-1	Configurable group management	The configurable group management capability enables the IoT applications to configure the parameters for creating, modifying, deleting, and querying IoT groups, as well as adding, modifying, deleting and querying IoT group members, based on the requirements of the IoT applications.	Group management numbered as C-3-2 in [ITU-T Y.4401].	Service platform
A-6-2	Configurable time synchronization	The configurable time synchronization capability enables the IoT applications to configure the parameters for synchronizing the time among related functional components with different degrees of reliability, in order to support global or local time stamping for applications based on the different Quality of Service requirements of the IoT applications.	Time synchronization numbered as C-3-3 in [ITU-T Y.4401].	Service platform

Table A.6 – List of configurable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-6-3	Configurable orchestration	The configurable orchestration capability enables the IoT applications to configure the parameters for automatic coordination of service provisioning or device operations based on the requirements of the IoT applications.	Orchestration numbered as C-3-4 in [ITU-T Y.4401].	IoT gateway, end-user device, service platform
A-6-4	Configurable application support operation acknowledgement	The configurable application support operation acknowledgement capability enables the IoT applications to configure the parameters for acknowledging the correct operations requested by applications in order to support reliable application operations in the IoT, based on the requirements of the IoT applications.	Application support operation acknowledgement numbered as C-3-6 in [ITU-T Y.4401].	IoT data server, IoT gateway

Table A.7 shows the list of configurable management capabilities.

Table A.7 – List of configurable management capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-7-1	Configurable redundant deployment enablement	The configurable redundant deployment enablement capability enables the IoT applications to configure deployment of redundant functional components of the IoT in order to provide different degrees of reliability required in communication, service provision and data management, based on the requirements of the IoT applications.	Redundant deployment enablement numbered as C-5-9 in [ITU-T Y.4401].	IoT data server, IoT service controller, service platform, service manager, IoT network controller, network manager, IoT gateway, device manager

Table A.7 – List of configurable management capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-7-2	Configurable service integrity check	The configurable service integrity check capability enables the IoT applications to configure the parameters for checking the service lifetime, the available resources required to provide the service in order to provide different degrees of availability in service provisioning, based on the requirements of the IoT applications.	Service integrity check numbered as C-5-10 in [ITU-T Y.4401].	Service manager
A-7-3	Configurable data integrity check	The configurable data integrity check capability enables the IoT applications to configure the parameters for checking the data lifetime, the available attributes of the data, and the consistency of data in order to provide different degrees of availability in data management, based on the requirements of the IoT applications.	Data integrity check numbered as C-5-11 in [ITU-T Y.4401].	IoT data server
A-7-4	Configurable device integrity check	The configurable device integrity check capability enables the IoT applications to configure the parameters for checking the status of all device functions in order to provide different degrees of availability in IoT devices, based on the requirements of the IoT applications.	Device integrity check as C-5-12 in [ITU-T Y.4401].	Device manager, IoT device, IoT gateway, end-user device

Table A.7 – List of configurable management capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
A-7-5	Configurable security integrity check	The configurable security integrity check capability enables the IoT applications to configure the parameters for checking the consistency of security policies deployed in all functional components of the IoT in order to provide different degrees of availability in security and privacy protection provisioning, based on the requirements of the IoT applications.	Security integrity check numbered as C-5-13 in [ITU-T Y.4401].	Service manager, network manager, device manager, IoT device, IoT gateway, end-user device
A-7-6	Configurable user profile integrity check	The configurable user profile integrity check capability enables the IoT applications to configure the parameters for checking the lifetime, subscription, privacy protection, and availability of services subscribed by users in order to provide different degrees of availability in service provisioning and privacy protection for users, based on the requirements of the IoT applications.	User profile integrity check numbered as C-5-14 in [ITU-T Y.4401].	Service manager, network manager, device manager, IoT device, IoT gateway, end-user device

Annex B

The list of adaptable capabilities for support of IoT applications

(This annex forms an integral part of this Recommendation.)

The following table lists and numbers the adaptable capabilities identified in this Recommendation for support of IoT applications.

The table in this annex has the following format:

– The first column of the table is named as "capability number" and assigns a number to each IoT capability. The numbering rule for each IoT capability is as follows: B-<the sub-clause number of clause 8.2>-<the sequence number of each adaptable capability in each sub-clause>. For example, the first adaptable capability described in clause 8.2.1 is numbered as B-1-1.

– The second column of the table is named as "capability name" and gives the name of each adaptable capability.

– The third column of the table is named as "capability summary" and shortly describes what the capability does.

– The fourth column of the table is named as "related basic capabilities" and describes the IoT basic capabilities specified in [ITU-T Y.4401] that are related with the adaptable capability.

– The fifth column of the table is named as "associated components" and lists the functional components of the deployment view of the adaptable application support model described in clause 8.1 that are associated with the adaptable capability. This column can be used to validate that the adaptable capability can be implemented and deployed.

NOTE – For simplification purpose, the prefixed "adaptable" is omitted for the associated components naming in the tables.

Table B.1 shows the list of adaptable application support capabilities.

Table B.1 – List of adaptable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
B-1-1	Adaptable service prioritization	The adaptable service prioritization capability enables the service platform and the IoT service controller to adjust services priorities, in order to adapt to differentiated services requirements from the IoT applications.	Service prioritization numbered as C-1-1 in [ITU-T Y.4401]	Service platform, IoT service controller

Table B.1 – List of adaptable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
B-1-2	Adaptable service composition	The adaptable service composition capability enables the service platform and the service manager to adjust service creation or service customization based on the requirements of the IoT applications.	Service composition numbered as C-1-3 in [ITU-T Y.4401].	Service platform, service manager
B-1-3	Adaptable mobility service	The adaptable mobility service capability enables the service platform to adjust the mechanism of remote service access, remote user authentication, and remote service execution.	Mobility service numbered as C-1-4 in [ITU-T Y.4401].	Service platform, service manager
B-2-1	Adaptable event-based Communication	The adaptable event-based communication capability enables the service platform, the end-user devices, and the IoT gateways to adjust the events for initiating communication based on predefined rules.	Event-based communication numbered as C-2-1 in [ITU-T Y.4401]	IoT device, IoT gateway, end-user device, service platform
B-2-2	Adaptable Quality of Service enabling communication	The adaptable Quality of Service enabling communication capability enables the network controller, the end-user devices, and the IoT gateways to adjust the mechanisms according to current network status and predefined rules to guarantee the Quality of Service required for the delivery and processing of data (e.g., time-sensible data).	Quality of service enabling communication numbered as C-2-8 in [ITU-T Y.4401]	IoT device, IoT gateway, end-user device, IoT network controller

Table B.1 – List of adaptable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
B-3-1	Adaptable group management	The adaptable group management capability enables the service platform to create, modify, delete, and query IoT groups, as well as to add, modify, delete and query IoT group members based on the requirements of the IoT applications and predefined rules.	Group management numbered as C-3-2 in [ITU-T Y.4401]	Service platform
B-3-2	Adaptable orchestration	The adaptable orchestration capability enables the service platform, the end-user devices, and the IoT gateways to dynamic coordinate service provisioning or device operations based on the requirements of the IoT applications and predefined rules.	Orchestration numbered as C-3-4 in [ITU-T Y.4401]	IoT device, IoT gateway, end-user device, service platform
B-4-1	Adaptable data processing	The adaptable data processing capability enables the IoT data server to adjust methods of data fusion and mining based on the IoT application requirements and predefined rules.	Data processing numbered as C-4-2 in [ITU-T Y.4401]	IoT data server
B-4-2	Adaptable information exchange	The adaptable information exchange capability enables the IoT data server to autonomously send data to or receive data from external data sources, e.g., data centres and data servers outside the IoT, based on the IoT application requirements and predefined rules.	Open information exchange numbered as C-4-5 in [ITU-T Y.4401]	IoT data server

Table B.1 – List of adaptable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
B-5-1	Adaptable identification based connectivity	The adaptable identification based connectivity capability enables the network manager, the end-user devices, and the IoT gateways to dynamic choose the ways of establishing the connectivity based on the identification of things and predefined rules.	Identification based connectivity numbered as C-6-1 in [ITU-T Y.4401]	IoT device, IoT gateway, end-user device, network manager
B-5-2	Adaptable device mobility	The adaptable device mobility capability enables the network manager, the end-user devices, and the IoT gateways to dynamic negotiate the ways of keeping the connectivity when the IoT devices or the IoT gateways are moving based on predefined rules.	Device mobility numbered as C-6-3 in [ITU-T Y.4401]	IoT device, IoT gateway, end-user device, network manager

Annex C

The list of reliable capabilities for support of IoT applications

(This annex forms an integral part of this Recommendation.)

The following table lists and numbers the reliable capabilities identified in this Recommendation for support of IoT applications.

The table in this annex has the following format:

– The first column of the table is named as "capability number" and assigns a number to each IoT capability. The numbering rule for each IoT capability is as follows: C-<the sub-clause number of clause 9.2>-<the sequence number of each reliable capability in each sub-clause>. For example, the first reliable capability described in clause 9.2.1 is numbered as C-1-1.

– The second column of the table is named as "capability name" and gives the name of each reliable capability.

– The third column of the table is named as "capability summary" and shortly describes what the capability does.

– The fourth column of the table is named as "related basic capabilities" and describes the IoT basic capabilities specified in [ITU-T Y.4401] that are related with the reliable capability.

– The fifth column of the table is named as "associated components" and lists the functional components of the deployment view of the reliable application support model described in clause 9.1 that are associated with the reliable capability. This column can be used to validate that the reliable capability can be implemented and deployed.

NOTE – For simplification purpose, the prefixed "reliable" is omitted for the associated components naming in the tables.

Table C.1 shows the list of reliable application support capabilities.

Table C.1 – List of reliable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
C-1-1	Reliable service prioritization	The reliable service prioritization capability enables service platform and IoT service controller to guarantee services priorities, in order to provide reliable differentiated services to the IoT applications.	Service prioritization numbered as C-1-1 in [ITU-T Y.4401]	Service platform, IoT service controller

Table C.1 – List of reliable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
C-1-2	Reliable service composition	The reliable service composition capability enables service platform and service manager to guarantee correct service creation or service customization based on the requirements of the IoT applications.	Service composition numbered as C-1-3 in [ITU-T Y.4401].	Service platform, service manager
C-1-3	Reliable mobility service	The reliable mobility service capability enables the service platform and the service manager to guarantee correct remote service access, remote user authentication, and remote service execution based on the IoT application requirements.	Mobility service numbered as C-1-4 in [ITU-T Y.4401].	Service platform, service manager
C-1-4	Reliable autonomic service	The reliable autonomic service capability enables the service platform, the service manager, and the IoT service controller to guarantee automatic capturing, transferring, and analyzing data of things, and automatic provision of services in correct ways based on predefined rules.	Autonomic service numbered as C-1-5 in [ITU-T Y.4401]	Service platform, service manager, IoT service controller
C-1-5	Reliable naming and addressing	The reliable naming and addressing capability enables the service manager, the network manager, and the device manager to guarantee creating, updating, deleting, querying names and addresses of users, devices and things in correct ways based on predefined rules.	Standardized naming and addressing numbered as C-1-9 in [ITU-T Y.4401]	Service manager, network manager, device manager
C-2-1	Reliable event-based Communication	The reliable event-based communication capability enables the service platform, the end-user devices, and the IoT gateways to guarantee correct ways of initiating communication based on predefined events and rules.	Event-based communication numbered as C-2-1 in [ITU-T Y.4401]	IoT gateway, end-user device, service platform

Table C.1 – List of reliable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
C-2-2	Reliable periodic communication	The reliable periodic communication capability enables the service platform, the end-user devices, and the IoT gateways to guarantee correct ways of periodically initiating communication based on predefined rules.	Periodic communication numbered as C-2-2 in [ITU-T Y.4401]	IoT gateway, end-user device, service platform
C-2-3	Reliable Quality of Service enabling communication	The reliable Quality of Service enabling communication capability enables the network controller, the end-user devices, and the IoT gateways to guarantee the Quality of Service required for the delivery and processing of data (e.g., time-sensible data) in correct ways.	Quality of service enabling communication numbered as C-2-8 in [ITU-T Y.4401]	IoT gateway, end-user device, IoT network controller
C-3-1	Reliable programmable interface provision	The reliable programmable interface provision capability enables the service platform to guarantee correct ways of providing services or customizing services from existing capabilities based on the IoT application requirements.	Programmable interface provision numbered as C-3-1 in [ITU-T Y.4401]	Service platform
C-3-2	Reliable group management	The reliable group management capability enables the service platform to guarantee correct ways of creating, modifying, deleting, and querying IoT groups, as well as of adding, modifying, deleting and querying IoT group members based on the requirements of the IoT applications and predefined rules.	Group management numbered as C-3-2 in [ITU-T Y.4401]	Service platform

Table C.1 – List of reliable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
C-3-3	Reliable time synchronization	The reliable time synchronization capability enables the service platform to guarantee correct ways of synchronizing the time among related functional components, in order to support global or local time stamping for the IoT applications.	Time synchronization numbered as C-3-3 in [ITU-T Y.4401]	Service platform
C-3-4	Reliable orchestration	The reliable orchestration capability enables the service platform, the end-user devices, and the IoT gateways to guarantee correct ways of coordinating service provisioning based on the requirements of the IoT applications and predefined rules.	Orchestration numbered as C-3-4 in [ITU-T Y.4401]	IoT gateway, end-user device, service platform
C-3-5	Reliable user management	The reliable user management capability enables the service platform to guarantee correct ways of creating, querying, updating and deleting IoT user profiles, and authenticating, authorizing, registering and auditing IoT users based on predefined rules.	User management numbered as C-3-5 in [ITU-T Y.4401]	Service platform
C-4-1	Reliable data processing	The reliable data processing capability enables the IoT data server to guarantee trustable results of data fusion and mining based on the IoT application requirements and predefined rules.	Data processing numbered as C-4-2 in [ITU-T Y.4401]	IoT data server
C-4-2	Reliable information exchange	The reliable information exchange capability enables the IoT data server to guarantee correct ways of sending data to or receiving data from external data sources, e.g., data centres and data servers outside the IoT, based on the IoT application requirements and predefined rules.	Open information exchange numbered as C-4-5 in [ITU-T Y.4401]	IoT data server

Table C.1 – List of reliable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
C-4-3	Reliable autonomic data operation	The reliable autonomic data operation capability enables the IoT data server, the end-user devices, and the IoT gateways to guarantee correct ways of automatically collecting, aggregating, transferring, storing, analyzing data of things, as well as automatically managing these data operations based on the IoT application requirements and predefined rules.	Autonomic data operation numbered as C-4-7 in [ITU-T Y.4401]	IoT gateway, end-user device, IoT data server
C-5-1	Reliable distributed processing management	The reliable distributed processing management capability enables the IoT data server, the service manager, the network manager, and the device manager to guarantee correct ways of managing IoT functional components in a distributed way based on predefined rules.	Managing distributed processing numbered as C-5-7 in [ITU-T Y.4401]	IoT data server, service manager, network manager, device manager
C-5-2	Reliable multi-domain management	The reliable multi-domain management capability enables the IoT data server, service manager, the network manager, and the device manager to guarantee correct ways of managing IoT functional components in multiple administrative domains based on predefined rules.	Managing multiple domains numbered as C-5-8 in [ITU-T Y.4401]	IoT data server, service manager, network manager, device manager
C-5-3	Reliable service integrity check	The reliable service integrity check capability enables the service manager to guarantee trustable ways of checking service lifetime and available resources required to provide the service in order to guarantee certain degree of service provision availability based on the IoT application requirements.	Service integrity check numbered as C-5-10 in [ITU-T Y.4401]	Service manager

Table C.1 – List of reliable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
C-5-4	Reliable data integrity check	The reliable data integrity check capability enables the IoT data server to guarantee trustable ways of checking data lifetime, available attributes of data, and consistency of data in order to guarantee certain degree of availability of data management based on the IoT application requirements.	Data integrity check numbered as C-5-11 in [ITU-T Y.4401]	IoT data server
C-5-5	Reliable device integrity check	The reliable device integrity check capability enables the device manager, the IoT gateway, and the end-user device to guarantee trustable ways of checking the status of all device functionalities in order to guarantee certain degree of device availability of IoT devices based on the IoT application requirements.	Device integrity check numbered as C-5-12 in [ITU-T Y.4401]	Device manager, end-user device, IoT gateway, end-user device
C-5-6	Reliable security integrity check	The reliable security integrity check capability enables the service manager, the network manager, the device manager, and the IoT data server to guarantee trustable ways of checking the consistency of security policies deployed in all functional components of the IoT, in order to guarantee certain degree of security availability in the IoT based on the IoT application requirements.	Security integrity check numbered as C-5-13 in [ITU-T Y.4401]	Service manager, network manager, device manager, IoT data server

Table C.1 – List of reliable application support capabilities

Capability number	Capability name	Capability summary	Related basic capabilities	Associated components
C-5-7	Reliable user profile integrity check	The reliable user profile integrity check capability enables the service manager, the network manager, the device manager, and the IoT data server to guarantee trustable ways of checking the lifetime, subscription, privacy protection, and availability of services subscribed by users, in order to guarantee certain degree of availability of service provisioning and privacy protection for users based on the IoT application requirements.	User profile integrity check numbered as C-5-14 in [ITU-T Y.4401]	Service manager, network manager, device manager, IoT data server
C-6-1	Reliable identification based connectivity	The reliable identification based connectivity capability enables the network manager, the end-user devices, and the IoT gateways to guarantee correct ways of establishing the connectivity based on the identification of things and predefined rules.	Identification based connectivity numbered as C-6-1 in [ITU-T Y.4401]	IoT gateway, end-user device, network manager
C-6-2	Reliable device mobility	The reliable device mobility capability enables the network manager, the end-user devices, and the IoT gateways to guarantee correct ways of keeping the connectivity when the end-user devices or the IoT gateways are moving based on predefined rules.	Device mobility numbered as C-6-3 in [ITU-T Y.4401]	IoT gateway, end-user device, network manager

Appendix I

Use cases for the IoT applications support models from the smart home environment

(This appendix does not form an integral part of this Recommendation.)

Smart home is one of the IoT applications that can be used to make the home environment comfortable and fully automated by connecting home appliances and other electronic devices and sensors through specific wired/wireless connectivity technologies, supporting networking, service provisioning and data collecting and processing functionalities and providing smart home applications, such as home energy management, home security and safety, remote monitoring and control, etc.

A smart home can be implemented and deployed based on its specific (vertical) protocol stack without depending on an IoT service platform. However, a smart home implemented and deployed based on an IoT service platform can make easier and more cost-effective development and deployment of configurable, adaptable and reliable applications by using the capabilities of the service platform.

The following use cases give some examples for smart home applications based on an IoT service platform providing application support model capabilities as specified in this Recommendation.

NOTE – An IoT service platform is identified as the "service platform" functional component of the IoT functional framework specified in [ITU-T Y.4401]

I.1 Use case 1: Configurable remote monitoring in a smart home

One of the procedures for configurable remote monitoring in a smart home is illustrated in Figure I.1.

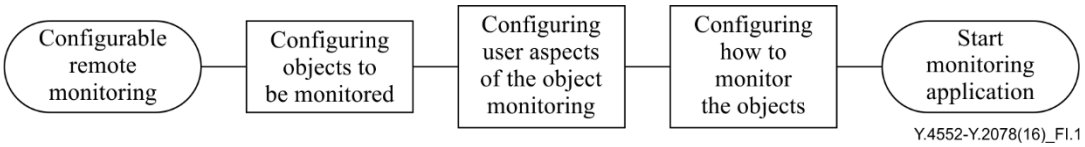

Figure I.1 – A procedure for configurable remote monitoring in a smart home

Configuring objects to be monitored involves activities for configuring the related devices that can sense objects to be monitored. These activities can be realized by making use of the configurable things' status notification capability numbered as A-4-2 and the configurable identification based connectivity capability numbered as A-4-1 and specified in clause 7.2.

Configuring the user aspects of the object monitoring involves activities for configuring data storage methods, mode of the communication and grouping mechanisms related to the end-user devices for monitoring the objects. These activities can be realized by making use of the configurable data storage capability numbered as A-3-1, the configurable communication mode capability numbered as A-2-3 and the configurable group management capability numbered as A-6-1 and specified in clause 7.2.

Configuring how to monitor the objects involves activities for configuring mechanisms for processing monitoring data, the time period for monitoring the objects and the quality of service for transferring monitoring data. These activities can be realized by making use of the configurable data

processing capability numbered as A-3-2, the configurable event-based communication capability numbered as A-2-1, the configurable periodic communication capability numbered as A-2-2, the configurable quality of service communication capability numbered as A-2-4 and the configurable content-aware communication capability numbered as A-2-5 specified in clause 7.2.

After finishing these configurations, the application of remote monitoring in a smart home can be started.

I.2 Use case 2: Adaptable home energy management

One of the procedures for adaptable home energy management is illustrated in Figure I.2.

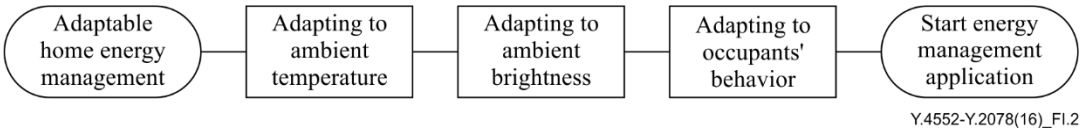

Figure I.2 – A procedure for adaptable home energy management

In this use case, only three types of energy management functions are considered, these are, adapting to ambient temperature, adapting to ambient brightness and adapting to occupants' behavior functions.

Adapting to ambient temperature involves activities for collecting and processing data of ambient temperature based on adaptable data models and adaptable rules of knowledge, adaptable grouping of the home functional components related to monitoring and controlling ambient temperature, such as temperature sensor, smart air conditioners, smart home controller, etc., and adaptable orchestrating of the actions in these home functional components. These activities can be realized by making use of the adaptable identification based connectivity capability numbered as B-5-1, the adaptable data processing capability numbered as B-4-1, the adaptable group management capability numbered as B-3-1 and the adaptable orchestration capability numbered as B-3-2 and specified in clause 8.2.

Adapting to ambient brightness involves activities for collecting and processing data of ambient brightness based on adaptable data models and adaptable rules of knowledge, adaptable grouping the home functional components related to monitoring and controlling ambient brightness, such as brightness sensor, smart lighting switches, smart home controller, etc., and adaptable orchestrating of the actions in these home functional components. These activities can be realized by making use of the adaptable identification based connectivity capability numbered as B-5-1, the adaptable data processing capability numbered as B-4-1, the adaptable group management capability numbered as B-3-1 and the adaptable orchestration capability numbered as B-3-2 and specified in clause 8.2.

Adapting to occupants' behavior involves activities for collecting and processing data of occupants moving and other activities at home based on adaptable data models and adaptable rules of knowledge, adaptable grouping the home functional components related with monitoring, controlling and processing occupants behavior, such as home activity sensor, smart phone, smart home controller, etc., and adaptable orchestrating of the actions in these home functional components. These activities can be realized by making use of the adaptable identification based connectivity capability numbered as B-5-1, the adaptable device mobility capability numbered as B-5-2, the adaptable data processing capability numbered as B-4-1, the adaptable group management capability numbered as B-3-1 and the adaptable orchestration capability numbered as B-3-2 and specified in clause 8.2.

Via the support of these activities, the application of adaptable home energy management can be started.

I.3 Use case 3: Reliable health monitoring at home

One of the procedures for reliable home health monitoring is illustrated in Figure I.3.

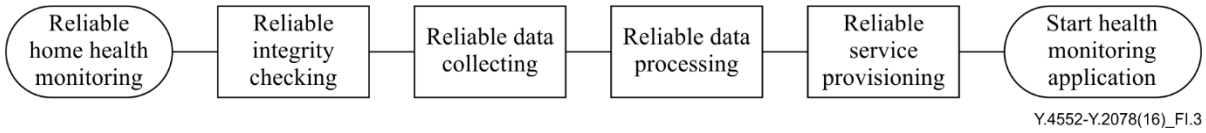

Figure I.3 – One of the procedures for reliable health monitoring at home

Reliable integrity checking involves activities for checking all functions to avoid any possible default. These activities can be realized by making use of the reliable service integrity check capability numbered as C-5-3, the reliable data integrity check capability numbered as C-5-4, the reliable device integrity check capability numbered as C-5-5, the reliable security integrity check capability numbered as C-5-6 and the reliable user profile integrity check capability numbered as C-5-7 and specified in clause 9.2 of this Recommendation.

Reliable data collection involves activities for gathering, transferring and storing data of health monitoring at home in a reliable way. These activities can be realized by making use of the reliable identification based connectivity capability numbered as C-6-1, the reliable device mobility capability numbered as C-6-2, the reliable autonomic data operation capability numbered as C-4-3, the reliable event-based communication capability numbered as C-2-1, the reliable periodic communication capability numbered as C-2-2 and the reliable quality of service enabling communication capability numbered as C-2-3 and specified in clause 9.2.

Reliable data processing involves activities for processing data of health monitoring at home locally or remotely in a reliable way. These activities can be realized by making use of the reliable data processing capability numbered as C-4-1 and the reliable distributed processing management capability numbered as C-5-1 and specified in clause 9.2.

Reliable service provisioning involves activities for providing reliable service interfaces, managing users, groups and services in a reliable way and providing reliable autonomic services. These activities can be realized by making use of the reliable user management capability numbered as C-3-5, the reliable group management capability numbered as C-3-2, the reliable programmable interface provision capability numbered as C-3-1, the reliable mobility service capability numbered as C-1-3 and the reliable autonomic service capability numbered as C-1-4 and specified in clause 9.2.

Via the support of these activities, the application of reliable health monitoring at home can be started.

Bibliography

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899

For further details, please refer to the list of ITU-T Recommendations.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016