

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



International
Telecommunication
Union
Documents

Document Sharing Hub

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/>.

© ITU 2015

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	2
6	Requirements for IoT devices in the context of disaster	3
	6.1 General requirements concerning disaster.....	3
	6.2 Requirements for IoT devices	3
7	Requirements for operation of IoT applications during disaster	3
	7.1 IoT applications with dedicated operation mode.....	4
	7.2 IoT applications temporally providing resources to external safety systems	4
	7.3 IoT applications with external control of operation during disaster.....	5
	7.4 Switching between two or more operation strategies during disaster	6
	Appendix I – Methods concerning assurance of integrity and reliability of the data produced by IoT devices during disaster	8
	I.1 General overview of a monitoring and control centre for IoT devices	8
	I.2 The distribution of the monitoring and control centre's responsibilities to local centres	9
	I.3 The monitoring and control centre's working scenarios.....	9
	I.4 Use of the stored data	10
	Bibliography.....	11

Document Sharing Hub

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.

ITU-T Y.2074 (01/2015)