International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2074

(01/2015)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

Requirements for Internet of things devices and operation of Internet of things applications during disaster

Recommendation ITU-T Y.2074

ITU International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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

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

Recommendation ITU-T Y.2074

Requirements for Internet of things devices and operation of Internet of things applications during disaster

Summary

Recommendation ITU-T Y.2074 provides requirements for Internet of things (IoT) devices used for operation of IoT applications in the context of disaster in addition to the common requirements of IoT in ITU-T Y.2066. It also provides requirements for the operation of IoT applications during disaster.

It is necessary to specify these requirements in order to use IoT devices and IoT applications during disaster for evacuation and rescue processes.

Appendix I describes methods concerning the assurance of integrity and reliability of data produced by IoT devices during disaster.

This Recommendation is relevant for IoT application developers and IoT service providers as well as emergency service providers.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2074	2015-01-13	13	11.1002/1000/12421

Keywords

Disaster, Internet of things (IoT), IoT application, IoT device, requirements, safety systems.

* 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

Introduction

Every new information and communication technology (ICT) aims to be helpful and useful for users. This means that, even during disaster, ICT should aim to provide support for the rescue of users in dangerous situations. In fact, users sometimes have no time to wait for a rescue team or external help. In these cases, the only way is for users to act by themselves and try to leave the disaster area as soon as possible. It is necessary therefore to develop requirements for Internet of things (IoT) devices, as well as requirements for operation of IoT applications during disaster despite the normal operation of these applications. In fact, IoT applications usually become practically useless during a disaster when the imperative aim of IoT users is to be saved. Since the IoT infrastructure is already widely deployed, its technical resources could be very useful in saving human lives.

From a practical point of view, it is extremely difficult to develop and successfully implement a new emergency safety system, due to the complex standardization and certification procedures required for disaster management. However, it is rather easy to enhance the functionalities of existing safety systems with enhanced capabilities for support of IoT applications during disaster. Also, IoT based services could be combined with existing safety systems and be used by the safety systems during disaster.

It is important to understand that new IoT intelligence systems will never replace the existing tested and certified safety systems proven over many years; however, new IoT intelligence systems may support the capability of interaction with existing safety systems. It would still be technically possible to manage IoT applications from the administration centre of the existing safety systems during disaster.

It is expected that the interaction of these enhanced IoT applications with existing safety systems will be useful for rescue procedures during disaster, such as alerting and evacuation.

Recommendation ITU-T Y.2074

Requirements for Internet of things devices and operation of Internet of things applications during disaster

1 Scope

This Recommendation provides requirements for IoT devices that can be used for operation of IoT applications in the context of disaster, in addition to the common requirements of IoT [ITU-T Y.2066]. It also provides special requirements for the operation of IoT applications during disaster.

The scope of this Recommendation includes requirements for:

- IoT devices in the context of disaster;
- operation of IoT applications during disaster (for each of the three identified operating strategies).

Appendix I describes methods concerning assurance of integrity and reliability of the data produced by IoT devices during disaster.

This Recommendation is relevant for IoT application developers and IoT service providers as well as emergency service providers.

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 X.1303] Recommendation ITU-T X.1303 (2007), *Common alerting protocol (CAP 1.1)*.

[ITU-T Y.1271] Recommendation ITU-T Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks*.

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

[ITU-T Y.2205] Recommendation ITU-T Y.2205 (2011), *Next Generation Networks – Emergency telecommunications – Technical considerations*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 alert [b-ITU-T X.674]: A warning or alarm message concerning an impending danger or problem.

3.1.2 device [b-ITU-T Y.2060]: With regard to the Internet of things, 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 emergency telecommunications (ET) [ITU-T Y.2205]: Any emergency-related service that requires special handling from the next generation network (NGN) relative to other services. This includes government authorized emergency services and public safety services.

3.1.4 Internet of things (IoT) [b-ITU-T Y.2060]: 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.

3.1.5 next generation network (NGN) [b-ITU-T Y.2001]: A packet-based network which is able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.2 Terms defined in this Recommendation

This Recommendation defines or uses the following terms:

None.

4 Abbreviations and acronyms

This Recommendation defines or uses the following terms:

CAP Common Alerting Protocol

ET Emergency Telecommunications

ICT Information and Communication technology

IoT Internet of Things

NGN Next Generation Network

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.

The keyword "disaster" indicates any kind of critical situation or emergency with natural or man-made origins.

The keywords "IoT device" indicate a device in IoT environment.

6 Requirements for IoT devices in the context of disaster

6.1 General requirements concerning disaster

The following Recommendations deal with telecommunications concerning disaster:

– [ITU-T Y.1271] provides network requirements and capabilities for emergency telecommunications (ET).

– [ITU-T Y.2205] specifies technical considerations that can optionally be applied within the next generation network (NGN) to enable ET. In addition, this Recommendation also outlines the underlying technical principles involved in supporting ET.

These Recommendations deal with requirements and technical aspects for emergency telecommunications. Assuming that the IoT applications will use the NGN during a disaster as a telecommunication infrastructure, these requirements are fully applicable to them.

According to [ITU-T Y.2205], it is recommended to use the common alerting protocol (CAP) defined in [ITU-T X.1303] in order to provide information interaction between alerting systems.

6.2 Requirements for IoT devices

All manufactured IoT devices are required to pass testing procedures.

These procedures should include testing of IoT devices under conditions beyond the operating range (e.g., temperature, pressure, radiation) in order to verify their safety for the environment and for humans during disaster. IoT devices must not cause complications or occurrences of emergencies of other types.

Test conditions should be selected based on the characteristics of possible emergencies in the area of deployment.

The test results and potential hazards caused by devices outside the operating range are required to be introduced in the technical characteristics of the devices.

New IoT devices are recommended to be developed with an extended range of operating characteristics (e.g., operating temperature, humidity, pressure). The requirement for IoT devices to extend the range of operating characteristics is essential for IoT applications which could potentially fail, due to the uncertainty of the environment behaviour and its impact on the IoT devices during disaster.

Dissemination of this practice is recommended on widely used IoT device types. The operation of IoT devices providing measurements during disaster might provide a database of environmental parameter measurements during disasters of different natures. Such measurements would help to make important conclusions about the stages of disaster occurrence and allow for taking them into account in the IoT device design phase.

7 Requirements for operation of IoT applications during disaster

This clause describes requirements for IoT applications concerning their operation during disaster. In particular, clauses 7.1 to 7.3 describe requirements for each of the three identified operating strategies for IoT applications related to disaster, and clause 7.4 describes switching between two or more operation strategies during disaster.

To improve the efficiency of the infrastructure resources associated with the operation of IoT applications, it is recommended that IoT applications implement one or more of the following operation strategies related to disaster.

All strategies assume that the IoT applications do not continue normal operation during a disaster, but instead perform only tasks aimed at rescuing people.

False emergency alerts are possible: a state of emergency may be cancelled (for example, in case of false emergency detection) and, in this case, the IoT application switches back to its normal operation. The time period required to decide on a false alert (continuation of current operation or switch back to normal operation) has a different duration for each particular implementation, depending on its complexity.

7.1 IoT applications with dedicated operation mode

If an IoT application has a dedicated operation mode, which can be activated in case of emergencies, it can be used without any further action or external control. Figure 1 shows the operation mode change of IoT applications following this strategy.

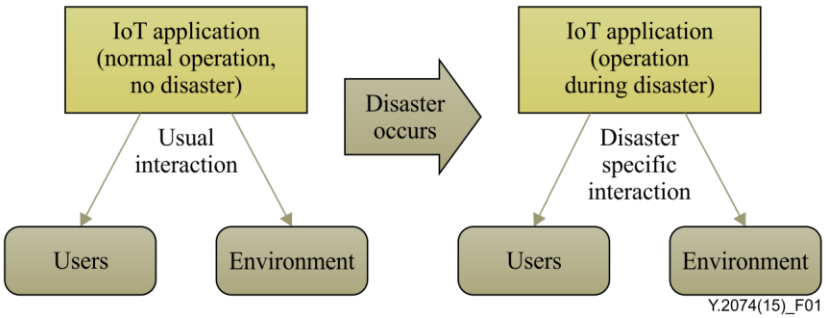

Figure 1 – Operation mode change for IoT applications with dedicated operation mode activated during disaster

Sensor network based applications designed for positioning users in a building and having dedicated operation modes activated during disaster can be extremely effective for self-evacuation from the building in case of fires, earthquakes or other disasters.

Another example of this operational strategy is that one of the IoT applications can act as a safety system.

NOTE – There are prototypes of such safety systems based on wireless sensor technologies (e.g., as described in [b-ITU-T Y.2222]), but they are not widely used because of long and complex standardization and certification procedures for the safety system equipment.

IoT applications with dedicated operation mode activated during disaster are required to comply with all appropriate regulatory rules.

7.2 IoT applications temporally providing resources to external safety systems

Normally, IoT applications have specific purposes and, for the most part, are not intended to assist or help users during disaster. Consequently, the resources of IoT applications should be assisted by external safety systems in order to improve the efficiency of the disaster management process. Figure 2 shows the operation mode change of IoT applications following this strategy.

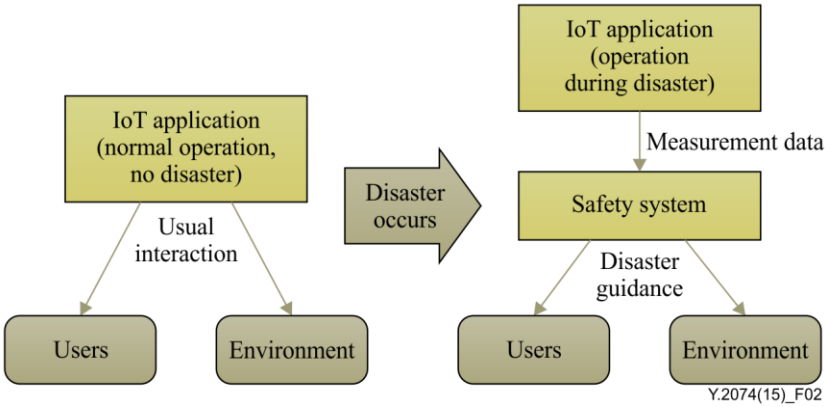

Figure 2 – Operation mode change for IoT applications temporally providing resources to external safety systems during disaster

IoT applications designed for users within a building or other environment equipped with a safety system should temporally (during disaster) share both the IoT application control capability and all kinds of measurement data with the safety system. These resources might be useful for the safety system operation, for example, data from the various sensors such as temperature and humidity in case of fire.

To simplify the integration of IoT applications with external safety systems, it is recommended to use CAP [ITU-T X.1303] for the interaction between IoT applications and external safety systems. CAP is a two-way communication protocol that can enable both the transmission of data from IoT applications to safety systems and the transmission of alert messages from safety systems to IoT applications.

The main disadvantage of this operation strategy is the possibility of failures of functional components of the IoT infrastructure if these are not designed to operate correctly during disaster. Such failures, in the case of functional components that are needed during disaster management processes, may cause negative consequences. These failures are possible due to the fact that there are no special certification procedures for the functional components of the IoT infrastructure to ensure correct operation during disaster, in contrast to the certified procedures of safety systems.

7.3 IoT applications with external control of operation during disaster

The third operation strategy for IoT applications during disaster involves a complete transfer of control capabilities and measurement data from IoT applications to external safety systems or external control centres.

NOTE 1 – The complete transfer of control capabilities implies the termination of the resource management process by the IoT application itself.

NOTE 2 –An external control centre may be, for example, an organization or a functional unit of an organization that carries the full legal and administrative responsibility for correct disaster management in a given area.

Figure 3 shows the operation mode change of IoT applications following this operation strategy.

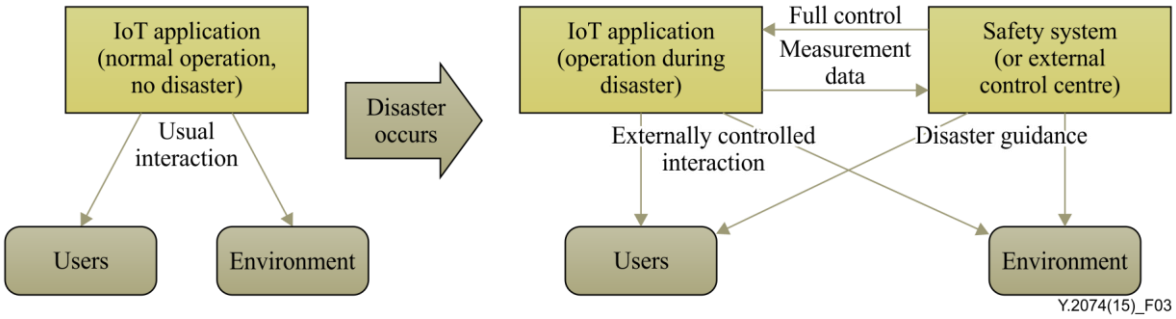

Figure 3 – Operation mode change for IoT applications with external control of operation during disaster

In this operation strategy, with respect to IoT applications following the operation mode described in clause 7.1, the users' behaviour during disaster is fully controlled by external safety systems and alerts.

The main purpose of this operation strategy is to ensure that the most effective use of all available resources of IoT applications, via proper resource management, is performed by safety systems or external control centres.

Appendix I describes methods concerning assurance of integrity and reliability of the data produced by IoT devices. A monitoring and control centre for IoT devices, as described in Appendix I, may serve as an external control centre for IoT applications for this operation strategy.

Similarly to the operation strategy described in clause 7.2, it is recommended to use CAP [ITU-T X.1303] for the interaction between IoT applications and external safety systems or external control centres in this operation strategy.

7.4 Switching between two or more operation strategies during disaster

Depending on the purpose of the IoT application and its capabilities, a combination of one or more operation strategies can be implemented in the IoT application. This involves the IoT application capability to switch between operation strategies in case of the appearance of certain external conditions, such as reception of control signals, excess of a prescribed degree in sensor readings, etc.

As an example, the operation of the IoT application can be realized as follows:

Consider an IoT application (within a geographical area) equipped with a safety system (external with respect to the IoT application). If the monitoring of the IoT device data shows an emergency occurring during normal operation, the IoT application automatically switches to dedicated operation mode for operation during disaster and implements the strategy described in clause 7.1.

At the end of the false alert decision time, the IoT application continues operation in dedicated operation mode or switches back to normal operation mode (in case of a false alert). If operation in dedicated operation mode continues, before the catastrophic phase of disaster, the IoT application generates customized information for each person, involved in the disaster, to manage his or her rescue.

Upon the occurrence of the catastrophic phase, when the IoT application is unable to manage rescues because of reduced capabilities, the IoT application switches to the operation strategy described in clause 7.2 (monitoring and transmission of gathered data to the external safety system). This may help save lives during the subsequent emergency rescue phase and will monitor the development of the disaster.

Appendix I

Methods concerning assurance of integrity and reliability of the data produced by IoT devices during disaster

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

Ubiquitous IoT devices may play a significant role in people's everyday life, influencing their decisions and actions. Hence, people may depend on their IoT devices, in particular on their information and sensor readings, as well as on the derived actions that impact the environment. Therefore, the integrity and reliability of data produced by IoT devices are very significant issues for the IoT in general.

The problem with the integrity and reliability of data produced by IoT devices becomes especially relevant during both natural and man-made disasters, where the integrity of the IoT devices themselves may not be guaranteed.

To preserve the integrity and reliability of data produced by IoT devices, it is necessary to establish a trusted environment for the IoT devices' operation. For this purpose, it is important to determine the scope of liability for the IoT devices' behaviour in general, e.g., for any incorrect sensor readings. There are two methods to achieve this goal:

1. the manufacturer of IoT devices is fully responsible for any malfunction of the produced IoT device and guarantees appropriate IoT device behaviour;
2. an independent authorized centre is fully responsible for any malfunction of an IoT device under its control (under its jurisdiction), and guarantees appropriate IoT device behaviour.

The first method is less effective than the second due to the complicated interaction between users and the manufacturers responsible for the user's IoT devices, because of the possible variety of IoT devices from different manufacturers used within the same deployment area. This problem becomes especially relevant during disaster, when the integrity and reliability of the data produced by IoT devices becomes a matter of protecting human lives. During disaster, neither users nor rescue services, or IoT devices will be able to make contact with the manufacturer of each particular IoT device to confirm the integrity and reliability of its data.

The second method is much more concrete in that it consists of the establishment of monitoring and control centres for IoT devices. These centres will be responsible for the correct operation of the IoT devices under their jurisdiction.

I.1 General overview of a monitoring and control centre for IoT devices

A monitoring and control centre (the Centre) for IoT devices is an organization, or functional unit of an organization, which carries full legal and administrative responsibility for the correct operation of the IoT devices under its jurisdiction. It also monitors the IoT devices and stores information about operations during disaster. The main goal of a monitoring and control centre for IoT devices is to check the integrity and reliability of information provided by the IoT devices under its jurisdiction. In addition, the Centre is responsible for prompt notification to users and/or owners of the IoT devices if malfunctions of any IoT device are identified.

In case of threat of disaster or during disaster, the Centre is responsible for:

- monitoring the status of the IoT devices under its jurisdiction and their output data (e.g., sensors' readings);
- identifying improperly operating IoT devices and promptly notifying users and/or owners about the malfunctions;

- determining the disaster area and the nature and parameters of the disaster, taking into account the information obtained from the IoT devices under its jurisdiction and external sources of information (e.g., emergency agencies);
- managing the IoT devices under its jurisdiction in order to safely evacuate people from the disaster area;
- recording and storing information obtained during disaster and the history of operations during disaster.

I.2 The distribution of the monitoring and control centre's responsibilities to local centres

Ubiquitous IoT devices are present in large quantities in apartments, houses, organizations, streets, public places, etc.

In the case of a monitoring and control centre for IoT devices, it is possible for all IoT devices in a given house or building to be under the jurisdiction of one local centre. Similarly, all IoT devices in other areas, for example, on the same street, could be managed by other local centres. All these local centres could be integrated into the infrastructure of the root Centre.

The infrastructure of the root Centre can be organized as a multi-level hierarchy containing monitoring and control nodes of several levels responsible for IoT devices in different: buildings (local centres), cities (municipal centres), regional (regional centres) and countries (federal centres).

Additionally, the responsibility of local centres may be distributed on an IoT device purpose basis. For example, the Centre may manage several local centres, one being responsible for IoT devices for household purposes, another for IoT devices for traffic management purposes, a third one for IoT devices for security system purposes, etc.

The following clauses describe possible working scenarios of the monitoring and control centre.

I.3 The monitoring and control centre's working scenarios

The main goal of the Centre is to check the integrity and reliability of the information provided by the IoT devices under its jurisdiction. This goal can be achieved in the following ways:

1. comparing the sensors' readings of the IoT devices under the Centre's jurisdiction, with the readings of autonomous (duplicated) sensor networks;
2. intelligent monitoring of the sensors' readings, under the Centre's jurisdiction, consisting of data collection and mathematical analysis (data mining) of the obtained information, thus allowing the identification of IoT device malfunctions.

Both methods may be implemented and used in combination in the appropriate proportion.

The above methods are described in more detail in clauses I.3.1 and I.3.2.

I.3.1 Autonomous sensor network

The Centre deploys autonomous sensor networks containing sensors of various physical parameters, which duplicate the sensors of the IoT devices under the Centre's jurisdiction.

The autonomous sensor network is required to cover the entire area under the Centre's jurisdiction. For instance, a local indoor centre should deploy a sensor network which covers the indoor area that contains IoT devices under the Centre's control.

The sensors of this autonomous sensor network are considered reference sensors, i.e., their readings are taken as reference values of physical parameters in this area. It is expected that the reference sensors are certified by a trusted and properly certified organization.

The Centre collects data from the IoT devices under its jurisdiction, and compares them with the reference values. On this comparison basis, the Centre makes decisions about integrity and reliability of the data produced by the IoT devices.

The advantage of this method is the potentially high-reliability of reference sensors, independent from the IoT devices. Hence, the malfunctions of IoT devices are identified with high accuracy.

The disadvantages of this method are the cost and complexity of deploying autonomous sensor networks and the possible failures of the reference sensors during disaster.

I.3.2 Intelligent monitoring

Intelligent monitoring concerns the collection of device information and sensor readings obtained from the IoT devices under the Centre's jurisdiction, and the mathematical analysis of this information. This includes, but is not limited to, the methods of statistical analysis and correlation signal processing.

Intelligent monitoring allows the identification of out of order IoT devices or their sensors within a group of similar devices.

The advantage of this method is complete independence from external parameters of the environment, allowing operation in every situation during disaster.

The disadvantage of this method is the need to have a group of similar IoT devices for more reliable determination of malfunctions.

I.4 Use of the stored data

The Centre implements monitoring, recording and storing of device information and sensor readings obtained from the IoT devices under its jurisdiction, including those obtained immediately before and during disaster.

This functionality allows the Centre to operate as a "black box" in emergencies. The Centre is assumed to help identify the causes of emergencies, in a similar way to what is done by the black box in aircraft.

Historical data collected in the Centre's data store may be used to improve the methods of intelligent monitoring and to develop IoT device management and control methods under the threat of disaster or during disaster in order to achieve the greatest possible evacuation of people, safely from the disaster area.

Bibliography

[b-ITU-T X.674] Recommendation ITU-T X.674 (2011), *Procedures for the registration of arcs under the Alerting object identifier arc*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

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

[b-ITU-T Y.2222] Recommendation ITU-T Y.2222 (2013), *Sensor control networks and related applications in a next generation network environment*.

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	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, 2015