ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.4220 (03/2023)

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 – Requirements and use cases

---

Requirements and capability framework of abnormal event detection system for smart home

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
Computing power networks	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.4220

Requirements and capability framework of abnormal event detection system for smart home

Summary

By deploying Internet of things (IoT) devices, smart home makes use of IoT technologies to collect ambient information, detect abnormal events at home and report to relevant personnel or institutions.

In this Recommendation the term "abnormal event" is intended as meaning a human health injury event at home. Examples of abnormal events at home include, but are not limited to, coughing, dyspnoea, falls, headache, quiescent behaviour, sleep apnoea, stroke, transient ischemic attacks.

Such a smart home system aims to reduce injuries and casualties at home. Various products have emerged in this field. However, the lack of standards could limit the abilities of vendors to meet the rising demands across the globe, such as lower false alarm rates, more convenient deployment, better handling of privacy concerns, etc. In order to ensure the system quality, Recommendation ITU-T Y.4220 specifies the requirements and capability framework of the abnormal event detection system (AEDS) for smart home.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4220	2023-03-28	20	11.1002/1000/15483

Keywords

Abnormal event detection, capability, Internet of things, IoT, requirements, smart home.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4220

Requirements and capability framework of abnormal event detection system for smart home

1 Scope

This Recommendation specifies the requirements and capability framework of the abnormal event detection system (AEDS) for smart home. It aims to report the abnormal event to relevant personnel or institutions in a timely manner, and as such to reduce injuries and casualties.

In this Recommendation the term "abnormal event" is intended as meaning a human health injury event at home. Environment related abnormal events, such as fire and flood, are out of the scope of this Recommendation.

NOTE – Examples of abnormal events at home include, but are not limited to, coughing, dyspnoea, falls, headache, quiescent behaviour, sleep apnoea, stroke, transient ischemic attacks.

The scope of this Recommendation includes:

– Introduction of abnormal event detection system (AEDS) for smart home

– Requirements of abnormal event detection system for smart home

– Capability framework of abnormal event detection system for smart home

Use cases of AEDS are provided in Appendix I.

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

[ITU-T Y.4105] Recommendation ITU-T Y.4105/Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.

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 device [b-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.

3.1.3 Internet of things (IoT) [b-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.

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

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	3rd Generation Mobile Communication Technology
4G	4th Generation Mobile Communication Technology
5G	5th Generation Mobile Communication Technology
AEDS	Abnormal Event Detection System
API	Application Programming Interface
GPU	Graphics Processing Unit
IoT	Internet of Things
MSD	Minimum Set of Data
NB-IoT	Narrow Band Internet of Things
PII	Personally Identifiable Information
WHO	Word Health Organization
WiFi	Wireless Fidelity

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 Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement needs 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 Introduction of abnormal event detection system for smart home

Abnormal events happening at home may require assistance to the person in need. If the abnormal event is not handled in a timely manner, it may cause injures or even death.

For example, falls are the largest threat to elderly people and those in need of assistance. According to the Word Health Organization (WHO), falls cause over 37.3 million severe injuries and 646 000 deaths per year [b-WHO Falls]. Even though a person may not have a physical injury after a fall event, psychological limitations may affect their life. Estimates suggest that between 25 and 50 percent of older adults are fearful of falling and half of them will limit their activities as a result. Such fear of falling will impact the quality of life for elderly people.

Other examples of abnormal events at home are diseases affecting sleep, such as sleep apnoea, stroke and transient ischemic attacks. Approximately a quarter of all strokes occur during sleep. It is difficult for people to reach out for assistance during sleep, and also some treatments may need health information at the moment when the first symptoms began. In the latter case treatments selection is made difficult due to the lack of information.

The maturity of Internet of things (IoT) technology and the widespread deployment of networks provides the necessary infrastructure conditions for deployment of abnormal event detection system (AEDS) for smart home. By deploying IoT devices, smart home may adopt IoT technology to provide abnormal event detection services. With emerging IoT technologies to collect and analyse the environment information of the home, the abnormal event may be detected and notified, reducing injuries and casualties.

Figure 1 shows an overall conceptual diagram of abnormal event detection system for smart home.

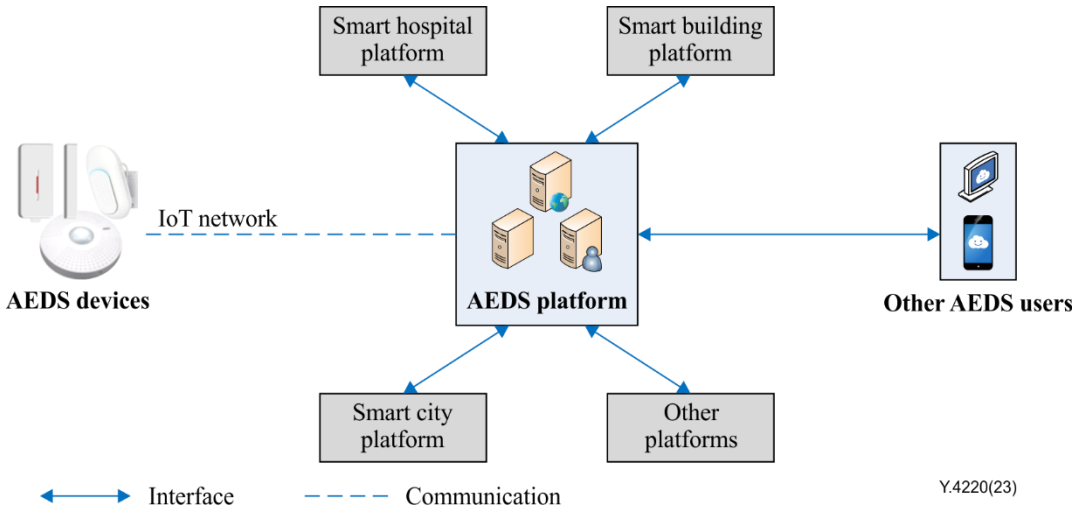

Figure 1 – Overall conceptual diagram for abnormal event detection system for smart home

Devices of abnormal event detection systems (AEDS) collect various data related to human health, such as body movement, posture, respiration, and heartbeat. Examples of AEDS devices include, but are not limited to, smart door locks to prevent patients from going out alone and getting lost, and millimetre-wave radars to detect fall events and/or abnormal heart rate and so on.

AEDS devices consist of sensors connected to an IoT network. The IoT network enables the interaction between AEDS devices and the AEDS platform. The platform is responsible for collecting and managing data. It provides the resulting information to users, including AEDS devices, medical assistance providers, third party applications and other platforms.

Other AEDS users such emergency contacts and medical assistance providers can keep abreast of the health status of the elderly through the AEDS platform, e.g., by means of mobile phone or computer.

NOTE – The AEDS platform may interface with other platforms, such as smart hospital platforms, smart building platforms and smart city platforms, for exchanging mutually beneficial information as shown in Figure 1. In some scenarios, the AEDS platform may even be integrated within a larger scope system such as a smart city system.

7 Requirements of abnormal event detection system for smart home

In addition to the common requirements specified in [ITU-T Y.4100], specific requirements for abnormal event detection system for smart home are listed in clauses 7.1 to 7.3.

7.1 Requirements of AEDS platform

The following are the AEDS platform requirements:

1 Information processing requirements

- The AEDS platform is required to record the abnormal event alarm reported by the AEDS devices.
- The AEDS platform is required to record contact information of emergency contacts and medical assistance providers.
- The AEDS platform is required to protect any personally identifiable information (PII) by applying appropriate information security management when an AEDS device generates PII.
- The AEDS platform can optionally to record the data collected from the AEDS devices.

2 Operation requirements

- The AEDS platform is required to provide abnormal detection capability to judge whether an abnormal event happened by using the data received from the AEDS devices.
- The AEDS platform is required to have the capability to filter out false alarms before contacting emergency contacts and medical assistance providers.
- The AEDS platform is recommended to display and manage the abnormal event process from the time of abnormal event occurs.
- The AEDS platform can optionally provide automatic notification to emergency contacts and medical assistance providers.

3 Data retention requirements

- The AEDS platform is required to delete the related raw data collected from the AEDS devices once the necessary procedures for information processing have been completed.

4 Interface requirements

- The AEDS platform is required to provide a test interface for the platform self-inspection.

7.2 Requirements of AEDS devices

1 Sensing related requirements

- The AEDS device is required to acquire data related to human health.
- The AEDS device is recommended to be non-intrusive.

NOTE – Wearable devices are not recommended because they imply the support of requirements such as their charging or wearing at all times. Cameras are not recommended because they collect person's image, which may cause privacy concerns.

2 Computation related requirements

- The AEDS device is required to report the abnormal event alarm information to the AEDS platform using minimal set of data (MSD).
- The AEDS device is recommended to have capability to filter out false alarms before reporting to AEDS platform.

– The AEDS device can optionally provide abnormal detection algorithms to judge whether an abnormal event happened by using the raw data collected from the AEDS devices.

3 Interface requirements

– The AEDS device is required to provide a test interface to the device self-inspection.

4 Information processing requirements

– The AEDS device is required to protect any PII by applying appropriate information security management when it generates PII.

– The AEDS device is recommended not to generate any PII.

7.3 Requirements of the network

– The AEDS network is recommended to be protected from home electricity supply failures.

NOTE – WiFi is considered to depend on home electricity supply whereas 5G and NB-IoT are not. When the AEDS network depends on the home electricity supply, the reliability of the system may be reduced.

8 Capability framework of abnormal event detection system for smart home

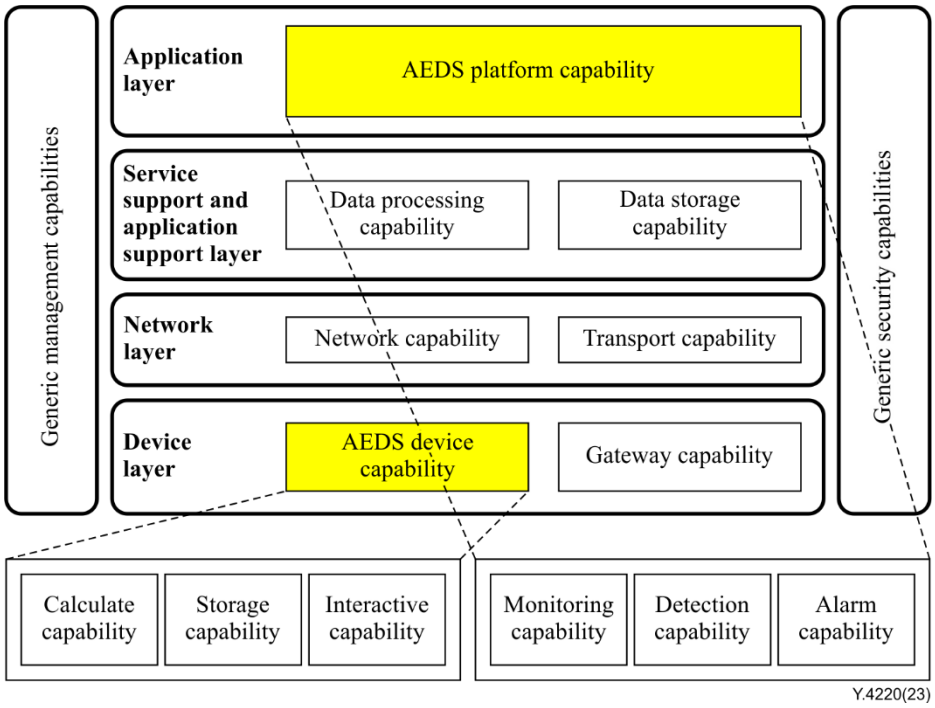

Figure 2 – Capability framework of abnormal event detection system for smart home

8.1 Capabilities of the application layer

According to AEDS platform requirements described in clause 7.1, the AEDS platform capability includes monitoring, detection and alarm capabilities. The details of these capabilities are described in clauses 8.1.1 to 8.1.3.

8.1.1 Monitoring capability

According to the requirements described in clause 7.1, the monitoring capability includes but is not limited to:

– Collecting data from indoor sensing equipment and monitoring data continuously based on time stamps. The collected data can be the data after desensitization or the monitoring results after AEDS calculation.

– Deleting the raw monitoring data saved on the platform once the necessary procedures for information processing have been completed.
– Grasping the operating conditions of the indoor monitoring equipment. When the equipment has abnormal conditions (such as abnormal offline, repeated offline, inaccurate clock), the AEDS platform can promptly remind the user to repair or replace the equipment.
– Obtaining the device location for calling the hospital.
– Providing the ability to monitor the normal operation of the test equipment and test system.

8.1.2 Detection capability

According to the requirements described in clause 7.1, the detection capability includes but is not limited to:

– Providing a variety of anomaly detection algorithms according to the identified purposes, such as fall detection, sleep apnoea detection, choking detection, etc.
– Providing a variety of data-supported algorithms to support alternative data solutions. For example, in the case of fall detection, if a camera is installed in the home, the platform calls a video-based fall detection algorithm; if there is no camera, but a millimetre-wave radar is installed, then the platform calls a fall detection algorithm based on point cloud data.
– Providing the capability to record the abnormal event process.

8.1.3 Alarm capability

According to the requirements described in clause 7.1, the alarm capability includes but is not limited to:

– Providing external warning capabilities. When a dangerous event has occurred among indoor personnel, the platform can inform emergency contacts or community service personnel of the event.
– Recording the city's hospital information and contact details.
– Providing the ability to search for the nearest hospitals.
– Providing the ability to call the ambulance or plan the shortest route based on distance and departments when emergencies occur.
– When detecting an abnormal event, the AEDS platform does not immediately alert, and leaves a certain buffer time to judge whether the abnormal event is mis-detected.

NOTE – In some pre-defined scenarios, the AEDS platform needs to alert immediately. e.g., for families that have installed sound collection devices, if the residents call for help, the AEDS platform needs to alert immediately.

– Providing the ability to control AEDS device alarms.

8.2 Capabilities of the device layer

According to AEDS device requirements described in clause 7.2, the AEDS device capability includes computing, storage and interactive capabilities. The details of these capabilities are described in clauses 8.2.1 to 8.2.3.

8.2.1 Computing capability

According to the requirements described in clause 7.2, the computing capability includes but is not limited to:

– Providing computing capability to perform data analysis, and knowledge graph calculations.
– Providing computing capability for data encryption or desensitization operations in order to protect user privacy.

8.2.2 Storage capability

According to the requirements described in clause 7.2, the storage capability includes but is not limited to:

– Providing the ability to store raw monitoring data, analysis results and algorithm models.

– Providing the ability to store indoor device parameter configurations and set the parameters to AEDS platform for backup.

– Deleting the raw data stored in the AEDS device periodically, although abnormal data and device data need to be saved separately in AEDS devices and manually deleted by the user.

8.2.3 Interactive capability

According to the requirements described in clause 7.2, the interactive capability includes but is not limited to:

– Providing an interactive page for users to configure the settings.

– Providing an interactive method for users to cancel error alarms.

– Providing an interactive method for testing the system and whether the AEDS device can function correctly.

8.3 Capabilities of the network layer

According to the requirements described in clause 7.3, the capabilities of the network layer include but are not limited to:

– Support of independent home network facilities installed in home (e.g., WiFi) in order to ensure that the AEDS device can send alarms to the AEDS platform through the network in case of emergency, e.g., power outage.

NOTE – The AEDS device can use 3G/4G/5G and other means to access the network.

Appendix I

Use cases of AEDS

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

I.1 Fall monitoring for the elderly

The AEDS device is installed in the user's home and collects the posture information of the elderly. The AEDS device can collect human posture data including camera, millimetre-wave radar, etc. According to the different AEDS devices installed in the home, there are two fall monitoring scenarios.

1) The AEDS device installed in the home acts as a camera, and does not support fall detection algorithms – see Figure I.1.

Most video-based fall detection algorithms are deep learning algorithms. Running deep learning models requires computing resources, such as a graphics processing unit (GPU), and it is difficult for devices installed in the home to support them. In this case, data needs to be uploaded to the AEDS platform and processed by the AEDS platform.

Fall monitoring for the elderly by camera has the following steps:

a Data collection: The camera collects video and carries out data encryption or desensitization operations in order to protect user privacy.

b Data transmission: The AEDS device uploads the data to the AEDS platform through a network module.

c Fall detection: The AEDS platform uses the fall detection algorithm to determine whether the elderly person has fallen. If the AEDS platform detects a fall event, it issues an instruction to the AEDS device and the AEDS device gives an alarm.

d Alarm confirmation: If the elderly person at home does not cancel the alarm within the set time, the AEDS platform sends an alarm message to the guardian or community to confirm whether the elderly person needs help.

e Data deletion: After the detection, if no fall event is found, both AEDS platform and AEDS device delete the saved raw video after a predetermined time.

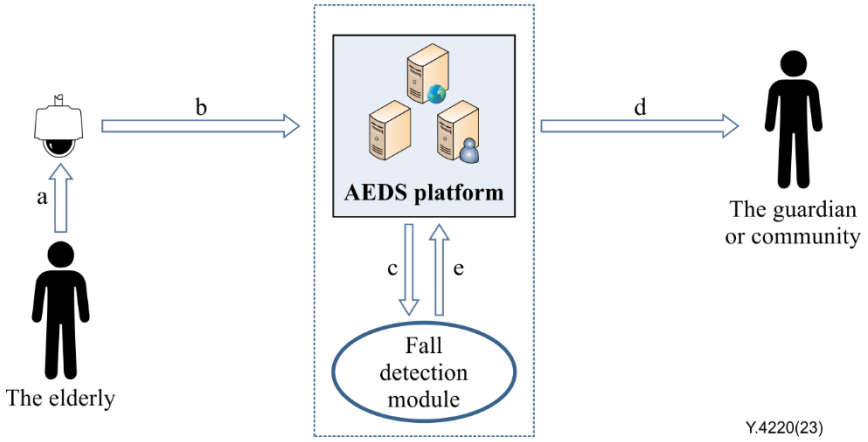

Figure I.1 – Use case of fall monitoring for the elderly with AEDS device installed in the home acting as a camera

2) The AEDS device installed in the home acts as a millimetre-wave radar, and supports fall detection algorithms – see Figure I.2.

A millimetre-wave radar can collect point cloud data of a body [b-ISO 20685-2]. Based on the point cloud data, some machine learning algorithms such as clustering algorithms can be used to calculate the centre of gravity. Then features such as height, inclination angle and speed can be calculated. These features can be used to determine whether a fall has occurred. This algorithm needs low computing resources and can also be implemented in the home without the AEDS platform support. In this case, data can be processed by the AEDS device and the AEDS device uploads the result to the AEDS platform.

Fall monitoring for the elderly by millimetre-wave radar comprises the following steps:

a Data collection: The millimetre-wave radar collects point cloud data.

b Fall detection: The AEDS device uses the fall detection algorithm to determine whether the elderly person has fallen. If the AEDS device detects a fall event, it gives an alarm and uploads the abnormal data and result to the AEDS platform after data encryption or desensitization.

c Alarm confirmation: If the elderly person at home does not cancel the alarm within the set time, the AEDS platform sends an alarm message to the guardian or community to confirm whether the elderly person needs help.

d Data deletion: The raw data stored in the AEDS device is deleted periodically. The abnormal data is manually deleted by the user after a predetermined time.

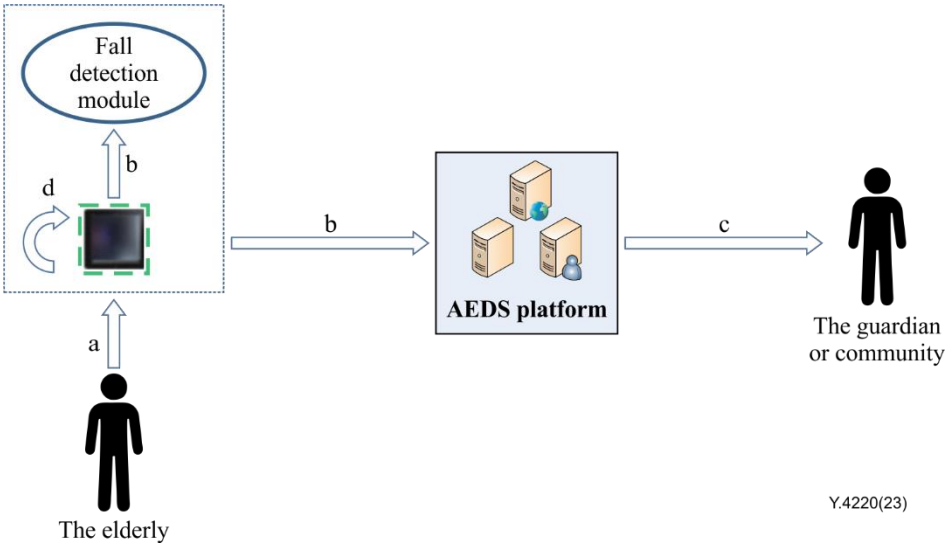

Figure I.2 – Use case of fall monitoring for the elderly with the AEDS devices acting as a millimetre-wave radar

Bibliography

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

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

[b-ISO 20685-2] ISO 20685-2:2015 *Ergonomics – 3-D scanning methodologies for internationally compatible anthropometric databases – Part 2: Evaluation protocol of surface shape and repeatability of relative landmark positions*.

[b-WHO Falls] WHO, Falls fact sheet, WHO fact sheet 16 January 2018, https://www.who.int/news-room/fact-sheets/detail/falls

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, 2023