International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4470

(08/2020)

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

Internet of things and smart cities and communities – Frameworks, architectures and protocols

Reference architecture of artificial intelligence service exposure for smart sustainable cities

Recommendation ITU-T Y.4470

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, 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.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–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
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.4470

Reference architecture of artificial intelligence service exposure for smart sustainable cities

Summary

Recommendation ITU-T Y.4470 establishes artificial intelligence service exposure (AISE) for smart sustainable cities (SSCs), and provides the common characteristics and high-level requirements, reference architecture and relevant common capabilities of AISE.

AISE is one of the basic supporting functional entities for SSCs, with which SSC services can use uniform reference points (exposed by AISE) to integrate and access the artificial intelligence (AI) capabilities of AI services (e.g., machine learning services for image recognition, natural language processing services and traffic prediction services). In addition, AISE can collect and open SSC data, and it supports AI services to train and supply AI capabilities in AISE in SSCs.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4470	2020-08-29	20	11.1002/1000/14373

Keywords

Artificial intelligence service; exposure; smart sustainable city.

* 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

Recommendation ITU-T Y.4470

Reference architecture of artificial intelligence service exposure for smart sustainable cities

1 Scope

This Recommendation establishes the concept of artificial intelligence service exposure (AISE) for smart sustainable cities (SSCs).

The scope of this Recommendation includes for AISE:

– the concept, analysis of common characteristics and high-level requirements;

– reference architecture and relevant common capabilities.

In addition, working modes for AISE to supply AI capabilities to SSC services are provided. Use cases are given in appendices.

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.*

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 artificial intelligence (AI) [b-ETSI GR ENI 004]: Computerized system that uses cognition to understand information and solve problems.

NOTE 1 – [b-ISO/IEC 2382] defines AI as "interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning".

NOTE 2 – In computer science AI research is defined as the study of "intelligent agents": any device that perceives its environment and takes actions to achieve its goals.

NOTE 3 – This includes pattern recognition and the application of machine learning and related techniques.

NOTE 4 – Artificial intelligence is the whole idea and concepts of machines being able to carry out tasks in a way that mimics the human intelligence and would be considered "smart".

3.1.3 capability [b-ITU-R M.1224-1]: The ability of an item to meet a service demand of given quantitative characteristics under given internal conditions.

3.1.4 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, date capture, data storage and data processing.

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 broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.6 machine learning (ML) [b-ITU-T Y.3172]: Processes that enable computational systems to understand data and gain knowledge from it without necessarily being explicitly programmed.

NOTE – This definition is adapted from [b-ETSI GR ENI 004].

3.1.7 service [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.8 smart sustainable city [b-ITU-T Y.4900]: A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental, as well as cultural aspects.

NOTE – City competitiveness refers to policies, institutions, strategies and processes that determine the city's sustainable productivity.

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3D	Three Dimensional
ACM-FC	AI Capability Management-Functional Component
ACP-FC	AI Capability Performer-Functional Component
AI	Artificial Intelligence
AISE	Artificial Intelligence Service Exposure
AM-FC	AI Model-Functional Component
AMA-FC	AI Model Agent-Functional Component
AMM-FC	AI Model Management-Functional Component
API	Application Programming Interface
DM-FC	Data Management-Functional Component
FC	Functional Component
IoT	Internet of Things

IP	Internet Protocol
ML	Machine Learning
MTM-FC	Model-Training Management-Functional Component
PM-FC	Policy Management-Functional Component
RM-FC	Resource Management-Functional Component
SAVC	Smart Appliance Voice Control
STC	Smart Traffic Controlling
SSC	Smart Sustainable City
TM-FC	Task Management-Functional Component
UGI	Urban Geographic Information

5 Conventions

The following conventions are used 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 Recommendation 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.

6 Introduction of AISE

AISE is a functional entity (see Figure 6-1) in an SSC that facilitates SSC services (e.g., S_1 to S_n) to integrate and access the capabilities of AI services (e.g., AI_1 to AI_m) provided by AI service providers (e.g., A_1 to A_k). AI service(s) can be deployed in AISE and part or whole of their AI capabilities can be exposed to SSC services. AISE provides uniform reference points to support SSC services to subscribe and access the AI capabilities exposed in AISE. SSC services can subscribe and access one or multiple AI capabilities that can be provided by different AI services.

AISE can collect SSC data from SSC services, and can support AI service providers to design and train AI services in the SSC using the collected SSC data. AISE provides a security and privacy protection mechanism for collected SSC data.

NOTE – The SSC data can be opened and shared with AI services and can be accessed only in the SSC. Specification of mechanisms for SSC data openness lies outside the scope of this Recommendation.

AISE also supplies AI services to SSC services (e.g., for inference or prediction).

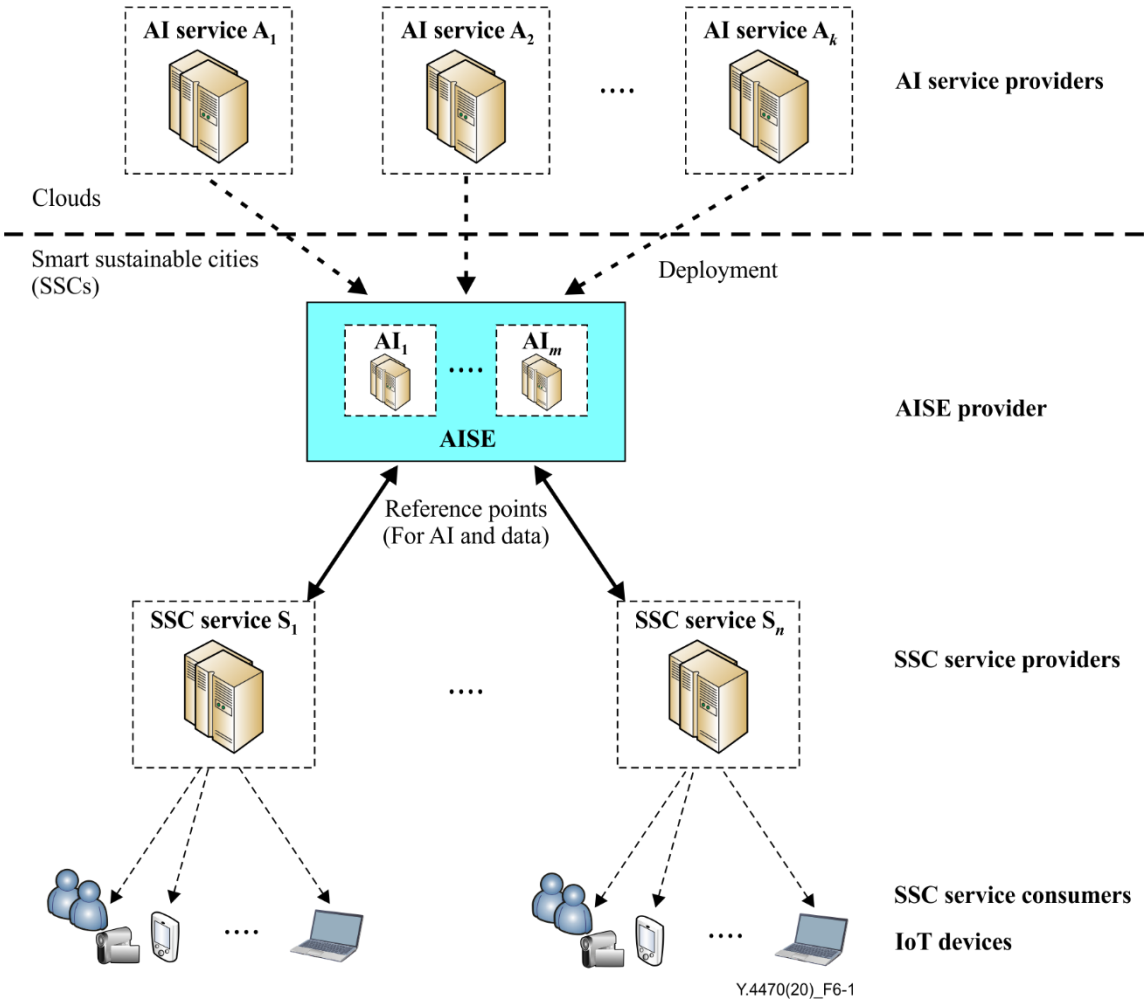

Figure 6-1 – Overview of AISE

AISE can provide benefits to AI service providers and SSC service providers. From the perspective of AI service providers, they can design and train AI capabilities with SSC data in AISE and provide AI capabilities to SSC services through AISE. From the perspective of SSC service providers, they can integrate and access AI capabilities exposed by AI services through AISE.

7 Common characteristics and high-level requirements of AISE

7.1 Common characteristics

This clause provides the general characteristics of AISE.

7.1.1 Integrating multiple AI models

AISE supports the integration of multiple AI models that have been provided by the same or different AI services.

In the tightly coupled working mode (see clause I.1), integrated AI models work within AISE. Conversely, in the loosely coupled working mode (see clause I.2), integrated AI models work outside AISE, and there are corresponding AI model agents in AISE to interact with the integrated AI models.

7.1.2 Supporting AI model training

AISE collects and manages SSC data, and opens it to authorized AI services for training their AI models. The opened SSC data in AISE can be accessed by SSC services.

In the tightly coupled working mode (see clause I.1), opened SSC data is accessed in AISE, and the training for AI models is also performed in AISE. In this mode, AISE provides underlying infrastructures for data openness and model training.

In the loosely coupled working mode (see clause I.2), opened SSC data is accessed through uniform reference points by authorized AI services, which train AI models. In this mode, AISE does not provide underlying infrastructures for model training.

7.1.3 Exposing AI capabilities

AISE exposes uniform reference points for AI services, which can access opened SSC data, and can deploy trained AI models in AISE or train AI models in AISE.

AISE publishes the AI capabilities exposed by the AI services.

In addition, AISE exposes uniform reference points for SSC services, which can discover, subscribe and access AI capabilities as exposed by the same or different AI services, even if the AI capabilities use different AI technologies.

7.1.4 Performing AI capabilities

AISE provides underlying infrastructures to supply AI capabilities to AI models. In the tightly coupled working mode (see clause I.1), the AI capabilities of AI models can be performed within AISE. Furthermore, in the loosely coupled working mode (see clause I.2), the AI model agents in AISE interact with the external AI models and their AI capabilities are performed outside AISE.

7.2 High-level requirements

This clause provides the high-level requirements of AISE.

7.2.1 Requirements for model training of AI capabilities

The requirements and recommendations for model training of AI capabilities are as follows:

– AISE is required to support authorized AI services to subscribe to and access opened SSC data for training the AI model;

– AISE is recommended to support authorized AI services to train the AI model in AISE.

7.2.2 Requirements for publication of exposed AI capabilities

The requirements and recommendations for publication of exposed AI capabilities are as follows:

– AISE is required to support authorized AI services to publish their AI capabilities;

– AISE is required to support authorized AI services to manage (e.g., add, update, delete and search) their published AI capabilities;

– AISE is recommended to allow authorized AI services to define access policies (such as when AI capabilities can be available) for SSC services to access exposed AI capabilities;

– AISE is recommended to support authorized AI services to monitor the subscription status of their AI capabilities.

7.2.3 Requirements for subscription to exposed AI capabilities

The requirements and recommendations for subscription to exposed AI capabilities are as follows:

– AISE is required to support SSC services to discover and subscribe to exposed AI capabilities;

– AISE is required to support SSC services to subscribe multiple exposed AI capabilities provided by the same or different AI service(s);

– AISE is recommended to notify SSC services of the status of their subscribed AI capabilities, if needed, such as whether the relevant AI capabilities are available;

– AISE is recommended to notify authorized AI services of the subscription information of their exposed AI capabilities, if needed, such as who subscribed to and unsubscribed from relevant AI capabilities.

7.2.4 Requirements for accessing exposed AI capabilities

The requirements and recommendations for accessing exposed AI capabilities are as follows:

– AISE is required to support authorized SSC services to access one or more subscribed AI capabilities provided by the same or different AI services;

– AISE is recommended to establish access policies for exposed AI capabilities based on configuration parameters (e.g., time of day, day of the week, location).

7.2.5 Security requirement

The following are the security requirements for AISE;

– AISE is required to authorize and authenticate AI services to access the opened SSC data in AISE;

– AISE is required to authorize and authenticate AI services to train, deploy and expose AI capabilities in AISE;

– AISE is required to authorize and authenticate SSC services to access exposed SSC capabilities as published by AISE.

7.2.6 Other requirement

In addition to the items listed in clauses 7.2.1 to 7.2.5:

– AISE is required to support statistics functions.

8 Reference architecture of AISE

AISE works on the service support and application support layer of the Internet of things (IoT) reference model specified in [ITU-T Y.4000], and it utilizes the capabilities provided by the underlying smart city infrastructures (such as networks, clouds, big data and security). Figure 8-1 is a schematic diagram of the reference architecture of AISE.

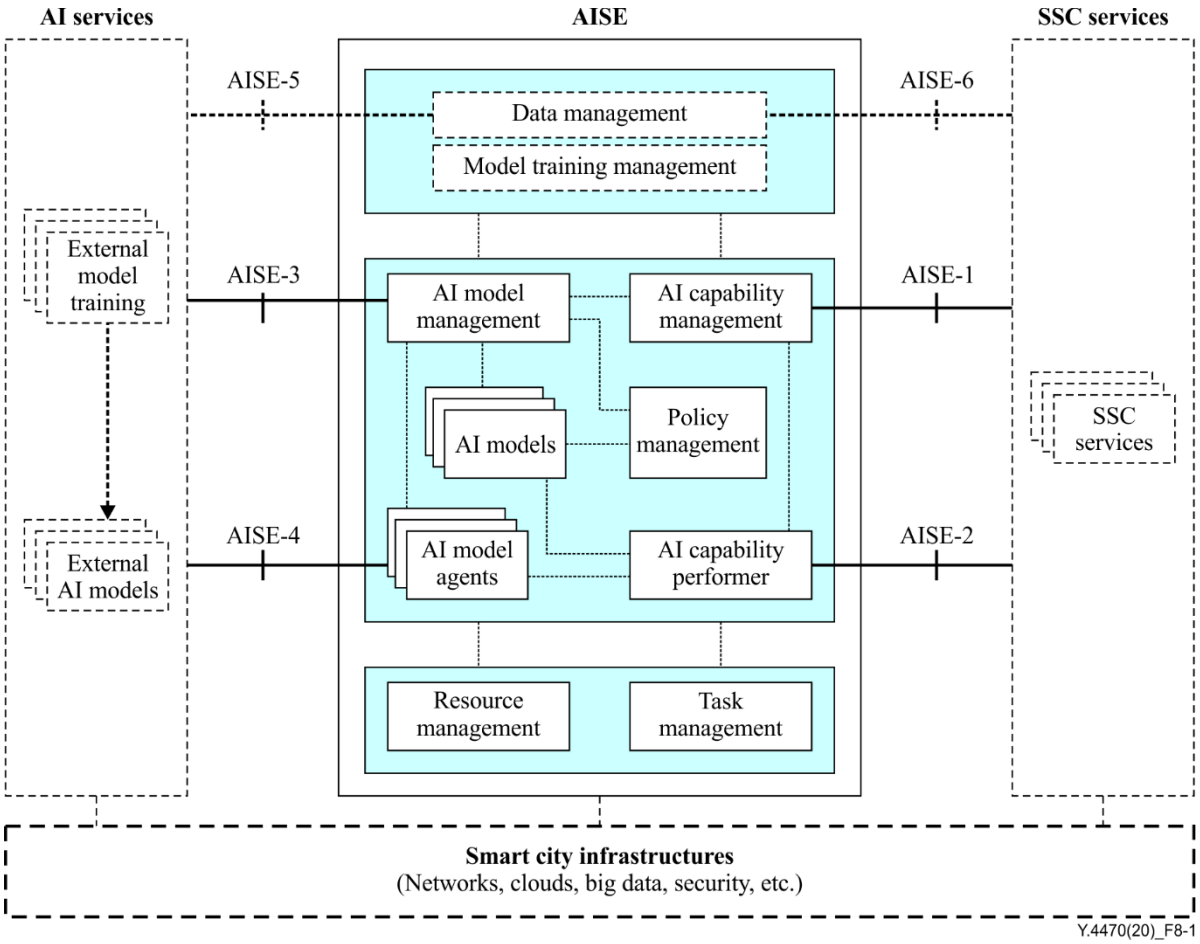

Figure 8-1 – Reference architecture diagram of AISE

AISE includes three groups of logical functional components (FCs) intended for: AI model-training and data management, supplying AI capabilities, and resource and task management.

– The FCs in the first group include resource management (RM-FC) and task management (TM-FC).

– The FCs in the second group include AI model management (AMM-FC), policy management (PM-FC), AI capability management (ACM-FC), AI capability performer (ACP-FC), and multiple AI models (AM-FC) and AI model agents (AMA-FC).

– The FCs in the third group include model-training management (MTM-FC) and data management (DM-FC).

AISE exposes a group of reference points to interact with AI services and SSC services, including:

– AISE-1: for SSC services to discover and subscribe to exposed AI capabilities in AISE;

– AISE-2: for SSC services to access the subscribed AI capabilities exposed in AISE;

– AISE-3: for AI services to deploy and expose AI capabilities in AISE;

– AISE-4: for interaction between the AI model agents of AISE and the external AI models of the AI services;

– AISE-5: for SSC data-related interaction between the AI services and AISE, with which the AI services access exposed SSC data through AISE to train their AI models;

– AISE-6: for SSC data-related interaction between AISE and SSC services.

AISE, AI services and SSC services work on the underlying smart city infrastructures (such as networks, clouds, big-data and security).

NOTE 1 – The MTM-FC utilizes the underlying resources and SSC data in AISE to train AI models. The FCs for model-training management and data management lie outside the scope of this Recommendation.

NOTE 2 – The DM-FC exposes two reference points, AISE-5 and AISE-6, to collect SSC data from SSC services and to open SSC data to other FCs or external AI services. The reference points AISE-5 and AISE-6 lie outside the scope of this Recommendation.

8.1 Resource management-functional component

The RM-FC monitors and manages underlying resources to support training AI models, supplying AI capabilities and managing SSC data in AISE. The RM-FC virtualizes the underlying resources and exposes uniform internal interfaces to leverage other FCs of AISE to utilize them.

The underlying resources may be hosted by multiple devices, which include at least:

– computational resources, such as a central processing unit and a graphics processing unit;

– storage resources;

– network resources, such as Internet protocol (IP) addresses and ports, and network bandwidth;

– micro-services, such as a timer service and messaging service.

The RM-FC, coordinating with other FCs of AISE, provides the following functionalities:

– monitoring and managing the underlying resources of one or multiple devices;

– virtualizing the underlying resources;

– exposing uniform internal interfaces to allow other FCs of AISE to utilize the virtualized underlying resources.

8.2 Task management-functional component

The TM-FC orchestrates and manages tasks in AISE, such as training AI models, supplying AI capabilities and sharing SSC data. A task can be performed by one or multiple micro-service(s) of AISE.

The TM-FC, coordinating with other FCs of AISE, provides the following functionalities:

– task orchestration and creation ;

– task monitoring and management.

8.3 AI model management-functional component

The AMM-FC manages the AI models (see clause 8.7) and AI model agents (see clause 8.8) in AISE.

The AMM-FC exposes reference point AISE-3 for external AI services to interact with AISE.

The AMM-FC, coordinating with other FCs of AISE, provides the following functionalities:

– managing the AI models (such as adding, deleting and updating the AI models);

– managing the AI model agents (such as creating, deleting, updating the AI model agents and their relationships with corresponding external AI models).

8.4 Policy management-functional component

The PM-FC provides access control for AI services to expose their AI capabilities and provides access control for SSC services to discover, subscribe to and access AI capabilities exposed by AI services. In addition, the PM-FC provides access control to expose and share SSC data with AI services.

The PM-FC, coordinating with other FCs of AISE, manages access permissions for:

– exposed AI capabilities;

– the discovery, subscriptions and accessing of exposed AI capabilities;

– exposure of SSC data;
– the discovery, subscriptions to and accessing of exposed SSC data;
– training AI models in AISE.

8.5 AI capability management-functional component

The ACM-FC manages and publishes information about exposed AI capabilities, and exposes reference point AISE-1 to support SSC services to discover and subscribe to the AI capabilities exposed in AISE.

The ACM-FC, coordinating with other FCs of AISE, through reference point AISE-1, manages information about:

– the AI capabilities exposed by the AI models;
– the AI capabilities exposed by the external AI models;
– the subscriptions to AI capabilities from SSC services.

8.6 AI capability performer-functional component

The ACP-FC exposes reference point AISE-2 to support SSC services to access subscribed AI capabilities.

The ACP-FC, coordinating with other FCs of AISE, through reference point AISE-2, provides the followed functionalities:

– supporting SSC services to access subscribed AI capabilities;
– notifying the SSC services of the status of their subscribed AI capabilities, if needed.

With reference point AISE-2, SSC services can use uniform approaches to access subscribed AI capabilities.

8.7 AI model-functional component

A group of AM-FCs provides AI capabilities, such as predicting weather, recognizing images and voices, and controlling robots. The AI models can be deployed both within and outside AISE.

AISE provides underlying infrastructures to allow the AI models to be performed.

8.8 AI model agent-functional component

The AMA-FCs interact directly with corresponding external AI models through reference point AISE-4 subject to the requests of SSC services. The AMA-FCs transfer the requests for AI capabilities from SSC services to the corresponding external AI models, and transfer the responses in the opposite direction.

An AMA-FC can interact with one or multiple AI capabilities at the same time.

The AMA-FCs, coordinating with other FCs of AISE, provide the following functionalities:

– tracking the status of exposed AI capabilities, e.g., available or unavailable;
– interacting with corresponding external AI models to support SSC services to access exposed AI capabilities.

NOTE 1 – When an SSC service subscribes to one AI capability published in AISE, if needed, AMA-FC can interact with the corresponding external AI models that expose the AI capability to check remote access permission.

NOTE 2 – The AMA-FCs can provide data format transformation between AISE and the external AI models. This Recommendation does not specify mechanisms for data or protocol format transformation between the AMA-FCs and the external AI models.

8.9 Reference points

8.9.1 AISE-1

Reference point AISE-1 is exposed by the ACM-FC, which supports SSC services to discover and subscribe to exposed AI capabilities in AISE.

8.9.2 AISE-2

Reference point AISE-2 is exposed by the ACP-FC, which supports SSC services accessing the subscribed AI capabilities, and get notifications for the status of their subscribed AI capabilities, if needed.

8.9.3 AISE-3

Reference point AISE-3 is exposed by the AMM-FC, which supports external AI services to deploy and expose AI capabilities in AISE.

8.9.4 AISE-4

Reference point AISE-4 is exposed by the AMA-FC, which supports interaction between the AI model agents of AISE and external AI models of the AI services.

9 Common capabilities of AISE

This clause provides common capabilities that correspond to the requirements listed in clause 7.

9.1 Training of AI models

AISE can provide underlying infrastructures (such as computational devices, computational frameworks, models) to support the training of AI models in AISE.

The trained AI models can be deployed in AISE, and can be retrained and updated according to its policies.

AISE may open SSC data to AI services according to the rules and policies of AISE. This Recommendation does not specify how to open SSC data to AI services.

9.2 Publication of AI capabilities

AISE is able to allow exposed AI capabilities to be performed both within and outside AISE.

AISE is able to collect information on AI capabilities to be exposed to SSC services. The information about exposed AI capabilities includes, but is not limited to:

– names of the AI capabilities;
– descriptions of the AI capabilities;
– access approaches and relevant parameters; and
– access profiles.

AISE is able to publish collected information about AI capabilities, in order to allow SSC services to discover and subscribe.

If AI models are deployed in AISE, AI services can directly expose their AI capabilities in AISE.

If an AI model is deployed outside AISE, AISE can deploy a corresponding AI model agent, which enables AISE and external AI model interaction. In this case, external AI models can use reference point AISE-3 to expose their AI capabilities.

Clause III.1 provides a reference procedure for publishing AI capabilities.

9.3 Subscription to AI capabilities

AISE is able to allow SSC services to discover and subscribe to published AI capabilities in AISE, through exposed reference point AISE-1.

AISE is able to support an SSC service to subscribe to one or more AI capability and the subscribed AI capabilities may be exposed by one or more AI services.

In the subscription process, AISE is able to validate access permissions according to the policies of AISE and the access profiles related to AI capabilities.

Alternatively, AISE is also able to connect to AI services that expose AI capabilities to negotiate access permission.

Clause III.2 provides a reference procedure for subscribing to published AI capabilities.

NOTE – This Recommendation does not specify a mechanism of interaction between AISE and AI services.

9.4 Access to AI capabilities

When an SSC service requests access to subscribed AI capabilities through exposed reference point AISE-2, AISE is able to verify the access permission, if needed.

If the AI capabilities are exposed by the AI models in AISE, then AISE is able to call the AI models to perform the requested AI capabilities. Clause III.3 provides reference procedures for accessing subscribed AI capabilities in this scenario.

If the AI capabilities are exposed by external AI models outside of AISE, then AISE is able to invoke the AI model agents to access the target AI capabilities, through exposed reference point AISE-3. Clause III.4 provides reference procedures for accessing subscribed AI capabilities in this scenario.

10 Security consideration

AISE, SSC services and AI services are usually deployed in different domains and may be in untrusted environments. AISE is required to provide security mechanisms to authorize and authenticate SSC services to discover, subscribe and access AI capabilities.

Additionally, the security mechanism should support security transportation technologies when the SSC data is transported between AISE and the SSC services, and between AISE and the AI services.

Appendix I

Working modes of AISE to provide AI services to SSC services

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

There are three types of working modes, classified by the management methods of AI capabilities in AISE: tightly coupled, loosely coupled and hybrid.

I.1 Tightly coupled working mode

In the tightly coupled working mode, AI models are tightly coupled with AISE (see Figure I.1). AISE manages the AI models and SSC data, exposes their AI capabilities and supplies them to IoT devices via SSC services.

In this working mode, AI service providers deploy external AI models (such as models M_1 … M_k) in AISE as internal AI models (such as AI models A_1 … A_k). Furthermore, AI service providers also can train their AI models in AISE using SSC data as opened by AISE.

When SSC services receive requests from IoT devices related to AI capabilities exposed by AISE, the SSC services forward them to AISE. Then AISE invokes the internal AI models to perform the requested AI services.

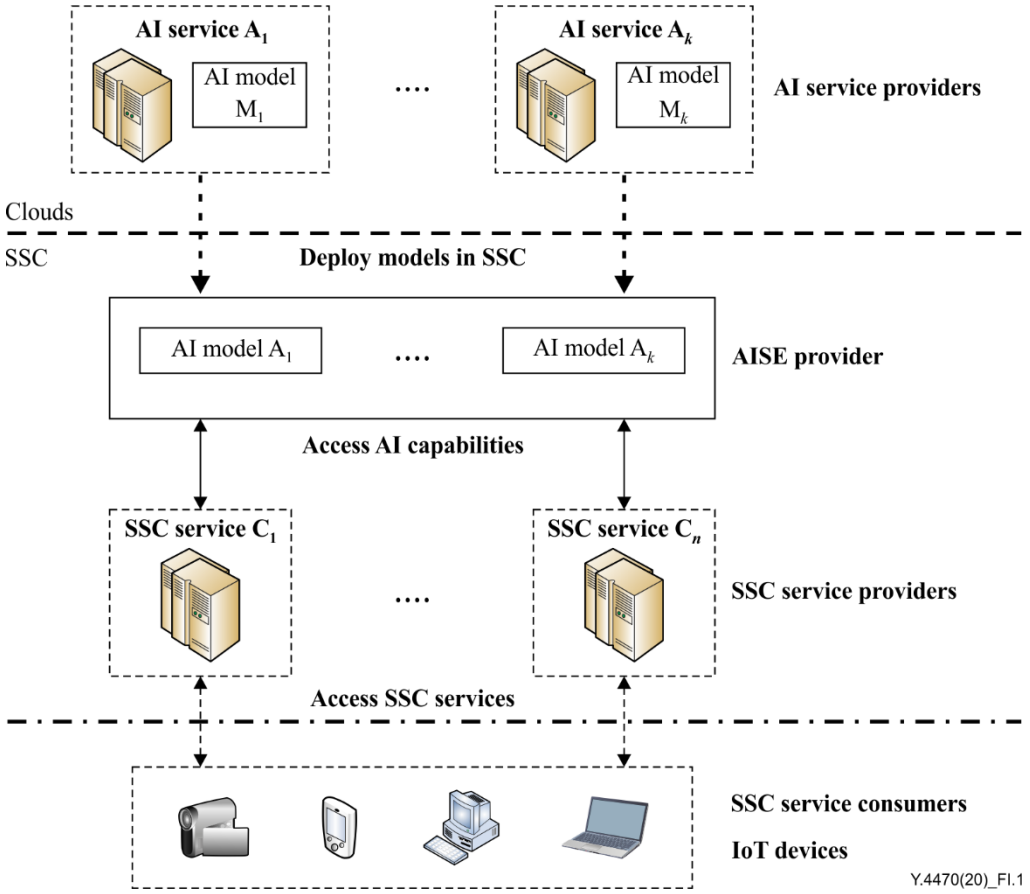

Figure I.1 – Tightly coupled working mode

I.2 Loosely coupled working mode

In the loosely coupled working mode, AI models are loosely coupled with AISE (see Figure I.2). AISE manages SSC data and supports the AI service providers to train and deploy their AI models (such as models M_1 … M_k) in SSC. These AI models are external AI models and are deployed outside of AISE.

In this working mode, AISE may create internal AI agents (such as AI model agents A_1 … A_k) corresponding to the external AI models and expose related AI capabilities. The internal AI model agents act as bridge. When SSC services receive requests from IoT devices related to AI capabilities exposed by AISE, the SSC services forward these requests to AISE. AISE then invokes the external AI models, via corresponding internal AI model agents, to perform the requested AI capabilities.

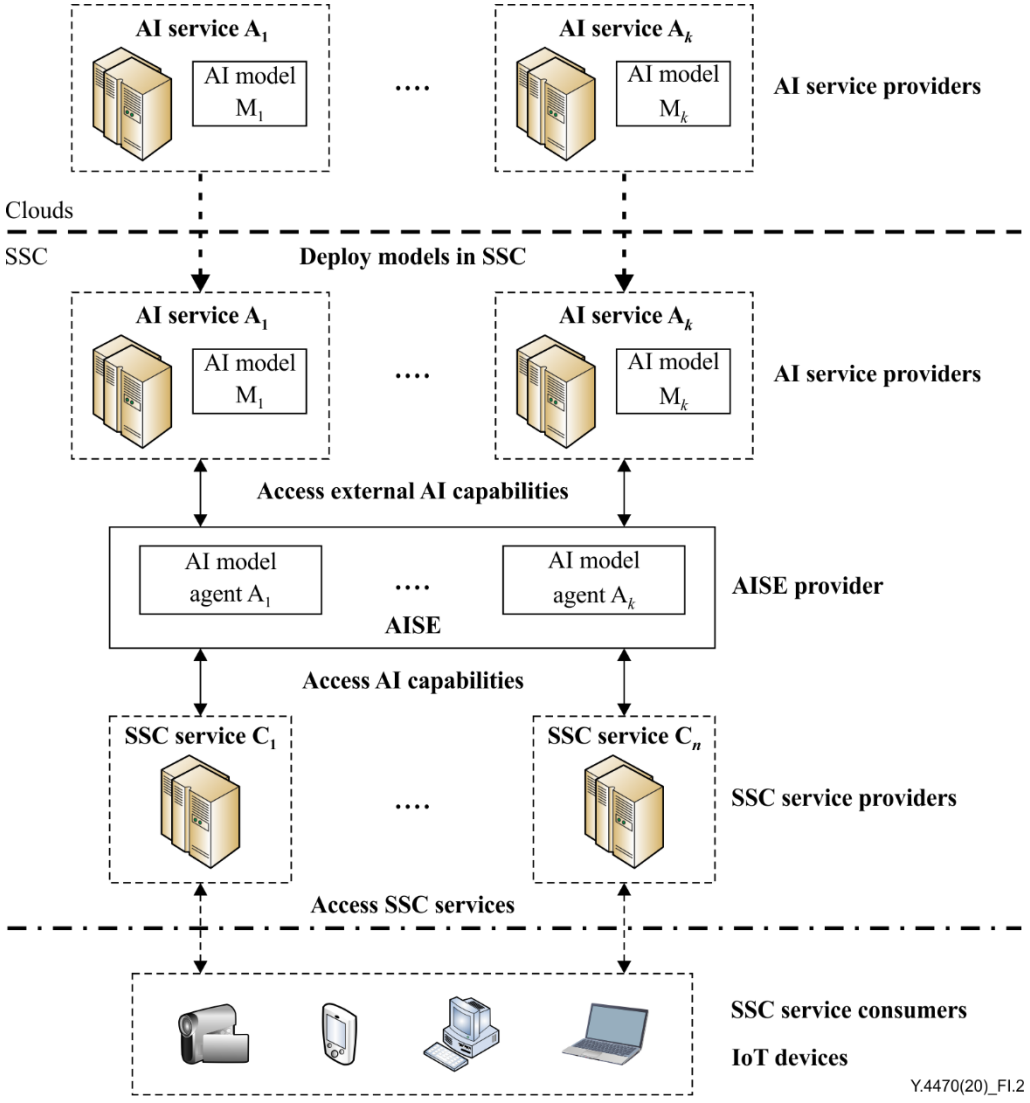

Figure I.2 – Loosely coupled working mode

I.3 Hybrid working mode

In the hybrid working mode, some AI models are tightly coupled with AISE, and some AI models are loosely coupled with AISE.

In this working mode, when SSC services receive requests, from IoT devices, related to AI capabilities exposed by AISE, the SSC services forward these requests to AISE. If the AI capabilities are performed by external AI models, the AI model agents forward the requests to the corresponding AI services to perform the requested AI capabilities. If the AI capabilities are performed by internal AI models, AISE then invokes internal AI models to perform the requested AI capabilities.

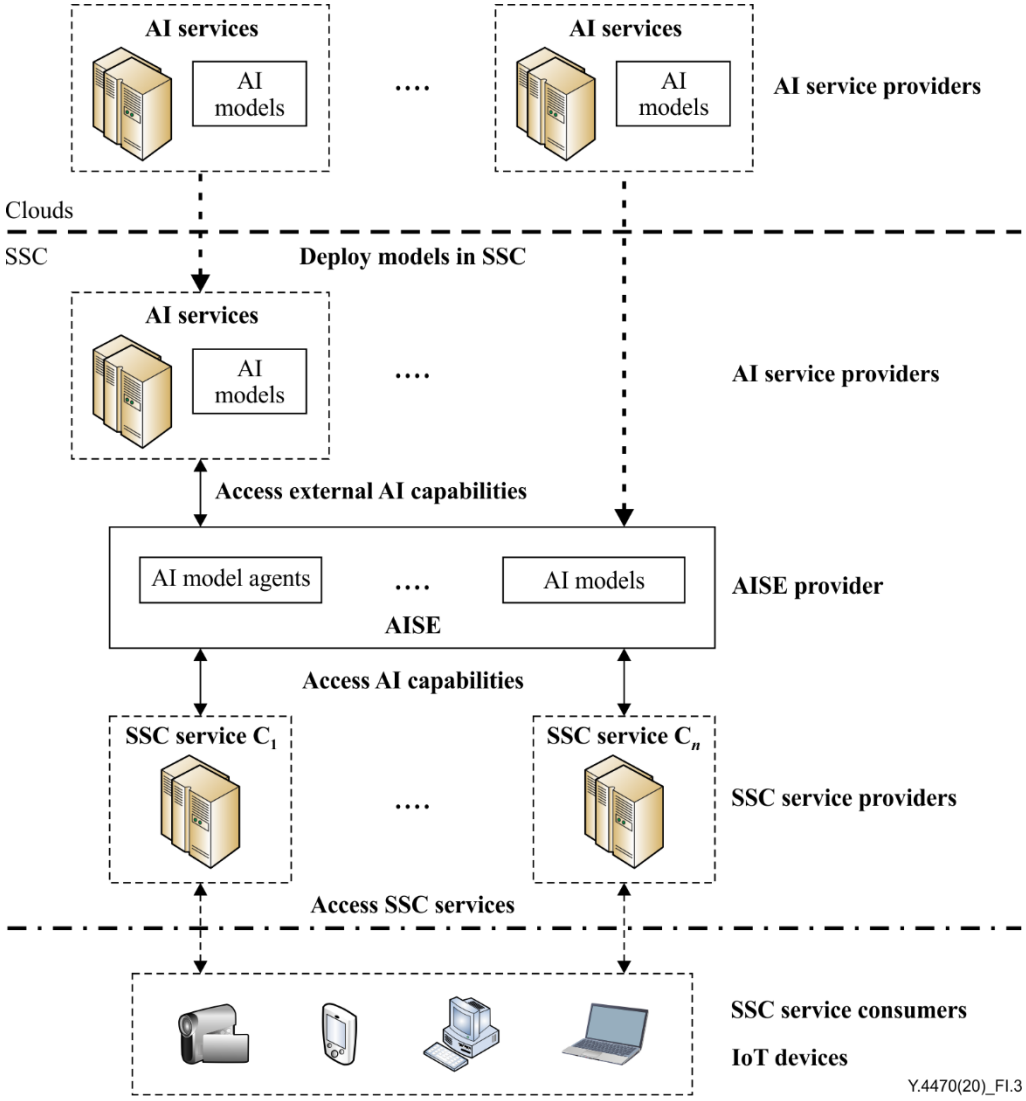

Figure I.3 – Hybrid working mode

Appendix II

Use cases of AISE for SSCs

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

This appendix provides use cases to illustrate the concept of AISE.

II.1 Use case: promoting smart traffic controlling services

This case shows smart traffic controlling (STC) services in an SSC that utilizes AISE to integrate and access AI capabilities for SSC traffic control.

The STC services can collect a large volume of traffic-related data from diverse resources (e.g., city citizens, traffic sensors and traffic tools) in a short time. The data format may be, for example, video, audio or text. Usually STC services need to process data in real time and make decisions to control SSC traffic.

Generally, STC service providers are the local government of the SSC or its contractors, which usually do not have enough technical and financial resources to develop their AI capabilities. Therefore, it is natural that STC service providers will integrate the AI capabilities of third parties, which, however, are usually not particular to a special STC service, because it may be that third parties do not get enough traffic-related SSC data to train their AI capabilities for STC services.

AISE can be deployed by a government or its contractors; this is shown in Figure II.1. AISE is in the SSC and it can collect traffic-related data through STC services.

AI service providers can deploy their common AI capabilities (e.g., for video, audio or text) in AISE, and if permitted, they also can design and train local AI capabilities in AISE. Because of the use of local traffic-related data, locally trained AI capabilities are more applicable to special STC services.

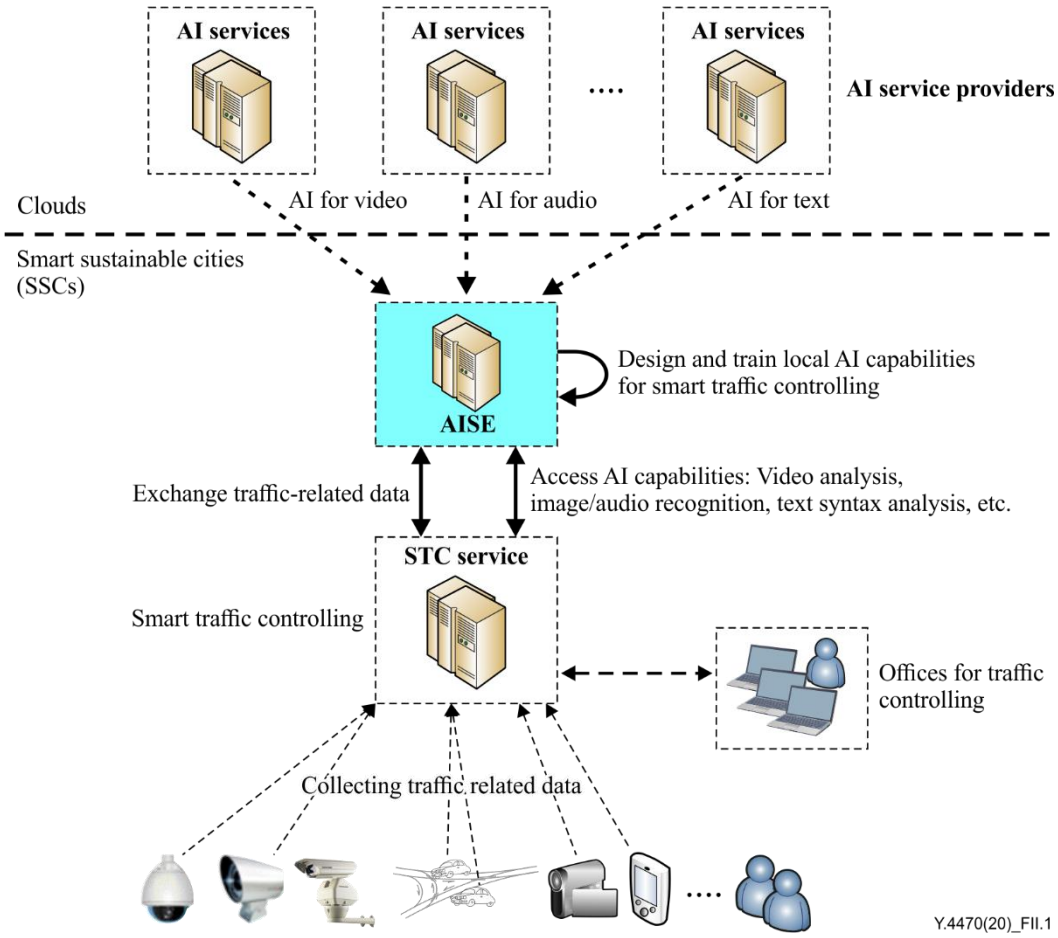

Figure II.1 – Use case for smart traffic controlling services

In this case, through AISE, STC services can integrate and access applicable AI capabilities for SSC traffic control.

II.2 Use case: promoting smart appliance voice control services

This case shows a smart appliance voice control (SAVC) service in smart homes using AISE to process and understand users' voices.

The SAVC service enables users to simply speak to a terminal (e.g., smart phone, smart speaker) in a natural way to open, close or operate appliances conveniently, instead of using specific applications.

Generally, SAVC service providers are smart appliance manufacturers, which only integrate communication modules into their traditional home appliances to make them smarter, but do not have enough AI capabilities to develop a voice control service. For this purpose, AISE may help SAVC service providers integrate third-party AI capabilities easily and flexibly.

As shown in Figure II.2, the SAVC service provider can access AISE, which contains the common AI capabilities for audio deployed by the AI service provider. In this case, the SAVC service receives voice input from users and sends it to AISE for processing, then the instructions derived from the input by relevant AI capabilities in AISE is transmitted back to smart appliances to respond to user requests.

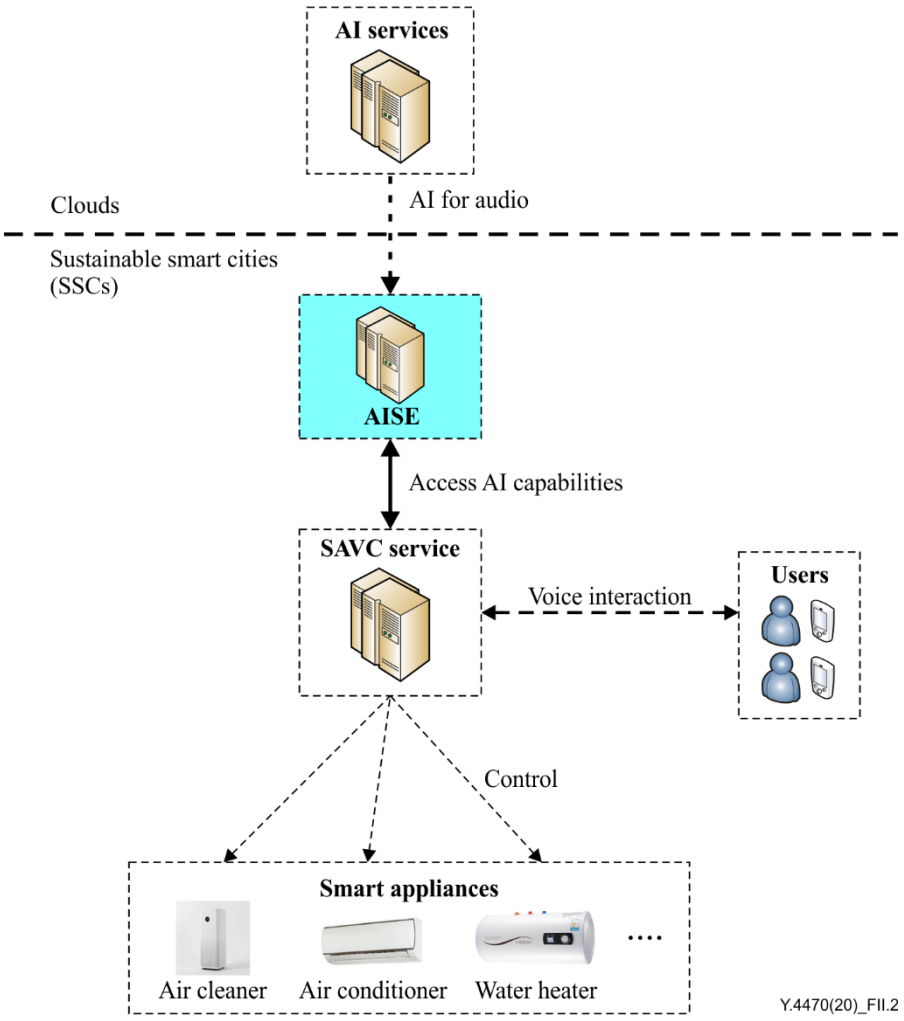

Figure II.2 – Use case for smart appliance voice control service

II.3 Use case: promoting smart urban geographical information services

This case shows a smart urban geographic information (UGI) service in an SSC integrating and accessing AI capabilities exposed by AISE to process SSC geographical information.

The UGI service can collect a large volume of urban geographical data from diverse resources in an SSC in a short time, such as city geographical information, digital maps, vehicle radars, cameras, traffic sensors and tools (see Figure II.3).

Using the AI capabilities exposed by AISE (e.g., related to the processing of images, video, audio, text and data searching), the UGI service can reconstruct geographical information according to user requests.

Take the three-dimensional (3D) map reconstruction as an example.

The UGI service can reconstruct and simulate the real world with 3D effects and bound the 3D maps with some other information (e.g., hotels). Making 3D maps is not only based on multiple data sources including at least data collected in real time, historical collected data and location data, but also on AI models and AI algorithms.

With exposed AI capabilities (such as for voice intelligent interaction), the UGI service can more accurately understand the needs of users and output more information to them. For example, users only need to input their demands to book hotels by voice and the 3D maps can quickly recommend hotels according to user preferences, while also helping users complete the reservation, plan the best route and remind them of the departure time. It can provide users with personalized one-stop travel decisions.

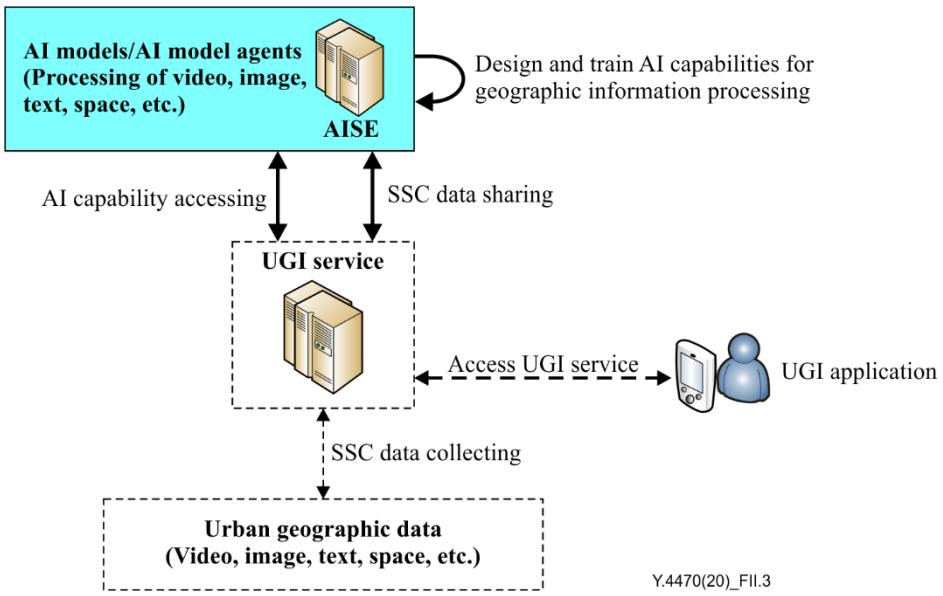

Figure II.3 – Use case for promoting smart urban geographical information services

In this case, through AISE, the UGI service can integrate and access applicable AI capabilities, and provide citizens and business entities with more geographical information.

Appendix III

Common procedures of AISE for SSCs

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

This appendix provides some common procedures to illustrate the reference architectures (see clause 8) and common capabilities (see clause 9) of AISE.

III.1 Publication of the AI capabilities to be exposed

Figure III.1 shows two common procedures of an AI service to expose and publish its AI capabilities in AISE; the major procedures are outlined in steps 1 to 6.

Step 1: The AI service registers its AI capabilities to AISE through the reference point AISE-1. The registration data provided by the AI service includes the information on the AI service and the information on the AI capabilities to be exposed (see clause 9.2).

Steps 2 and 3: The AMM-FC, collaborating with other FCs of AISE, processes the registration request, including validating the information and checking permissions.

If the registration request is validated and accepted, the AI capabilities are exposed in AISE and relevant information is published by AISE.

Steps 4 and 5: AISE sends a response to the AI service. The response information includes whether the registration request is accepted, whether the AI capabilities are exposed and the publishing information if published.

Step 6: If the registration request is accepted and exposed AI capabilities are published, the AI service should update the status of the AI capabilities to AISE when the status is changed.

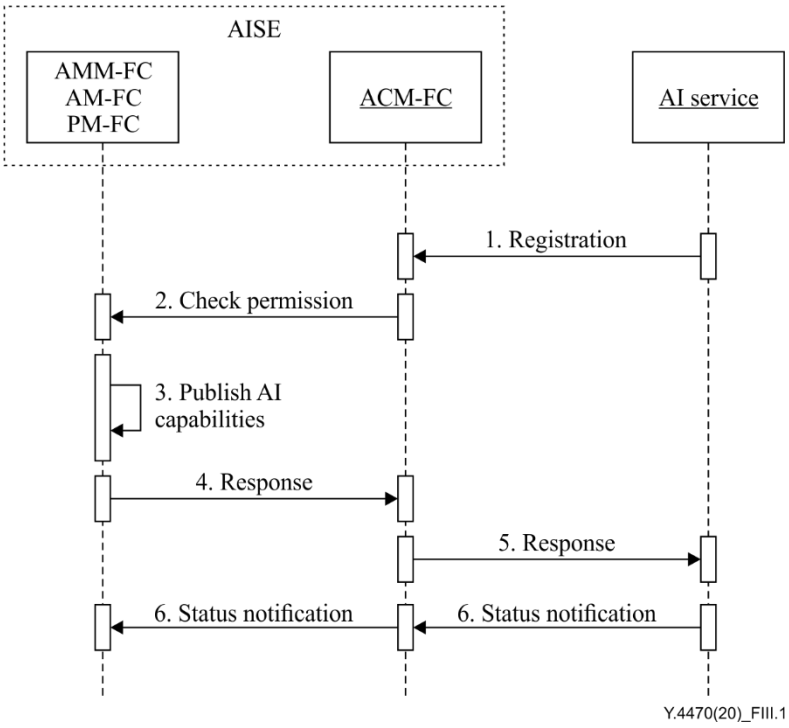

Figure III.1 – Flow for exposing and publishing AI capabilities

III.2 Subscription to exposed AI capabilities

Figure III.2 shows the common procedures of an SSC service subscribing to exposed AI capabilities in AISE; the major procedures are outlined in steps 1 to 7.

Step 1: The SSC service sends a subscription request to AISE to subscribe to one or a group of exposed AI capabilities. The target AI capabilities can be exposed by one or more AI services.

Step 2: AISE validates the subscription request and checks access permission of the SSC service for subscribing to the target exposed AI capabilities.

AISE checks access permission according to the access policies of the target exposed AI capabilities and the policies of AISE.

AISE, if needed, can get external access permission from the AI services that expose the target AI capabilities. In this case, if the target AI capabilities are provided by different AI services, AISE connects them one by one.

Steps 3, 4, 5 and 6: After checking the access permission, AISE sends a subscription response to the SSC service and sends a subscription notification to the AI services that expose the target AI capabilities.

If the subscription request is validated and accepted, the subscription response to the SSC service includes information about subscribed AI capabilities (see clause 9.2). In this case, the subscription notification sent to AI services includes subscription information (e.g., who is subscribing to the AI capabilities and which AI capabilities are subscribed).

If the subscription request is not validated or not accepted, the subscription response to the SSC service will include the rejection information and AISE may not send subscription information to the AI services.

Step 7: If the subscription request is accepted, AISE sends the SSC service the status notification that is received from the AI services continuously; otherwise, AISE will not send anything to the SSC service.

NOTE – From the perspective of the SSC service, it is transparent that the ACM-FCs interact with AI services which exposing AI capabilities. The SSC service subscribes to the published AI capabilities from AISE and does not interact directly with the AI services.

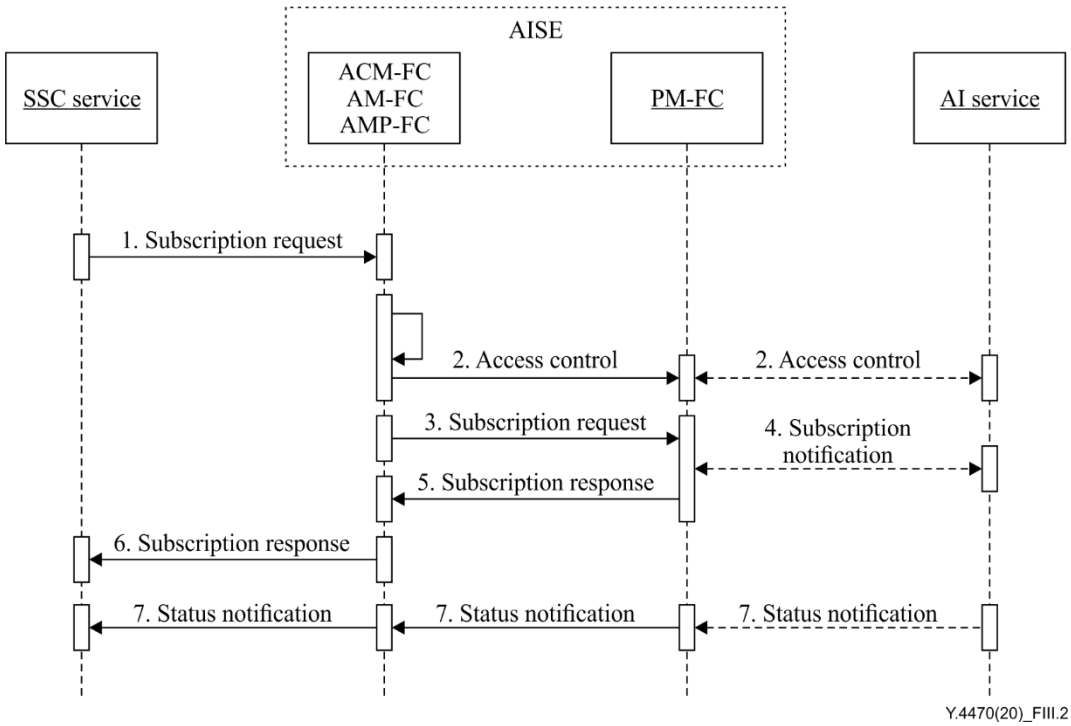

Figure III.2 – Flow for subscribing exposed AI capabilities

III.3 Accessing the subscribed AI capabilities in AISE

Figure III.3 shows the common procedures of an SSC service accessing subscribed AI capabilities through AISE; the major procedures are outlined in steps 1 to 5.

Step 1: The SSC service sends AISE the request to access the subscribed AI capabilities, through the reference point AISE-2. In the access request, it may include one or more AI capabilities and the target AI capabilities may be exposed by one or more AI services.

Step 2: AISE validates the access request and checks access permission. If part or all of the target AI capabilities in the access request are not subscribed, AISE may reject the access request.

NOTE – There are many methods to control access permission. The method in step 2 is a simple example. This Recommendation does not limit the methods to control access permission.

Steps 3, 4 and 5: If the access request is rejected, AISE sends the SSC service the access response, which includes the reasons for the rejection. AISE then ends the processes for the access request.

If the access request is accepted, the ACP-FCs of AISE send access requests to the AI services as exposing the target AI capabilities. In this case, if the target AI capabilities are exposed by different AI services, AISE will call the corresponding AM-FC to connect the appropriate AI services.

AISE receives the access response from the AI services and forwards it to the SSC service.

When the access response is received for its access request, the SSC service may end this access request.

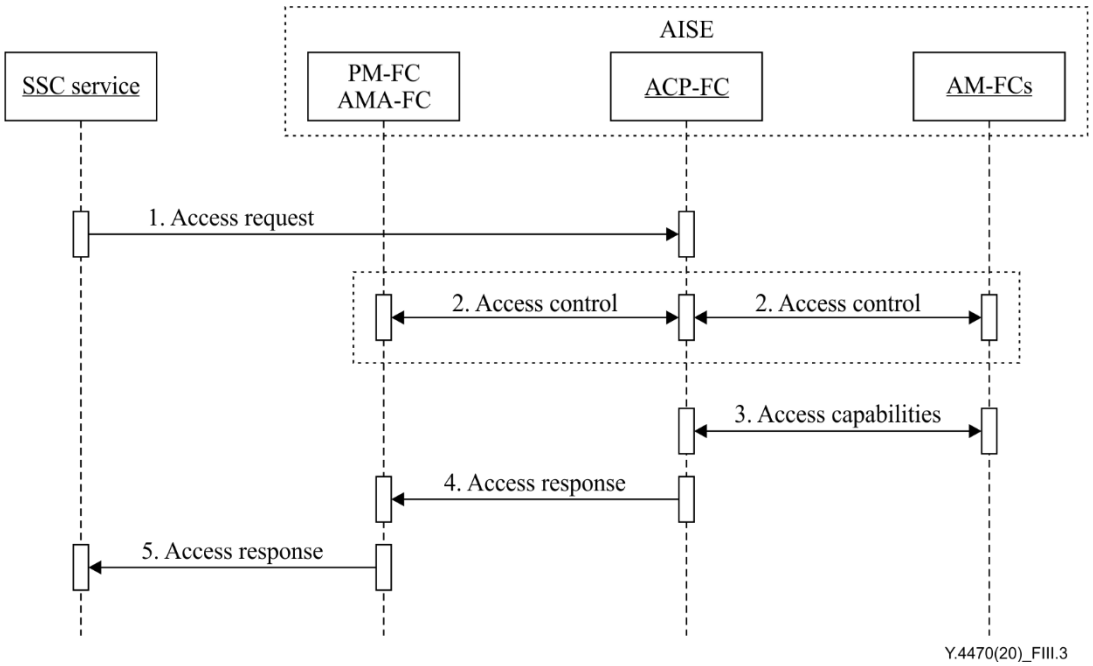

Figure III.3 – Flow for accessing subscribed AI capabilities in AISE

III.4 Accessing the subscribed AI capabilities outside of AISE

Figure III.4 shows the common procedures of an SSC service to access subscribed AI capabilities through AISE. The main difference is the AI capabilities are performed by external AI models through the supports of the AMA-FCs.

The major procedures are outlined in steps 1 to 5.

Step 1: Same as step 1 in clause III.3.

Step 2: Similar to step 2 in clause III.3.

NOTE – The access permission may be checked further by external AI services because they provide the requested AI capabilities. Furthermore, this Recommendation does not limit the methods to control access permission.

Steps 3, 4 and 5: The ACP-FC forwards the requests to the AMA-FC that is bound to the requested AI capabilities, and then the AMA-FC interacts with external AI services (invoking AI capabilities) according to the requests and forwards the responses from external AI services to the SSC service.

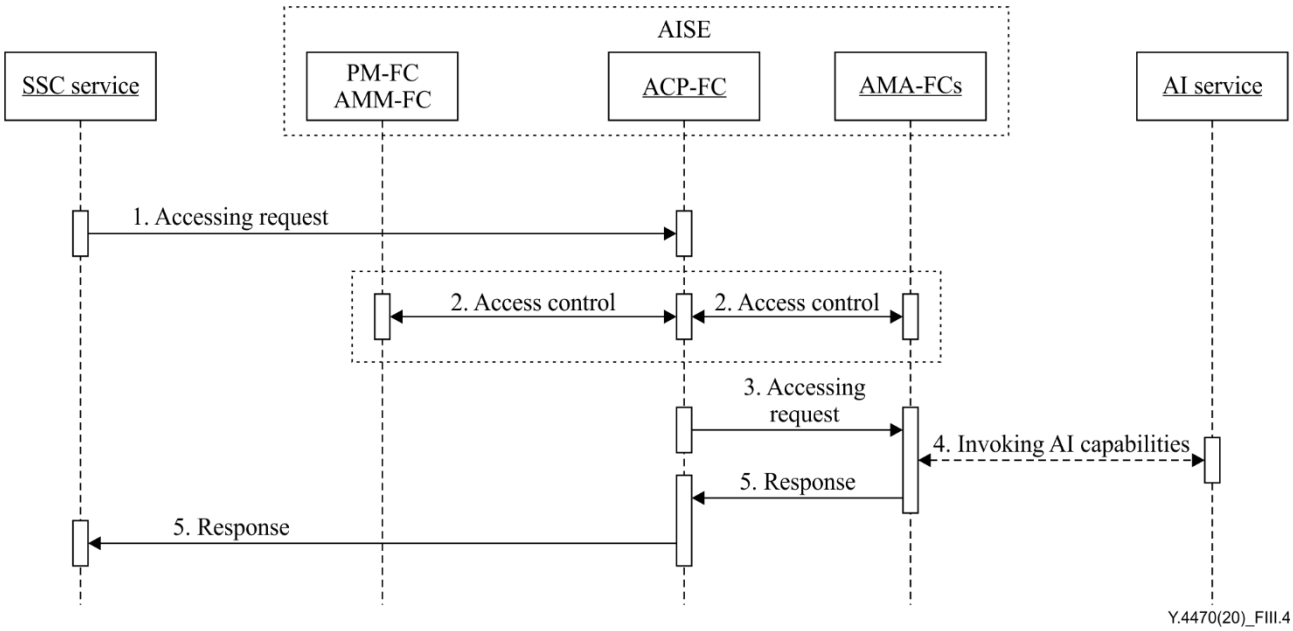

Figure III.4 – Flow for accessing subscribed AI capabilities outside of AISE

Bibliography

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

[b-ITU-T Y.3172] Recommendation ITU-T Y.3172 (2019), *Architectural framework for machine learning in future networks including IMT-2020*.

[b-ITU-T Y.4900] Recommendation ITU-T Y.4900/L.1600 (2016), *Overview of key performance indicators in smart sustainable cities*.

[b-ITU-R M.1224-1] Recommendation ITU-R M.1224-1 (2012), *Vocabulary of terms for international mobile telecommunications (IMT)*.

[b-ETSI GR ENI 004] ETSI GR ENI 004 V2.1.1 (2019); *Experiential networked intelligence (ENI); Terminology for main concepts in ENI*.

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020