ETSI TR 103 582 V1.1.1 (2019-07)

EMTEL;
Study of use cases and communications involving IoT devices in provision of emergency situations

Reference
DTR/EMTEL-00041

Keywords
emergency, emergency services, IoT, public safety, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Special Committee Emergency Communications (EMTEL).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Since the Internet has matured, society has become more interconnected, as have the devices used to enhance everyday lives. This has led to the emergence of the so-called "Internet of Things" (IoT), in which autonomous devices as well as people act as connected endpoints in a massive network of networks.

The purpose of the present document is to consider communications involving IoT devices in all types of emergency situations, such as emergency calling, mission critical communications, Public Warning System communications and a new domain identified as automated emergency response, and to prepare the potential standardization requirements enabling a safe operation of these communications.

The reader will find in clause 4 a general overview of the topic.

Clause 5 provides a comprehensive state of the art at the date of the present document, covering IoT in emergency communications, as well as emergency handling in IoT communications. It analyses existing standards, communications networks, previous studies and solutions being already deployed.

A set of eight exemplary use cases, presenting different types of communications and applications involving IoT devices for emergency services, is presented in clause 6. The use cases are analysed from the point of view of potential failures putting safety at risk. Potential means to prevent these points of failure are also identified.

Finally, the impact of these use cases on existing or future standards is assessed. A set of potential requirements is proposed in clause 7, for each emergency domain under study, leading to recommendations for the different standardization groups targeted by this study, including SC EMTEL, IoT service platform specification groups and network specification groups.

1 Scope

The present document considers communications involving IoT devices in all types of emergency situations. This includes the use of IoT devices to enhance:

- Emergency calling, e.g. between individuals and emergency authorities/organizations, between emergency authorities/organizations, and between individuals.
- Mission critical communications within emergency services/public safety organizations, e.g. between public safety officers and control centres, between the control centres of different public safety organizations, and between individual public safety officers.
- Public Warning System type communications from authorities to the general public.
- Automated emergency response (new IoT domain) between two IoT devices.

The current state of the art for IoT device communications, especially when relevant to emergency situations, is described and use cases illustrate how such communications can be used to provide additional/enhanced information for communicating parties involved in emergency situations.

The impact of the use cases on the existing emergency, public warning, and mission critical communications is then considered, and recommendations for requirements to existing specifications for each domain are provided.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 181: "Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies".

[i.2] ETSI TS 102 182: "Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies".

[i.3] ETSI TR 102 410: "Emergency Communications (EMTEL); Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress".

[i.4] ETSI TR 103 338: "Satellite Earth Stations and Systems (SES); Satellite Emergency Communications (SatEC); Multiple Alert Message Encapsulation over Satellite (MAMES) deployment guidelines".

[i.5] ETSI TS 103 337: "Satellite Earth Stations and Systems (SES); Satellite Emergency Communications; Multiple Alert Message Encapsulation over Satellite (MAMES)".

[i.6] ETSI TR 118 501: "oneM2M; Use Case collection (oneM2M TR-0001)".

[i.7] ETSI TR 103 375: "SmartM2M; IoT Standards landscape and future evolutions".

[i.8] ETSI TS 122 261: "5G; Service requirements for next generation new services and markets (3GPP TS 22.261)".

[i.9] EENA Technical Committee Document: "Public Safety Digital Transformation, The Internet of Things (IoT) and Emergency Services, March 2016.

[i.10] GSMA Whitepaper, February 2017: "Network 2020: Mission Critical Communications".

[i.11] 91/396/EEC: Council Decision of 29 July 1991 on the introduction of a single European emergency call number.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31991D0396.

[i.12] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L1972&from=EN.

[i.13] ETSI TS 122 268: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Public Warning System (PWS) requirements (3GPP TS 22.268)".

[i.14] 3GPP TR 36.888: "Study on the provision of low-cost MTC User Equipment based on LTE".

[i.15] 3GPP TS 26.850: "MBMS for IoT".

[i.16] 3GPP Study Item for FS-MBMS-IoT.

NOTE: Available at SP-170592: http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_76/Docs/SP-170592.zip.

[i.17] ETSI TS 122 011: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Service accessibility (3GPP TS 22.011)".

[i.18] ETSI TS 122 261: "5G; Service requirements for next generation new services and markets (3GPP TS 22.261)".

[i.19] ETSI SR 002 180: "Emergency communications; Requirements for communication of citizens with authorities/organizations in case of distress (emergency call handling)".

[i.20] Keysight white paper - 5992-2943EN: "Key Technologies Needed to Advance Mission-Critical IoT", May 7, 2018.

NOTE: Available at http://literature.cdn.keysight.com/litweb/pdf/5992-2943EN.pdf.

[i.21] IETF RFC 3261: "Session Initiation Protocol".

[i.22] IETF RFC 6881: "Best Current Practice for Communications Services in Support of Emergency Calling (BCP 181)".

[i.23] IETF RFC 6443: "Framework for Emergency Calling Using Internet Multimedia".

[i.24] IETF RFC 4190: "Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony".

[i.25] IETF draft-ietf-ecrit-data-only-ea-17: "Data-Only Emergency Calls".

[i.26] GSMA Mobile IoT Rollout Report.

NOTE: Available at https://www.gsma.com/iot/miot-rollout/.

[i.27] ITU-T Terms of Reference - Internet of Things Global Standards Initiative (IoT-GSI).

[i.28] CENELEC EN 55011:2017: "Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement".

[i.29] Recommendation ITU-T Y.2060/Y.4000: "Overview of the Internet of things".

[i.30] Recommendation ITU-T Y.2061/Y.4001: "Requirements for the support of machine-oriented communication applications in the next generation network environment".

[i.31] ETSI TR 118 501: "oneM2M; Use Case collection (oneM2M TR-0001)".

[i.32] ETSI TR 118 526: "oneM2M: Vehicular Domain Enablement (oneM2M TR-0026)".

[i.33] oneM2M-REQ-2013-0264R05: Traffic Accident Information Collection Use Case.

[i.34] oneM2M-REQ-2012-0074R09: Information Delivery Service in The Devastated Area Use Case.

[i.35] ETSI TR 103 376: "SmartM2M; IoT LSP use cases and standards gaps".

[i.36] AIOTI WG03: "IoT LSP Standard Framework Concepts", Release 2.0, October 2015.

[i.37] Going beyond the technical analysis (Part 1), IoT Platforms, STF505, Samir Medjiah.

NOTE: Available at http://ec.europa.eu/information_society/newsroom/image/document/2017-7/stf_505_-_4-iot_platforms_C8B323CB-D37C-DB62-1A6210643559CBB5_42842.pdf.

[i.38] IETF draft-zuniga-lpwan-sigfox-system-description-04: "SIGFOX System Description".

[i.39] IETFdraft-farrell-lpwan-lora-overview-01: "LoRaWAN Overview".

[i.40] Luca Simone Ronga, Sara Jayousi, Renato Pucci, Simone Morosi, Matteo Berioli, Josef Rammer, Alessio Fanfani, and Stefano Antonetti: Multiple Alert Message Encapsulation Protocol: Standardization and Experimental Activities, Proceedings of the ISCRAM 2015 Conference - Kristiansand, May 24-27, Palen, Büscher, Comes & Hughes, eds.

[i.41] ETSI TR 102 022-1 (V1.1.1) (2012-08): "User Requirement Specification; Mission Critical Broadband Communication Requirements".

[i.42] ETSI TR 102 022-2 (V1.1.1) (2015-01): "User Requirements Specification; Mission Critical Broadband Communications Part 2: Critical Communications Application".

[i.43] Recommendation ITU-T X.1303: "Common alerting protocol (CAP 1.1)".

[i.44] IETF Journal: "Internet of Things: Standards and Guidance from the IETF", April 17, 2016.

[i.45] ETSI TS 103 260-1 (V1.1.1) (2015-05): "Satellite Earth Stations and Systems (SES); Reference scenario for the deployment of emergency communications; Part 1: Earthquake".

[i.46] ETSI TS 103 260-2 (V1.1.1) (2015-05): "Satellite Earth Stations and Systems (SES); Reference scenario for the deployment of emergency communications; Part 2: Mass casualty incident in public transportation".

[i.47] "The future of Public Safety", Ulrich Ruefuess, ETSI PPDR workshop, September 2016.

[i.48] New opportunities for broadband PPDR: "How will police officers work in this new era of critical communications?", Jeppe Jepsen, ETSI PPDR workshop, September 2016.

[i.49] Raimundo Rodulfo: "Connected through a disaster", IEEE standards University E-Magazine, vol 9, no. 2, July 2018.

[i.50] Yatin Trivedi: "Disaster recovery - Can we be prepared by simulation?", IEEE standards University E-Magazine, vol 9, no. 2, July 2018.

[i.51] ETSI TR 102 641: "Satellite Earth Stations and Systems (SES); Overview of present satellite emergency communications resources".

[i.52] ETSI TR 103 166: "Satellite Earth Stations and Systems (SES); Satellite Emergency Communications (SatEC); Emergency Communication Cell over Satellite (ECCS)".

[i.53] IETF RFC 7668: "IPv6 over BLUETOOTH(R) Low Energy".

[i.54] IETF RFC 7428: "Transmission of IPv6 Packets over ITU-T G.9959 Networks".

[i.55] IETF RFC 6550: "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks".

[i.56] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[i.57] IETF RFC 7390: "Group Communication for the Constrained Application Protocol (CoAP)".

[i.58] IETF RFC 7641: "Observing Resources in the Constrained Application Protocol (CoAP)".

[i.59] IETF RFC 6690: "Constrained RESTful Environments (CoRE) Link Format".

[i.60] IETF RFC 7049: "Concise Binary Object Representation (CBOR)".

[i.61] IETF RFC 7744: "Multicast Protocol for Low-Power and Lossy Networks (MPL) Parameter Configuration Option for DHCPv6".

[i.62] IETF RFC 8392: "CBOR Web Token (CWT)".

[i.63] IETF RFC 7554: "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement".

[i.64] IETF RFC 8180: "Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration".

[i.65] IETF RFC 7228: "Terminology for Constrained-Node Networks".

[i.66] IETF RFC 7815: "Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation".

[i.67] IETF RFC 8352: "Energy-Efficient Features of Internet of Things Protocols".

[i.68] IETF RFC 8387 "Practical Considerations and Implementation Experiences in Securing Smart Object Networks".

[i.69] Recommendation ITU-T Y.2074: "Requirements for Internet of things devices and operation of Internet of things applications during disaster".

[i.70] Recommendation ITU-T Y.4116: "Requirements of transportation safety services including use cases and services scenarios".

[i.71] Recommendation ITU-T Y.4119: "Requirements and capability framework for IoT-based automotive emergency response system".

[i.72] Recommendation ITU-T Y.4806: "Security capabilities supporting safety of the Internet of things".

[i.73] Recommendation ITU-T Y.4457: "Architectural framework for transportation safety services".

[i.74] ETSI TS 123 041: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041)".

[i.75] ETSI TS 126 281: "LTE; Mission Critical Video (MCVideo); Codecs and media handling (3GPP TS 26.281)".

[i.76] ETSI TS 123 282: "LTE; Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2 (3GPP TS 23.282)".

[i.77] ETSI TR 103 393: "Emergency Communications (EMTEL); Advanced Mobile Location for emergency calls".

[i.78] EENA Operations Document, "RPAS and the Emergency Services", November 2015.

[i.79] EENA Next Generation 112 Document "Long Term Definition", April 2012.

[i.80] ETSI TR 103 140: "Mobile Standards Group (MSG); eCall for VoIP".

[i.81] eCall in all new cars from April 2018.

NOTE: Available at https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018.

[i.82] CEN TS 17184: "Intelligent transport systems. eSafety. eCall High level application Protocols (HLAP) using IMS packet switched networks".

[i.83] CEN TS 17240: "Intelligent transport systems - ESafety - ECall end to end conformance testing for IMS packet switched based systems".

[i.84] Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC.

[i.85] ETSI TS 103 479: "Emergency Communications (EMTEL); Core elements for network independent access to emergency services".

[i.86] IETF- charter-ietf-atoca-01: "Authority-to-Citizen Alert".

NOTE: Available at https://datatracker.ietf.org/doc/charter-ietf-atoca/.

[i.87] ETSI EN 302 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[i.88] Theilen-Willige, Barbara & Wenzel, Helmut (2012). Remote Sensing and GIS Contribution to the Inventory of Areas and Infrastructure susceptible to Tsunami Hazards - demonstrated by Case Studies in Chile and Japan.

[i.89] M. Wetterwald et al: "Integrating Future Communication Technologies for the Downstream Component of Public Warning Systems", International Journal on Advances in Networks and Services, 2012 vol 5 nr 3&4.

[i.90] ETSI TS 102 900: "Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service".

[i.91] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[i.92] Recommendation ITU-T G.9959: "Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications".

[i.93] ETSI TS 118 102: "oneM2M Requirements (oneM2M TS-0002)".

[i.94] oneM2M TR-0046: "Study on Public Warning Service Enabler".

[i.95] COM/2008/0886.

NOTE: Available at http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20080886FIN.do.

[i.96] IEEE 802.15.4™: "IEEE Standard for Low-Rate Wireless Networks".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

authority: organization within the public sector fully or partly responsible for emergency preparedness and handling of incidents

NOTE: Source ETSI TS 102 181 [i.1].

emergency response organization: organization, e.g. the police, fire service and emergency medical services, that provides immediate and rapid assistance in situations where there is a direct risk to life, individual or public health or safety, to private or public property, or the environment but not necessarily limited to these situations

NOTE: Source ETSI TS 102 182 [i.2].

citizen: any individual (resident, visitor, passer-by), present in the vicinity of an emergency situation (from the first notice till the complete clearance) and subject to be affected by it, but who has no identified role in the actions of rescue and of restoration of normal conditions

NOTE 1: Source ETSI TS 102 182 [i.2].

NOTE 2: Depending on his situation, the citizen can send alerts or provide information to the emergency services, but in many cases is either passive or a potential victim. A visitor can be either local or foreign individual, members of the armed forces are included as well.

Internet of Things (IoT): dynamic global network with (self-)configuring capabilities based on communication protocols where physical and virtual "things" have identities, physical attributes, and virtual representation, and use interfaces to be integrated into the information network

NOTE: IoT represents the next step towards digitization where all physical objects, machines, servers, other devices and people can be interconnected through communication networks, in and across private, public and industrial spaces, report about their status and/or about the status of the surrounding environment and exchange data for intelligent applications and services to be developed. The data transmitted over the IoT can be small in size and frequent in transmission. The number of devices is greater in IoT than in traditional PC computing.

IoT device: non-conventional, most often resource-limited, computing device (i.e. not a computer, server, tablet, or smartphone but comprising e.g. a micro-controller-based embedded system) which is connected to a communication network and which includes one or multiple sensors and actuators to interact with its deployment environment

NOTE: In most cases, an IoT device is a physical, previously unconnected, object that has been embedded with new IoT technology (i.e. communication, processing, and/or storage capabilities) to turn it into a smart device.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	Third Generation Partnership Project
5G	5th Generation (of mobile networks)
AAA	Authentication, Authorization and Accounting
ACE	Authentication and Authorization for Constrained Environments
AE	Automated Emergency
AED	Automatic External Defibrillator

AERS	Automotive Emergency Response System
AI	Artificial Intelligence
AIOTI	Alliance for IoT Innovation
AML	Advanced Mobile Location
ANT	Protocol of ANT+ consortium
API	application program interface
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
ATOCA	Authority-to-Citizen Alert
BBF	Broadband Forum
BCP	Best Current Practice
BLE	Bluetooth Low Energy
BR	Basic Rate
BR/EDR	Basic Rate/Enhanced Data Rate
CAP	Common Alerting Protocol
CBOR	Concise Binary Object Representation
CBRN	Chemical, Biological, Radiological And Nuclear
CBS	Cell Broadcast Service
CCA	Critical Communications Application
CCP	Casualty Collection Point
CEPT	European Conference of Postal and Telecommunications
CFECC	Coordinating Field Emergency Control Centre
CMAS	Commercial Mobile Alert System
CoAP	Constrained Application Protocol
COP	Common Operating Picture
CoRE	Constrained RESTful Environments
COSE	CBOR Object Signing and Encryption
D2D	Device to Device
DAB	Digital Audio Broadcasting
DENM	Decentralized Environment Notification Message
DTLS	Datagram Transport Layer Security
DVB	Digital Video Broadcasting
ECC	emergency control centre
ECCS	emergency communication cell over satellite
EC-GSM-IoT	Extended Coverage GSM Internet of Things
ECRIT	Emergency Context Resolution with Internet Technologies
EDR	Enhanced Data Rate
EENA	European Emergency Numbering Association
eMBMS	enhanced MBMS
EMC	electromagnetic compatibility
EMI	Electromagnetic interference
eMTC	enhanced MTC
EMTEL	Emergency Communications
ePWS	enhanced PWS
ESInet	Emergency Services IP network
ETS	Emergency Telecommunication Service
ETWS	Earthquake and Tsunami Warning System
EWF	Emergency Warning Functionality
FCC	Federal Communications Commission
FECC	Field Emergency Control Centre
GDPR	General Data Protection Regulation
GMLC	Gateway Mobile Location Centre
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Services
GSI	Global Standards Initiative
GSM	Global System for Mobile telephony
GSMA	GSM Association
HEMS	Helicopter Emergency Medical Service
HTTP	Hypertext Transfer Protocol
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers

IET	Institute of Engineering and Technology
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IoT	Internet of Things
IP	Internet Protocol
IPSO	IP Smart Objects
IPTV	Internet Protocol Television
IR	Infra-Red
ISM	Industrial, Scientific and Medical
ISO	International Standards Organization
ITS	Intelligent Transport System
ITU	International Telecommunications Union
JOSE	JavaScript Object Signing and Encryption
JSON	JavaScript Object Notation
KA	Knowledge Area
KPN	Koninklijke PTT Nederland
LPWA	Low Power Wide Area
LPWA	Low Power Wide Area
LSP	Large Scale Pilot
LTE	Long Term Evolution
LTE-M	LTE for Machine-Type Communications
M2M	Machine-to-Machine
MAC	Media Access Control
MAMES	Multiple Alert Message Encapsulation over Satellite
Mbit/s	Mega bit per second
MBMS	Multimedia Broadcast and Multicast Service
MC	Mission Critical
MCI	Mass Casualty Incident
MCPTT	Mission Critical Push to Talk
MNO	Mobile Network Operator
MTC	Machine-Type Communications
MTOW	Maximum Take-Off Weight
NB-IoT	Narrowband Internet of Things
NFC	Near Filed Communication
NG112	Next Generation 112
NGN	Next Generation Network
NIST	National Institute of Standards and Technology
NTT	NTT DoCoMo mobile operator
NWK	Network (Layer)
OCF	Open Connectivity Foundation
OMA DM	OMA Device Management
OMA LWM2M	OMA Lightweight M2M
OMA	Open Mobile Alliance
OSI	Open Systems Interconnection
P25	Project25
PAMR	Public Access Mobile Radio
PAN	Personal Area Network
PC	Personal Computer
PCP-TDR	Partnership Coordination Panel - Telecommunication for Disaster Relief and Mitigation
PDF	Portable Document Format
PHY	Physical Layer
PII	Personally Identifiable Information
PMR	private mobile radio
PPDR	Public Protection and Disaster Relief
ProSe	Proximity Based Services
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTT	Push To Talk
PWS	Public Warning System, also known as Public Warning Service
QoS	Quality of Service
RATCOM	Réseau d'Alerte aux Tsunamis et submersions COtières en Méditerranée
RDM	Requirements and Domain Models

REST	Representational State Transfer
RESTCONF	REST Configuration Protocol
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
ROLL	Routing Over Low-power Lossy networks
RPAS	Remotely Piloted Aircraft System
RPL	Ipv6 Routing Protocol for Low-Power and Lossy Networks
SDN	Software-defined Network
SDO	Standards Developing Organization
SDS	System Design and Security
SECC	Sector Emergency Control Centre
SIP	Session Initiation Protocol
SLAM	simultaneous localization and mapping
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCC	Temporary Care Centre
TCCE	TETRA and Critical Communications Evolution
TCP	Transmission Control Protocol
TETRA	Terrestrial Trunked Radio
TLS	Transport Layer Security
TSCH	Time-Slotted Channel Hopping
TSG	Technical Specification Group
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UE	User Equipment
ULE	Ultra Low Energy
UMTS	Universal Mobile Telecommunication System
UNB	Ultra-Narrow Band
UPNP	Universal Plug-and-Play
URL	Uniform Resource Locator
USA	Unite States of America
UTRAN	UMTS Terrestrial Radio Access Network
VLC	Visible Light Communication
VoIMS	Voice over IMS
WEA	Wireless Emergency Alerts
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

4 General Overview

Since the Internet has matured, society has become more interconnected, as have the devices used to enhance everyday lives. This has led to the emergence of the so-called "Internet of Things" (IoT), in which autonomous devices as well as people act as connected endpoints in a massive network of networks.

The large number of deployed IoT devices collectively send huge amounts of data about their status, that of the environment which they are managing or in which they are operating, and/or other object specific data. Such ‘big data' can be processed directly by those deploying the devices for their primary intended purposes or used as operational metrics to be fed back into the system to fine tune operation for greater efficiency and effectiveness. Data can also be aggregated by third parties in innovative and previously unthought of ways to identify emerging trends or even predict future behaviour.

In its paper on the IoT and emergency services [i.9], EENA has recognized the potential value of IoT device data and has considered how it might be utilized in emergency situations to the advantage of the parties involved from an emergency calling perspective. Communications arising from emergency situations are however not limited to those between individual citizens and public safety authorities. Neither is the potential benefit from using data from IoT devices limited only to the emergency calling perspective.

Table 1, identifies three emergency communications domains that could be enhanced with and benefit from additional information provided by IoT devices, and a fourth new emergency domain that is enabled by the proliferation of IoT devices.

Table 1: Emergency communications domains

Emergency communication domain	Actors	Nature of communication
Emergency calling	The general public Public Safety Answering Points Emergency services organizations	Two-way communication between individuals and authorities/organizations, between authorities/organizations, and between individuals.
Mission critical communications	Emergency services Public safety agencies/ organizations	(Multi-)point-to-(multi-)point communication between public safety personnel.
Public Warning System (PWS)	National or local authorities, the general public	One-way broadcast communication from authorities to individuals.
Automated emergency response (new emergency communication domain)	IoT devices The general public Emergency services organizations Verticals (example utilities organizations)	One-way broadcast communication from authorities to IoT devices or from IoT devices to individuals. Point-to-point communications between IoT devices. Point-to-Point communication between IoT devices and automated responding entity (example server).

5 State of the art for communications relevant to emergency situations involving IoT devices

5.1 General overview

This clause reviews the state of the art for communications involving IoT devices, especially those relevant to emergency situations.

The review considers standardization work already done, including the associated standards reference documents, and when necessary further input documents, whitepapers, etc. A description of the state of the art related to communications involving IoT devices is included, especially those relevant to emergency situations. The review also covers the connectivity capabilities, as well as other features such as interoperability, devices and sensors, security, etc. On each topic, an analysis of the existing material and specifications is provided and the main properties of communications involving IoT devices are identified.

5.2 Emergency-related standardization state of the art

5.2.1 ETSI SC EMTEL standardization

5.2.1.1 General

SC EMTEL is a Special Committee on emergency communications within ETSI. It is responsible for specifying emergency communications and covers functional and service requirements:

1) communications of citizens/individuals with authorities/organizations (emergency calling, see ETSI SR 002 180 [i.19]);

2) communications between authorities/organizations (between the authorized representatives who can be involved in the responses and actions when handling an emergency, mission critical communications see ETSI TS 102 181 [i.1]);

3) communications between individuals and between individuals and authorities whilst emergencies are in progress (emergency calling, see ETSI TR 102 410 [i.3]); and

4) communications from authorities/organizations to the individuals (PWS, see ETSI TS 102 182 [i.2]).

5.2.1.2 Summary of ETSI SC EMTEL Requirements

SC EMTEL high level principles and requirements for the domains listed in clause 5.2.1.1 can be summarized as:

1) Communications of citizens/individuals with authorities/organizations (emergency calling, see ETSI SR 002 180 [i.19]):

- the availability of the emergency numbers as 112 Europe wide and national emergency numbers to make an emergency call towards a designated PSAP;
- terminals capable of making emergency calls free of charge using different types of communication networks; and
- specific requirements considered for Design-for-All of any emergency call system or terminal where people with disabilities, older people and children will need special requirements for emergency call handling. Data protection and privacy of all users should be considered.

2) Communications between authorities/organizations (PSAPs, Emergency services organizations and authorities, Mission critical, Public Safety) (see ETSI TS 102 181 [i.1]):

- SC EMTEL considers the relationships among authorized representatives responsible for handling emergency situations as well as those between the different organizations, e.g. between PSAP and emergency control centre, among PSAPs, between emergency control centres, etc.;
- required communication services, to facilitate the exchange of information between authorized organizations, are speech (Point-To-Point, group call, Push-to-Talk), video teleconferencing, and data services (varies in capacity, time criticality and robustness). Data services need bandwidth provided by the fixed and mobile networks that provide the required throughput and minimizes end to end delay. Paging services are needed to contact emergency personnel/agent. Location services are essential for real time information to locate emergency personnel, emergency vehicle or an IoT device, for the latter especially with status monitoring (e.g. using sensors);
- interoperability of communication services allows information to be communicated rapidly, widely and effectively to all relevant parties. Scalability is also an important consideration especially when the communications system (networks in combination) handle the escalation from a case involving e.g. one ambulance and one emergency control centre up to national authorities (regional control centres, ministries, municipal authorities as well as local services);
- traffic management is essential, especially in cases where public and private networks are affected and the bulk of traffic is caused by the crises. Access restriction to emergency authorities should be handled with priority;

- emergency preference scheme solutions for fixed and mobile, public and private, communication networks are essential. A public safety/mission critical user always wants to be able to establish communications instantly and at all times. Because of limited physical resources (number of trunks, lines, radio channels, etc.) communication networks can become overloaded in emergency situations, thus solutions as pre-emption to priorities priority calls, dynamic traffic management algorithms, and many others should be considered; and

- for all emergency communication, the organizations involved have to make sure that data is protected according to its sensitivity level during transmission, processing and storage and that access to communication channels and critical systems is only granted to authorize persons. This includes confidentiality of data, protection of signalling information, authentication of persons or devices, access authorization, integrity of data, non-repudiation, logging records of communications. Security is a requirement that should support interoperability among different systems using "red-gateways", or "swivel chair interoperability"- where a single user is provided with terminals for multiple systems.

3) Communications between individuals and between individuals and authorities whilst emergencies are in progress (Emergency calling, see ETSI TR 102 410 [i.3]).

- this concentrates on means of communication between affected individuals in an emergency situation and establishes a basis of requirements for the corresponding communication functions. A state of emergency as such may have coverage of a city, a valley or a district, or it might be more concentrated to a single point (e.g. a piece of a motorway, a city block, etc.). Initially, there is a need to consider the condition of the infrastructure in the affected area and how badly they are affected. In a less severe case, the communication network in the surroundings of the accident may technically be in order, but may experience blocking and overloading due to the increased traffic. In both cases there might be an urgent need for individuals to learn about the state of relatives and friends (and property); and to coordinate mutual actions;

- individuals that can be members of non-governmental organizations (e.g. Red Cross) may provide help in the emergency area or in liaising with authorities. Others such as utility staff (gas, electricity) may also help from the control centre under their responsibility. Broadcast and media centres (TV, Radio) and their reporters can also help in spreading the information. Such support requires communication networks that have the capacity and resilience to cater for the traffic caused by the different players; and

- today, via social media, an individual can indicate being safe in an emergency situation. SC EMTEL proposes having an emergency database (database to handle large amount of information about distressed persons and items) see ETSI TR 102 410 [i.3], able to handle a large amount of information and store it in a systematic way can be used to address individuals as well as groups of people (according to their role in the situation). One example of use can be to send a concise message containing an identity to register oneself, preferable with a condition/availability status (e.g. "I am alive and fine", I am alive and taken care of", location and how to be reached, etc.) to an emergency communications database. This database could then be used for addressing purposes (contains associations between personal identity and a given terminal. A database is also capable of giving quick access to stored information to a large number of users at the same time. Setting up such a database and providing access need considerations on privacy and personal integrity.

4) Communications from authorities/organizations to the individuals (PWS, see ETSI TS 102 182 [i.2]):

- in the space of communication from authorities/organizations to citizens in all types of emergencies, so called Public Warning System (PWS), operational and organizational requirements are considered as a basis for a common notification service, including targeting of the area to be notified. Examples for the emergency situations in this case can be hurricane warning, flooding, earthquake etc. The warning information needs to be clear and comprehensive to the user. The exact information regarding the performance of the telecommunication network in the affected area needs to be known to the authority;

- an effective Emergency Notification system will be capable of disseminating information to a large number of individuals within specific affected areas. Emergency Notification systems will provide high speed messages delivery within a specified time including details of the situation, instructions to the citizens, strategic information delivery to targeted audience and locations of impacted areas. Security and data protection (user authentication, authorization, and access) and privacy associated with subscriber/citizen records potentially stored as part of the system needs to be ensured. Communicating with the population during the late evening, overnight and early morning periods when most people are sleeping needs to be addressed;

- a heterogeneous strategy for offering suitable channels through which the public can receive the emergency messages is required to ensure efficient and quick notification (e.g. voice, SMS, cell broadcast and MBMS, broadcast radio, digital audio broadcast (DAB EWF) and digital television, web notification and emails, among others), and to allow an increased level of content delivery in the notification message. The warning messages should be sent in emergency situations to the affected geographic area. The warning messages should reach citizens at their homes, work place, public venues, travelling on foot, travelling using transportation and other citizens visiting the country;

- in case of crisis, e.g. caused by dramatic weather conditions, terrorist attack or traffic accidents there is a demand for assistance and information communications services from the individuals to individuals and to authorities; and

- Common Alerting Protocol (CAP), in Recommendation ITU-T X.1303 [i.43], provides a standardized and widely accepted protocol by which emergency notification messages may be conveyed from an administration body responsible for originating an emergency notification message to organizations responsible for the dissemination of the emergency notification (e.g. TV/Radio Broadcast companies, network operators) to individuals. CAP contains information such as the nature of the alert (e.g. fire), the severity (e.g. extreme), affected area, and advice/instructions etc. Other information elements within CAP (e.g. nature, severity, advice, instruction) should be embodied in the emergency notification conveyed by whatever method is used to reach the individual.

NOTE: EMTEL EU-Alert using Cell Broadcast ETSI TS 102 900 [i.90] defines the system requirements for a European Public Warning System using the Cell Broadcast Service as a means of message distribution and delivery to the mobile user equipment.

5.2.1.3 Advanced Mobile Location for emergency calls

In addition, ETSI SC EMTEL has described Advanced Mobile Location (AML) (see ETSI TR 103 393 [i.77]), which is a positioning solution that allows use of native smart phone technology to pass (Assisted) GNSS or WLAN based location data to Emergency Service PSAPs. Such technologies can provide a location precision as good as 5 metres outdoors (and averaging to within circular areas of ~25 m radius for indoor locations). This provides a significant improvement over the cell-coverage based positioning methods of mobile networks. AML functionality is triggered in the handset by an emergency call (which is unaffected) and is designed to supplement the basic network location feed wherever possible. In order to verify the handset location, locations obtained through the AML functionality are compared to the location provided by mobile network Gateway Mobile Location Centres (GMLCs) currently based on cell coverage information, using an algorithm that analyses factors such as time of positioning and the separation of the two locations.

5.2.1.4 Conclusion

SC EMTEL requirements that are considered for emergency communications can be summarized as below. These requirements may apply for emergency communications using IoT devices as well:

- all current and future public electronic communications networks capable of carrying emergency traffic of any emergency communication domain should take into account the principles and requirements of SC EMTEL;

- a high level of interoperability between different systems and applications allows information to be communicated rapidly, widely and effectively to all relevant parties;

- different kind of communication services are required to facilitate the exchange of information. This includes speech, broadcast, SMS, emails, web-services, etc. Priority and traffic management for emergency communications is essential and providing the required characteristics for the offered service (bandwidth, throughput, delay sensitivity, speed message delivery, etc.);

- security in its wide perspective is required. This includes but is not limited to, data protection and privacy, integrity, authentication of persons and devices, logging records, etc.; and

- SC EMTEL strongly recommends to perform a risk analysis in each emergency scenario and to define the respective priorities for handling these scenarios where the emergency situations and events combine, considering their organizational and technical handling leads to a very large number of different scenarios.

5.2.2 ETSI SES/SatEC standardization

Satellite Emergency Communications (SatEC) is a working group created in September 2006 within the ETSI Technical Committee (TC) on Satellite Earth Stations and Systems (SES). Its terms of reference read "to perform standardization in the area of satellite-based emergency management including functional architectures, services for communication and the supporting protocols". SES SatEC has been dormant since 2016.

Technical Report ETSI TR 102 641 [i.51] provides an introduction to disaster management, basic requirements of telecommunication systems deployed for disaster management, typical space resources, and a brief list of initiatives in the field of emergency communications.

Technical Report ETSI TR 103 166 [i.52] outlines the concept of Emergency Communication Cells over Satellite (ECCS). ECCS are understood as temporary emergency communication cells supporting terrestrial wireless and wired standard(s), which are linked/backhauled to a permanent infrastructure by means of bi-directional satellite links.

The main objectives of the "Multiple Alert Message Encapsulation over Satellite (MAMES)" standardization activities were according to paper presented at the ISCRAM 2015 conference [i.40]:

- to define an extensible multiple alert message encapsulation protocol for alert messages transport over satellite links;
- to support encapsulation of one or more differently formatted alert messages (e.g. Common Alerting Protocol, text, binary objects, paging protocols, etc.);
- to allow integration with the main telecommunication satellite architectures (Galileo Services, DVB-suite, any IP-based satellite access etc.) and with already existing terrestrial networks;
- to define additional (optional) functions for service extension, enabling the adaption towards a large variety of situations (including network resource limitations).

MAMES results were documented as ETSI TR 103 338 [i.4] and ETSI TS 103 337 [i.5].

The main objectives of the "reference scenario for the deployment of emergency communications" standardization activities were:

- to provide reference scenarios for the evaluation/dimensioning of satellite-based emergency telecommunications;
- to describe the events causing the emergency situation (earthquake, public transportation accident);
- to describe the missions composing the response (e.g. search-and-rescue; logistics; first aid; emergency sheltering; water sanitization);
- to provide the important parameters dimensioning the mission activities (e.g. the number of injuries, number of displaced people and families, number of people affected by water shortage);
- to describe the information exchanges supporting these emergency missions;
- to provide a mathematical topological model showing how end-users are deployed/move on their activity field.

These results were documented in ETSI TS 103 260-1 [i.45] and ETSI TS 103 260-2 [i.46].

5.2.3 ETSI TCCE standardization

An excerpt from TCCE's terms of reference reads: "ETSI TCCE shall have responsibility:

- For the provision of user driven standards for authority to authority secure voice and data services and facilities over broadband and narrowband air interfaces.
- To collect and specify requirements from relevant stakeholders such as the Emergency Services, Government, Military, Transportation, Utility and Industrial organizations as well as Public Access Mobile Radio (PAMR) Operators.
- To maintain and develop the existing TETRA standard.

- For ETSI deliverables (in whole or in part) dealing with both TETRA and mobile broadband critical communications.
- To ensure that work programmes within ETSI TC TCCE are co-ordinated with other European and International Standards making bodies to avoid duplication of deliverables.

The work programme "mission critical broadband communications" within the ETSI Technical Committee (TC) TETRA and Critical Communications Evolution (TCCE) addresses facilitating and enhancing the services and facilities of digital PMR such as TETRA operating over LTE in order to meet new user requirements for data and voice.

Technical report ETSI TR 102 022-1 [i.41] provides the user requirement specifications for mission critical broadband communications. Apart from operational requirements it lists application requirements of PPDR which are categorized as follows:

- Location data.
- Multi-media.
- Office Applications.
- Download/upload operational information.
- Online database enquiry.
- Miscellaneous.

IoT communications and devices are implicitly covered by the categories: location data, upload of operational information, and miscellaneous.

The technical report ETSI TR 102 022-2 [i.42] summarizes critical communications application requirements (and voice requirements) related to a Critical Communications Application (CCA) sitting above the LTE protocol. It does not provide use cases or user requirements.

5.2.4 3GPP standardization

5.2.4.1 General

3GPP covers cellular telecommunications network technologies including; radio access, the core transport network, and service capabilities which itself includes work on codecs, security, and quality of service. It thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with WLAN networks.

From early days of GSM, the emergency call service in ETSI TS 122 011 [i.17] and ETSI TS 122 261 [i.18] has been used to connect users, through GSM and the fixed circuit switched networks, to the PSAP using national emergency numbers as well as the standardized 112 emergency number. In 1972, 112 was recommended by European Conference of Postal and Telecommunications Administrations (CEPT) and later being regulated by a decision of the EU Council in 1991 (91/396/EEC [i.11]). It was subsequently reaffirmed in 2002 by article 26 of the Universal Service Directive and was superseded by Article 109 of the European Electronics Communications Code [i.12]. With the emergence of IP Multimedia Subsystem (IMS), Voice over IMS (VoIMS) was and continues to be one of the main features implemented for packet switched domains of 3GPP system. Thus, support of emergency services using VoIMS was introduced in UMTS and was enhanced with the introduction of LTE and 5G, especially from radio capacity perspective.

Public Warning Systems (PWS) is another feature that has been supported by 3GPP, see ETSI TS 122 268 [i.13]. PWS was first specified in Release 8, allowing for direct warnings to be sent from national or local authorities to mobile users on conventional User Equipment (UE) capable of displaying a text-based and language-dependent Warning Notification. PWS warning messages are sent to the UE cell broadcast (CBS) mechanisms. Support for PWS for 5G is now specified in 3GPP Rel-15. Based on 3GPP specifications, Earthquake and Tsunami Warning System has been deployed in Japan since 2007, with Earthquake Early Warning System being developed by ATIS for the US west coast. WEA/CMAS is continuously being extended by FCC ruling and is standardized by ATIS, with several countries following what has been specified for WEA e.g. Netherlands, Canada, Chile, Taiwan, Korea, Philippines, New-Zealand, China, UAE, Lithuania, Romania, etc. This solution has been supported in main smartphone operating systems, (which cover 99,8 % of devices sold in 17Q4 in the US. Looking towards the change in the industry, with the growth of IoT devices where little to no user interface and the need of alternative to text notification, additional requirements for an enhanced Public Warning System (ePWS) were introduced and included in ETSI TS 122 268 [i.13]. The target for ePWS is to specify messages especially for IoT devices that are intended for machine type communications and enabling language-independent content to be included in Warning Notifications as for users with disabilities and users who are not fluent in the language of the Warning Notifications.

Public safety is represented by Mission Critical (MC) in 3GPP webpage: http://www.3gpp.org/NEWS-EVENTS/3GPP-NEWS/1875-MC-SERVICES. A platform for MC communications and MC Services has been a priority of 3GPP in recent years and its evolution is driven by requirements from different sectors of the global critical communications industry. MC Services benefited from existing 3GPP functionalities as the use of multicast bearers in LTE due to the standardization of eMBMS and Group Communication System Enablers (GCSE). Additionally, D2D Proximity Based Services (ProSe) were enhanced to support public safety use. The application domain of MC was standardized in Rel-13, as Mission Critical Push to Talk (MCPTT). It was completed in 2016. In Rel-14, enhancements were added to MCPTT, MCData (see ETSI TS 123 282 [i.76], MCVideo (see ETSI TS 126 281 [i.75], and a General Framework was agreed that facilitated standardizing additional MC Services. The Rel-14 work on MC Services required not only a large set of new protocol additions and new security functionality, but also enhancements to the MCPTT of Rel-13 specifications to enable reuse of common functionality across MC Services, offering stand-alone functionality that enriches the existing base of MC Services, with general MCPTT enhancements in Rel-14 including the services as Mcdata and Mcvideo. Rel-15 continues adding enhancements for MCPTT and the supported services as well as adding new features as MC system migration and interconnection, MBMS usage for MC communication services, MC security enhancements. In Rel-16, enhancements to the existing system and services continues as well as adding new features, including Mission Critical Communication Interworking with Land Mobile Radio Systems.

5.2.4.2 Conclusion

The mobile communication provides the enhanced infrastructure to facilitate various emergency communications domains. Services as MC, PWS, MTC and others already exist and can be used to provide IoT for emergency communications, possibly with or without further enhancements. Work on the emergency communications domains remains ongoing under various 3GPP work items which should be referred to directly for up to date information.

5.2.5 IETF standardization

The IETF has undertaken work to develop communications protocols for emergency communications over the Internet. The IETF WG ECRIT (Emergency Context Resolution with Internet Technologies) has specified methods and procedures for routing emergency calls over the Internet using the Session Initiation Protocol of IETF RFC 3261 [i.21]. The work provides a universal solution for emergency calling via IP, between individuals and emergency services as covered by SC EMTEL.

ECRIT's work has focused on emergency speech calls, video calls, and text messaging. The core requirements of an Internet-based emergency communications system are defined as the following:

- Identification and validation of emergency calls (along all the carriers).
- Identification of calls' locations.
- Routing calls to appropriate call centres.
- Protection against spoofing.

ECRIT has published its work in best practice and framework specifications for emergency calling via IP, IETF RFC 6881 [i.22], IETF RFC 6443 [i.23], and IETF RFC 4190 [i.24]. The work of IETF ECRIT is being taken into account in the ETSI Work Item DTS/EMTEL-00037 resulting in ETSI TS 103 479 [i.85].

At the time of writing, ECRIT is in the process of addressing the issue of communications from IoT devices to support emergency situations and a draft RFC has been produced for "data only emergency calls" - see IETF Draft "Data-only Emergency Calls" [i.25]. Specifically, the draft acknowledges that in some cases the transmission of application data is all that is required to trigger an emergency response, rather than the establishment of a full-blown session between an individual and a PSAP. Such cases may include alerts issued by e.g. a temperature sensor, burglar alarm, or chemical spill sensor, and the alerts can be conveyed as one-shot data transmissions. The draft includes provision for communication to be between IoT device and an aggregator who may decide to forward the information to a PSAP, or directly between the device and the PSAP. A container for the emergency data is described based on the Common Alerting Protocol (CAP) and its transmission using the SIP MESSAGE transaction.

5.2.6 ITU standardization

The ITU is a place for many standardization efforts related to emergency situations. Indeed, works within ITU-R already deal with emergency radiocommunications. The Radiocommunications Study Groups (SG4, SG5, SG6 and SG7) carry out studies related to the development of radiocommunication systems used in disaster mitigation/relief operations.

Regarding ITU-T, different aspects of emergency situations are considered within the different Study Groups. The Partnership Coordination Panel - Telecommunication for Disaster Relief and Mitigation (PCP-TDR) has been created in February 2003. It was first approved by SG16 (Multimedia), but now is under the responsibility of SG2 (Operational Aspects).

Recommendation ITU-Ts relevant to use of IoT technologies during emergency situations include:

- **Y.2074** "Requirements for Internet of things devices and operation of Internet of things applications during disaster" [i.69]: This recommendation provides requirement for IoT devices that can be used for operation of IoT applications in the context of disaster. In includes methods concerning assurance of integrity and reliability of the data produced by IoT devices during disasterμ. It is relevant for IoT application developers, IoT service providers and emergency service providers.

- **Y.4116** "Requirements of transportation safety services including use cases and services scenarios" [i.70]: This recommendation addresses requirements for providing transportation safety services based on IoT technologies. It can be applied to various means of transportation: road, rail, maritime and air.

- **Y.4119** "Requirements and capability framework for IoT-based automotive emergency response system" [i.71]: This recommendation identifies requirements of an IoT-based automotive emergency response system (AERS) for aftermarket devices and provides a capability framework of the AERS. In particular, it addresses the overview, the requirements, and a capability framework of an AERS.

- **Y.4806** "Security capabilities supporting safety of the Internet of things" [i.72]: This recommendation identifies security threats that may affect safety and security capabilities. It determines security threats and which security capabilities can be applied to mitigate the threats. It is mostly applicable to safety-critical IoT systems such as industrial automation, automotive systems, transportation, smart cities, wearables, and standalone medical devices.

- **Y.4457** "Architectural framework for transportation safety services" [i.73]: This recommendation addresses a transportation safety management model that describes disaster management steps based on IoT technologies in order to reduce damage from disasters.

5.2.7 CEN and 3GPP standardization for the eCall

The eCall is a European initiative, defined in the Action Plan COM/2008/0886 [i.95], whose objective is to speed up the assistance to people in the event of a road accident. When the device detects an impact, for example via the airbags, or in the case of manual activation, the in-vehicle eCall system establishes a 112-voice connection directly with the relevant PSAP. This solution is based on emergency call in GSM and UMTS networks. European Parliament voted in favour of eCall regulation which requires all new cars be equipped with eCall technology from April 2018 (see eCall in all new cars from April 2018 [i.81] and Regulation (EU) 2015/758 [i.84]).The call received in less than 4 seconds (under optimal communication conditions) by emergency services is associated with a data transmission (also called Minimum Set of Data (MSD), with a maximum length of 140 bytes and containing the exact location of the vehicle, the event date, the travel direction, the vehicle identification number (VIN) and in the future, the number of passengers, the type of cargo on board if it is a heavy goods vehicle, or other information from the on-board system. Thanks to the VIN, the call provides information on the type of vehicle involved (e. g. small two-seater or seven-seater family MPVs).

When it receives the call, the PSAP can call back the vehicle's passengers if they are conscious, immediately initiate appropriate emergency assistance and report the accident to the relevant traffic management centre, which will disseminate the information on its own network. Except in the case of an accident, the eCall system remains inactive. Furthermore, it is important to prevent unintentional or malicious triggering of the system, which could, if it were to happen too often, overload PSAPs.

This technology has been standardized by CEN TC278 WG15, in cooperation with 3GPP. The standards specify how the system works, the content and format of the MSD as well as the methods for transferring the call to emergency services through the cellular network, and the methods and content of the validation tests. The introduction of a standardized system on all new models from April 2018 make it possible to offer this emergency calling service to the entire automotive market.

The longevity of GSM networks in the EU over the lifetime of vehicles is uncertain and GSM spectrum is likely to be re-allocated for UMTS, LTE and/or 5G. There is no CS emergency call in LTE and 5G on one hand, on the other hand LTE spectrum leads to extensive LTE coverage. The applicability of the existing technical solution for eCall (in-band modem) is assessed for VoIP/VoLTE, as well as new technical solutions is developed that are suitable for packet switched (UMTS, LTE and 5G) and offer better performance for eCall for VoIP (see ETSI TR 103 140 [i.80]). The related normative specifications can be found in CEN TS 17184 [i.82] (IMS eCall) and CEN TS 17240 (testing) [i.83]. CEN TS 17184 [i.82] has references to 3GPP and IETF where the details are specified.

5.3 IoT-related standardization state of the art

5.3.1 3GPP Standardization

5.3.1.1 General

The introduction and enhancement of 3GPP to accommodate Internet of Things (IoT) has impacted both the 3GPP radio and network. In Rel-11, LTE introduced network optimizing for machine-type communications (MTC). Based on this, low cost devices were studied in 3GPP TR 36.888 [i.14] and 3GPP subsequently set minimum requirements that match 2G data rates. Following that, normative work started in Rel-12, where eMTC is introduced delivering further LTE enhancements for Machine Type Communications, with UE Cat 0 type that has the characteristics of less complexity, saving battery life significantly, having one antenna with uplink and downlink throughput reduced to 1 Mbit/s. In Release 13, 3GPP developed new technologies for the support of internet of things; Extended Coverage GSM Internet of Things (EC-GSM-IoT), LTE for Machine-Type Communications (LTE-M) and Narrowband Internet of Things (NB-IoT). The different technologies EC-GSM-IoT, NB-IoT, and LTE-M are also called CIoT.

Study on MBMS User Services for IoT; Rel-16, described in [i.16]. The technical specification can be found in 3GPP TS 26.850 [i.15]. From the scope of 3GPP TS 26.850 [i.15], this WI studies and evaluates the enhancements at the service layer to support massive file delivery for IoT devices to support simplified mechanisms and protocols in a typically constrained environment associated with IoT communications (e.g. processing power, storage, battery life, bandwidth) by looking at different requirements of different IoT device categories. This covers NB-IoT or eMTC devices. It also reviews the existing multicast/broadcast service architecture in support of MBMS delivery to IoT devices.

3GPP Rel-16 also defines CIoT over 5G. The solution for CIoT over 5G is in line with what has been defined earlier for 4G taking into consideration the 5G requirements, noting that 5G core network is a service-based architecture.

5.3.1.2 Conclusion

3GPP has studied IoT in the framework of MTC/CIoT (Rel-11 to Rel-14) that covers 2G, 3G and 4G. In 5G, 3GPP Rel-15 covers IoT in its framework specifically reusing the existing multicast/broadcast service architecture in support of MBMS delivery to IoT devices as well as introducing CIoT over 5G system.

Work in the domain of IoT remains ongoing under various 3GPP work items which should be referred to directly for up to date information.

5.3.2 IETF standardization

5.3.2.1 General

Regarding IoT standardization at IETF, seven different WGs are active and have already produced the first wave of mature standards for the IoT. The summary below has been adapted and updated from an article "Internet of Things: Standards and Guidance from the IETF" in the IETF Journal [i.44].

IETF 6LoWPAN: Ipv6 over Low-power WPAN. The 6LoWPAN Working Group defined methods for adapting Ipv6 to IEEE 802.15.4 (WPAN) networks that use very small packet sizes by means of header compression and optimizations for neighbour discovery. The present 6Lo WG that replaced 6LoWPAN once it had concluded its work in 2014, has applied similar adaption mechanisms to a wider range of radio technologies, including "Bluetooth Low Energy" (IETF RFC 7668 [i.53]), Recommendation ITU-T G.9959 [i.92] (as used in Z-Wave, IETF RFC 7428 [i.54]), and the Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE) cordless phone standard.

IETF ROLL: Routing Over Low-power Lossy networks. IETF ROLL WG has produced specifications for both the RPL protocol "Ipv6 Routing Protocol for Low-Power and Lossy Networks" (IETF RFC 6550 [i.55]) as well as a set of related extensions for various routing metrics, objective functions, and multicast. ROLL has also produced requirements documents, applicability statements, a terminology document, and a security threat analysis.

IETF CoRE: Constrained RESTful Environments. IETF CoRE remains one of the most active IoT groups in IETF. Its main output has concerned the "Constrained Application Protocol" (CoAP, IETF RFC 7252 [i.56]), a radically simplified UDP-based analogue to HTTP. Extensions to CoAP enable group communications (IETF RFC 7390 [i.57]) and low-complexity server-push for the observation of resources (IETF RFC 7641 [i.58]). This is complemented by a discovery and self-description mechanism based on a weblink format suitable for constrained devices (IETF RFC 6690 [i.59]). More recently, the WG has focused on extensions that enable transfer of large resources, use of resource directories for coordinating discovery, reusable interface descriptions, and the transport of CoAP over TCP and TLS. The CoRE WG work now includes RESTCONF-style management functions and publish-subscribe style communication over CoAP, and CoRE has also been looking at a data format to represent sensor measurements, which will benefit from the "Concise Binary Object Representation" (CBOR) (IETF RFC 7049 [i.60]), a JSON analogue optimized for binary data and low-resource implementations.

IETF DICE: DTLS In Constrained Environments. IETF DICE has produced a TLS/DTLS profile that is suitable for constrained IoT devices.

IETF ACE: Authentication and Authorization for Constrained Environments. IETF ACE is working on authenticated authorization mechanisms for accessing resources hosted on servers in constrained environments and a comprehensive use case document (IETF RFC 7744 [i.61]) has been produced. The work of IET ACE has also been supported by the COSE WG that built simplified CBOR analogues for the JSON object signing and encryption methods that were developed in the JOSE WG a specification was published in May 2018 in IETF RFC 8392 [i.62].

IETF 6TiSCH: Ipv6 over the TSCH mode of IEEE 802.15.4e. IETF 6TiSCH was chartered in 2014 to work on issues beyond the usual 6Lo work, and in particular to enable Ipv6 for the Time-Slotted Channel Hopping (TSCH) mode that was added to IEEE 802.15.4 networks. The 6TiSCH overview and problem statement document (IETF RFC 7554 [i.63]) was published in 2015 and IETF RFC 8180 [i.64] specifying a minimal configuration interface in 2017.

IETF LWIG: Lightweight Implementation Guidance. The Lightweight Implementation Guidance (LWIG) WG is working on producing guidance documents for efficient implementation techniques and other considerations, including for CoAP and IKEv2 protocols, asymmetric cryptography, and CoAP in cellular networks. IETF RFC 7228 [i.65] defines common terminology for constrained-node networks. IETF RFC 7815 [i.66] covers Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation. IETF RFC 8352 [i.67] published in April 2018 provides guidance on Energy-Efficient Features of Internet of Things Protocols, and IETF RFC 8387 [i.68] gives Practical Considerations and Implementation Experiences in Securing Smart Object Networks.

5.3.2.2 Conclusion

IETF is tackling various aspects of IoT ranging from adapting IP technologies to constrained devices (IPv6 for low power networks, Lightweight RESTful protocol, routing in multi-hop networks, etc.) to optimized data formats and communications security.

Work in the domain of IoT remains ongoing in various IETF groups which should be referred to directly for up to date information.

5.3.3 ITU-T standardization

5.3.3.1 General

IoT standardization has been part of ITU-T efforts since 2011 through the Internet of Things Global Standards Initiative (IoT-GSI). The purpose of IoT-SGI [i.27] was to provide a visible single location for information on and development of necessary standards for IoT deployment. IoT-GSI also seek to harmonise different approaches to the IoT architecture worldwide. It concluded its activities in July 2015 following the creation of the new Study Group 20 on "IoT and its applications including smart cities and communities". All the ongoing activities in IoT-GSI were transferred to the SG20 where the main and current ITU-T activities on IoT are conducted. Other aspects are being tackled within other SGs:

- **SG11 - APIs and protocols for IoT:** The Study Group 11 is responsible for "signalling". It produces international standards that define how telephone calls, and also other calls such as data calls, are handled in the network. Today, SG11 studies signalling requirements and protocols for IP-based networks, SDN, NGN, M2M, IoT, future networks, IPTV, cloud computing mobility, ad hoc networks (WSN, RFID, etc.), QoS, and inter-network signalling for legacy technologies (ATM, PSTN, etc.)

- **SG13 - Network aspects of IoT:** The Study Group 13 works on next-generation networks and their evolution. Focus is also put on future networks and network aspects of mobile telecommunications. Now, it also covers network aspects of the Internet of Things, support of IoT across future networks, and Cloud computing in support of the IoT.

- **SG15 - Smart grids and Home networks:** The Study Group 15 develops technical specification of global communications infrastructures. It defines technologies and architectures for access networks, home networks. And power-utility network infrastructures.

- **SG16 - IoT applications:** The Study Group 16 works on multimedia coding, systems, and applications. It is the lead study group on ubiquitous and IoT applications, telecommunication/ICT accessibility for persons with disabilities, Intelligent transport systems (ITS) communications, e-health, and IPTV.

- **SG17 - Security and privacy protection aspects of IoT:** The Study Group 17 coordinates security-related works across all ITU-T Study Groups. It works on cybersecurity, security management, security architecture and frameworks, countering spam, identity management, protection of PII, the security of applications and services for the IoT, web services big data, social networks, cloud computing, mobile financial systems, IPTV, and tele-biometrics.

In 2012, ITU-T has published the Recommendation Y.2060/Y.4000 [i.29] where the Internet of Things (IoT) has been defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communications technologies. Recommendation Y.2061/Y.4001[i.30] has identified a set of requirements for the support of IoT applications in the next generation networks. Multiple recommendations have been published covering different aspects of the IoT and Smart Cities and Communities:

- **Y.4000 - Y.4049 General:** contains Recommendation ITU-Ts giving an overview of the Internet of Things, reference model, and machine socialization.

- **Y.4050 - Y.4099 Definitions and terminologies:** contains one Recommendation ITU-T defining IoT concepts and terminology.

- **Y.4100 - Y.4249 Requirements and use cases:** contains Recommendation ITU-Ts about common requirements and use cases of the IoT, device and gateway operations, IoT middleware and application services, semantics requirements, monitoring and quality assessment of IoT applications, etc.

- **Y.4250 - Y.4399 Infrastructure, connectivity and networks:** contains Recommendation ITU-Ts on control networks, capabilities of ubiquitous sensor networks for supporting metering services, and energy saving using smart object in home networks.

- **Y.4400 - Y.4549 Frameworks, architectures and protocols:** contains Recommendation ITU-Ts on IoT frameworks, API and protocols for M2M service layer, web of things architecture, etc.
- **Y.4550 - Y.4699 Services, applications, computation and data processing:** contains Recommendation ITU-Ts on application support model of the IoT, service description, Smart farming, etc.
- **Y.4700 - Y.4799 Management, control and performance:** contains ITU-T requirements on guidelines for deploying IoT applications and services, and framework for managing IoT networks (through the extension of SNMP).
- **Y.4800 - Y.4899 Identification and security:** contains ITU-T requirements on requirements and architecture for automatic location identification (devices, applications and services), common characteristics of IoT identifier, etc.
- **Y.4900 - Y.4999 Evaluation and assessment:** contains ITU-T requirements on key performance indicators definitions of: smart sustainable cities, the use of information and ICT, and the sustainability impacts of using ICT.

5.3.3.2 Conclusion

IoT standardization is achieved through multiple working groups at the ITU-T. Standardization activities cover multiple aspects of IoT: terminology setting, requirements collections, architecture and frameworks definition, processes and protocol specification, security management, and evaluation/assessment of IoT solutions.

Work in the domain of IoT remains ongoing in various ITU-T Study Groups which should be referred to directly for up to date information.

5.3.4 IEEE standardization

5.3.4.1 General

IEEE 802 is a group of IEEE standards that deals with local area networks and metropolitan area networks. The services and protocols designed within IEEE 802 can be mapped to the physical and data link layers of the seven-layer OSI networking reference model.

Some of the working groups belonging to IEEE 802 deal with network technologies that are used in the IoT domain. Such groups are mainly those who deal with wireless networks:

- IEEE 802.11 - Wireless Local Area Networks (WLAN): a standard base for networks using Wi-Fi certified devices;
- IEEE 802.15 - Wireless Personal Area Networks: a standard base for networks such as Bluetooth, ZigBee, Z-wave, etc.; and
- IEEE 802.16 - Broadband Wireless Access: a standard base for networks as also known as WiMAX.

In the following clauses, a short description of IEEE 802.15 technologies is given, as they are widely used in the IoT domain among other IEEE 802-based technologies such as WLAN and WiMAX.

5.3.4.2 IEEE 802.15.1 Bluetooth®

Communications between Bluetooth® devices operate over small distances and in ad hoc manner. These networks are called piconets. The network may have between 2 and 8 devices. One the network is established, one of the devices will take the role of "master" and the other will be "slaves". The piconets are dynamically and automatically formed whenever the Bluetooth® devices are within communication range.

There are several Bluetooth® specifications. The most used is Bluetooth® Basic Rate/Enhanced Data Rate (BR/EDR) and Bluetooth Low Energy (BLE).

5.3.4.3 IEEE 802.15.3 High Rate WPAN

IEEE 802.15.3 defines a protocol and compatible interconnection of data and multimedia communication equipment via 2,4 GHz and 60 GHz radio transmission in wireless personal area networks (WPAN) using low power and multiple modulation formats to support scalable data rates. It is a MAC and Physical standard for high-rate WPANs (11 to 55 Mbit/s) and it is mainly designed for multimedia streaming within local networks.

5.3.4.4 IEEE 802.15.4 Low Rate WPAN

IEEE 802.15.4 is a well-known network standard in the IoT. It has been developed by the Personal Area Network (PAN) of IEEE. It is designed to mitigate the problem of limited transmission power of IoT devices. It targets the physical and MAC layers of the ISO layered stack.

The IEEE 802.15.4 is known to offer a maximum of 250 kbit/s as a data rate with an output power that does not exceed 1 mW. Data packets' size is of 127 bytes making it a suitable technology for less "chatty" IoT applications on top of constrained devices.

5.3.4.5 IEEE 802.15.7 Visible Light Communication

IEEE 802.15.7 Task Group is working on developing standards for free-space optical communication using visible light. As of December 2011, the group has completed drafts for PHY and MAC layers.

Visible Light Communication (VLC) integrated with the emerging technology of Internet-of-Things (IoT) opens up to wide range of indoor applications. Shortage of energy budget has led to emergence of the energy efficient variant of the VLC i.e. VLC in the dark, which works with extremely low level of illuminance. It consumes much lower energy than the conventional VLC, which makes it more suitable for IoT applications.

5.3.5 oneM2M standardization

5.3.5.1 General

The oneM2M global initiative is an international partnership project established in June 2009 by the seven most important standard defining organizations in the world and many industrial alliances. The main goal of oneM2M is to define a globally agreed M2M service platform by consolidating isolated M2M service layer standards activities. oneM2M has the objective to boost M2M market by removing the need to re-develop common components, to simplify development of applications by providing a common set of APIs, to leverage existing worldwide networks, and to provide evolution and interoperability of standard functions support. The oneM2M technical working groups are focusing on requirements, system architecture, protocols, security, management, abstraction and semantics. Within oneM2M, all SDO members were required to stop their efforts on IoT standardization and invite their members to directly contribute to oneM2M working groups. Therefore, all the technical specification produced by oneM2M are simply transposed into corresponding SDO's technical specifications and publications.

Interoperability is at the heart of oneM2M. Indeed, oneM2M architecture aim to achieve interoperability at both the communication (i.e. the ability to communicate with any IoT device/application independently from the underlying protocol or network technology) and the data (i.e. the ability to automatically understand the data being exchanged between heterogeneous devices and applications) levels.

The development of oneM2M architecture and protocols is based on the study of use cases and the requirements derivation from these use cases. On a consensus basis, the agreed requirements are then translated into technical specifications within the relevant working groups.

oneM2M currently supports a capability to prioritize communication making it possible IoT platform for emergency situations. However, this capability may need further enhancements to support additional functionality needed for communications in emergency applications. In addition, a oneM2M platform will require mechanisms to guarantee the required quality of service for such applications. As part of if its Release 4 work, oneM2M has begun work on adding support for quality of service functionality.

5.3.5.2 Conclusion

oneM2M continues to develop the oneM2M architecture and protocols by enriching them with additional features. oneM2M has published stable specifications for releases 1, 2 and 2A. Releases 3 and 4 are currently published as drafts.

oneM2M is a promising standard in the IoT domain and is likely to be widely deployed in the near future. oneM2M platforms will be at the centre of communications between IoT devices and IoT applications where some of them will be used in emergency situations.

5.4 Communication networks deployed

5.4.1 Networks related to emergency communications domains

5.4.1.1 Emergency Calling

Network Operators are not necessarily responsible for the deployment of networks for emergency calling, rather they provide prioritized routing and communications between users of the network and Public Safety Answering Points (PSAPs) within the emergency services network. In the past this has been based on Circuit Switched voice telephony, but since the deployment of next generation including LTE networks, the emergency services and Public Safety authorities in some countries have started to upgrade their networks to SIP based multimedia solutions as described in the EENA NG112 report [i.79].

5.4.1.2 Mission critical communications

Figure 1 and Figure 2 are based on ETSI TS 103 260-2 [i.46]. They depict the main involved entities/roles and typical communication channels during a small/medium and a large-scale incident. These set-ups are largely common for emergency and disaster management approaches in Europe, but there are various regional differences. In fact, the authority(s) to decide on incident related issues depend(s) on the actual legislation, on the sort and extent of the incident, and on the involved emergency/public safety services.

Directly and indirectly affected individuals interact with public safety answering points (PSAPs) and/or authorities via fixed/mobile voice services via emergency calling (see above).

Examples for the "infrastructure" block are hospitals, shelters, technical equipment, materials, catering, etc.

"Information sources" provide information about emergency management that includes but is not limited to:

- preparedness activities;
- contingency plans including e.g. alarm plans and dispersion models; and
- weather forecasts.

In the background, the support area in strategic and administrative level of communication is mainly based on fixed (private) networks for voice and data.

Each deployed emergency/public safety service discipline may have its own hierarchy structure in the incident area consisting of teams, sector commands, and a service incident command. Emergency/public safety services may combine two or more disciplines (e.g. technical rescue and emergency medical service) within the same command hierarchy. This applies to public safety answering points (PSAPs) and emergency control centres (ECCs) in the background support area, too. The coordinating on-site incident command can be subject to individuals or task forces.

Figure 1 and Figure 2 provide an overview of state-of-the-art communications between authorities/organizations during small to medium incidents and large-scale incidents. The involved rescue services (e.g. technical/medical rescue, social care, firefighting, police, etc.) are shown as "services A, B, C…". Depending on the incident there might be none, one or many field emergency control centres (FECCs) for each rescue service operating in a hierarchical structure. E.g. in case of a mass casualty incident the medical emergency command structure might have dedicated sector FECCs for the triage area, for the interim care centre, and for the transport section (see ETSI TS 103 260-1 [i.45] and ETSI TS 103 260-2 [i.46]).

Emergency/public safety services communicate between the incident area and the off-site area mainly by means of dedicated push-to-talk trunked mode operation PMR systems, whereas on-site communications are normally based on direct-mode operation PMR services.

As an anticipation of future developments including IoT applications "private mobile data" is depicted as separate information exchange entity.

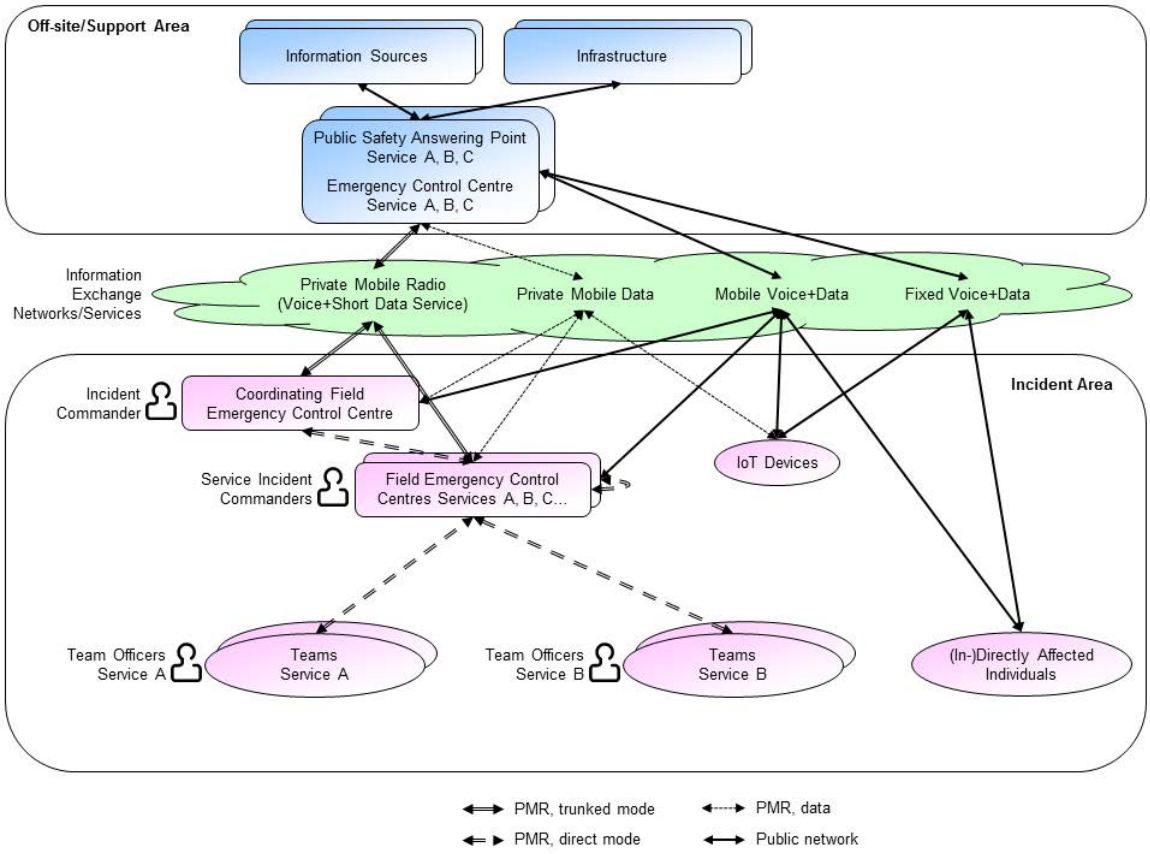


Figure 1: Overview state-of-the-art communications between authorities/organizations during small to medium incidents

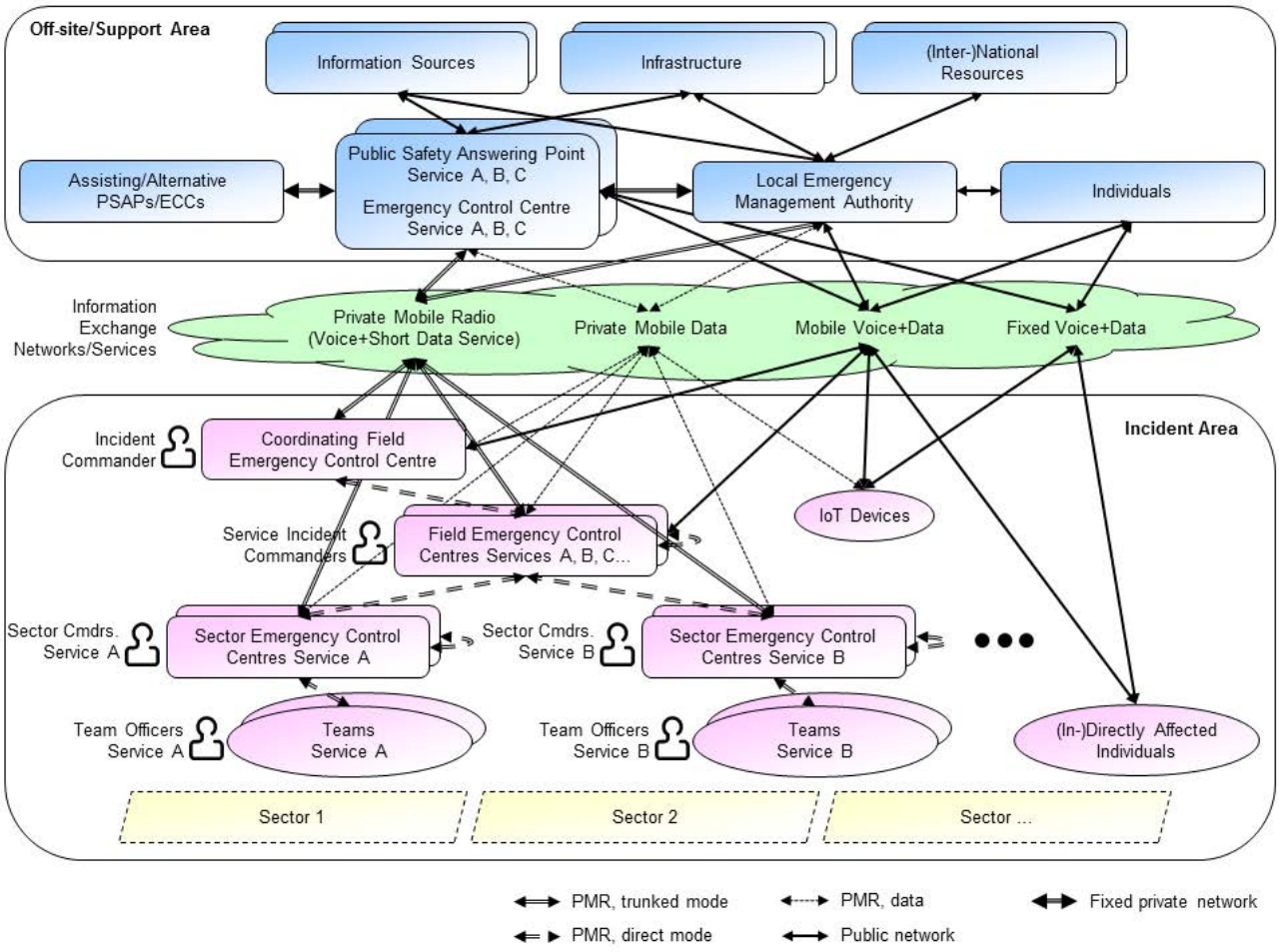


Figure 2: Overview state-of-the-art communications between authorities/organizations during large scale incidents

The voice communications systems of emergency / public safety services have been traditionally based on private narrow band radio network systems such as TETRA (Terrestrial Trunked Radio) or Project25 (P25). Although such systems offer critical communication essential functionality such as device to device communication, group management, floor control, etc., they tend to suffer from low spectral efficiency, limited data transport capabilities, slow evolution, and high-cost due to lack of economies of scale, as well as problems with interoperability and interconnectivity to different deployed systems. For these reasons, emergency/public safety services are increasingly looking to supplement their communications with the enhanced capabilities offered by mobile broadband networks and connected smart devices.

The need for enhanced capabilities for emergency/public safety services was recognized by the mobile telecommunications industry, and a new working group was subsequently established in 3GPP (Working Group SA6) specifically to look at mission critical communications and applications.

A whitepaper from the GSMA [i.10] discusses how the enhanced capabilities of LTE networks can be leveraged to provide not only critical communications at the same level as existing solutions, but also to provide an enriched experience allowing users to exchange multimedia content and to access supporting information from other sources via mobile broadband, thus extending the traditional Mission Critical Push To Talk (MCPTT) communications to also Mission Critical Video, and Mission Critical Data. The paper gives an overview of the SIP based MCPTT technology specified in 3GPP and talks about the opportunities that user of mobile broadband networks provides. It also outlines a case study for establishing Public Safety Mobile Broadband Network, based on the activities of Telstra in Australia.

According to the GSMA whitepaper [i.10], more than 30 countries worldwide have now started assessment, planning, and even deployment of mobile broadband based mission critical services with the primary focus being on replacement of legacy systems.

5.4.1.3 Public Warning System

Public Warning Systems (PWS - also known as Public Warning Service), are sometimes considered part of mission critical communications, see GSMA Whitepaper [i.10]. For the purposes of the present document however, they are treated separately.

Work on PWS has been ongoing in 3GPP since release 8 and deployments are therefore more mature than those for Mission Critical Communications. However, the amount of information broadcast by PWS systems remains constrained up to 9 600 octets in E-UTRAN and 5G (1 230 octets in UMTS and GSM), see ETSI TS 123 041 [i.74]. Neither of the existing 3GPP specified systems (PWS nor ETWS) have been defined to make use of LTE broadcasting technology that could deliver enriched messages requiring higher bandwidth to users in a given geographical area. As such, they have limited capabilities in terms of the content that can be delivered.

In GSMA Whitepaper [i.10], GSMA discusses how PWS solutions might exploit eMBMS to provide an enhanced Public Warning System. It should be noted however that although deployments of eMBMS are beginning to pick up, the number of devices supporting eMBMS remains very limited compared with the overall number of devices in use. As such, the provision of enhanced PWS services in the future may be as dependent on the deployment of eMBMS services and availability of eMBMS capable handsets, as it will be on the specification of eMBMS enriched PWS and regulatory requirements for such a service.

5.4.1.4 Conclusion

- The use of additional information from IoT devices to support emergency calling, requires such devices to support and/or interwork with protocols such as SIP and its extensions that are being deployed as part of the next generation 112 services.
- The use of IoT devices to effectively support Mission Critical Communications, requires such devices to support and/or interwork with protocols such as SIP and its extensions that will be used to implement future Mission Critical systems.
- The current limitations of PWS in terms of message size will, unless there are changes to the PWS standard, constrain the amount of additional information that could potentially be provided to the IoT devices in PWS broadcasts, between IoT devices, or between an IoT device and a responding entity.

5.4.2 IoT networks from mobile telecom operators

5.4.2.1 General

The state of the art concerning IoT from the network operators' point of view can be found in the Mobile IoT Rollout Report from GSMA [i.26]. Based on interviews with 23 mobile operators, the report outlines how two different types of mobile IoT networks (LTE-M and NB-IoT) are being deployed around the world, as well as the lessons learned so far by the operators and their future plans.

According to the GSMA in [i.26], there are at the time of writing 48 commercial networks provided by the 23 operators in 25 countries. Of these, 23 are in Europe with Deutsche Telekom and Vodafone providing NB-IoT connectivity across Austria, the Czech Republic, Ireland, Italy, Germany, Spain, Turkey, Slovakia, Greece and the Netherlands. Velcom in Belarus and Telia in Norway and Finland have also launched NB-IoT networks, while Telecom Italia's NB-IoT network exposes services using the oneM2M platform. Turkcell and Orange have rolled out both NB-IoT and LTE-M across their LTE footprints in Turkey and Belgium respectively, while KPN has switched on LTE-M in the Netherlands.

The LTE-M and NB-IoT networks are based on solutions standardized by 3GPP in 2016 for use in licensed spectrum. They enable mobile operators to address a wide range of potential use cases from smart metering and smart parking to asset tracking and consumer wearable devices. In agriculture and forestry, Mobile IoT connectivity can enable farmers to monitor the location and condition of their livestock, while tracking the health of crops and plantations. NB-IoT and LTE-M can also be used to cost-effectively connect sensors monitoring the performance of an array of industrial machinery. As demand grows, the Mobile IoT ecosystem is expanding and a multitude of Mobile IoT modules, chipsets and software are said to have been certified as compliant with Release 13 of the 3GPP standards. In 2018, many more mobile network operators are expected to roll out commercial Mobile IoT services. By March 2019 the GSMA expects the Mobile IoT will be available in more than 40 countries.

5.4.2.2 LTE-M (Long Term Evolution for Machines)

LTE-M is the industry term for the eMTC LPWA technology standardized by 3GPP in Release 13 and it specifically refers to LTE CatM1, which is designed to support the IoT (Category 1 UE suitable for IoT). The deployed LTE-M is a low power wide area (LPWA) technology operating in a bandwidth of 1,08 MHz and with a peak data rate of 1 Mbit/s, providing low device complexity and extended coverage, while allowing the reuse of existing LTE base stations. The technology can allow connected devices to have a battery lifetime of at least 10 years for a wide range of use cases. LTE-M also supports mobility, roaming, and potentially voice services via VoLTE. The LTE-M solution is promoted and supported by the GSMA LTE-M Task Force.

5.4.2.3 NB-IoT (Narrowband Internet of Things)

Narrowband IoT (NB-IoT) is a low power wide area (LPWA) technology standardized by 3GPP in Release 13 and also related to LTE. NB-IoT minimizes the power consumption of connected devices, which allows for increased capacity in deployed systems with greater spectral efficiency, especially in locations that cannot easily be covered by conventional cellular technologies. In a wide range of use cases, NB-IoT connected devices are expected to have a battery life of more than 10 years. NB-IoT employs a new physical layer with signals and channels to meet the demanding requirements of extended coverage in rural areas and deep indoors, while enabling very low device complexity (much less than that of GSM/GPRS modules). It operates in a bandwidth of 180 kHz with a peak data rate of up to 100 kbit/s. The NB-IoT solution is promoted and supported by the GSMA NB-IoT Forum.

5.4.2.4 Conclusion

The number of MNO providing IoT network continues to grow and are potentially capable of delivering large amounts of data from IoT devices in emergency situations.

5.4.3 Additional long-range IoT networks

5.4.3.1 General

Recently, IoT network deployment has witnessed the arrival of new actors other than classic telecom operators such as Sigfox. Indeed, these new IoT network operators mainly use unlicensed frequencies. This allows the network operator to rapidly deploy and operate a network. Moreover, the nature of the chosen frequencies bands (ISM [i.28]) and coding-modulation techniques offer long-range and energy-efficient communications using a single radio access point (base station). Such advantages come at the cost of low data rates and duty-cycle limitation. However, such networks are still a viable solution for some IoT applications. Such networks include but are not limited to Sigfox, and LoRa/LoRaWAN networks.

5.4.3.2 Sigfox

Founded in 2009, Sigfox company develops a proprietary technology, described in their website (https://www.sigfox.com/en/sigfox-iot-technology-overview) and in an IETF draft [i.38] in order to connect IoT devices to the Internet at very low costs.

The radio technology uses ultra-narrow band (UNB). The signal is within a frequency band of only few tens of Hertz (EU/Middle East 868 MHz, North America 902 MHz, South America/Australia/New Zeeland 920 MHz). The technology developed by Sigfox allows a long range up to 40 km, and the power consumption of the radio chip is 1 000 times lower than a GSM radio chip. Thus, Sigfox connected devices may pretend to 10 years lifetime. Finally, the low cost per device allowed a large adoption of this technology.

The Sigfox network architecture can be seen as a star topology with Sigfox Cloud at the canter and Sigfox gateways/base stations around. Data communications are as follows:

- IoT devices send data to one or more gateways within communication range.
- Sigfox gateways relay all the received messages to Sigfox back-end servers where duplicates are suppressed.
- Sigfox servers will forward the received data to the customer IT through a notification mechanism. A copy of the data is also kept on Sigfox servers and can be accessed through a simple REST APIs over HTTP.

- Finally, if there are data to be send back to the IoT devices, then they are cached and piggybacked to the target device whenever it will transmit a message.

Sigfox connected devices are uniquely identified and since Sigfox servers are accessible worldwide, no roaming is necessary if IoT devices are transported from one country to another.

However, the Sigfox radio technology only allows a very low data rate. Precisely, a Sigfox device can transmit 150 messages of 12 bytes each per day. Therefore, Sigfox does not compete with classic telecom operators, but still provides a solution of choice for many IoT applications offering services with constrained devices.

5.4.3.3 LoRaWAN

Similar to Sigfox technology, LoRaWAN (https://lora-alliance.org/about-lorawan) and [i.39] is a network technology that allows communication over long distances with low data rate using the ISM frequency bands (EU 863 - 870 MHz, US 902 - 928 MHz, Australia 915 - 928 MHz, and China 779 - 787/470 - 510 MHz) [i.28] . It can be used as a primary communication infrastructure for connecting constrained IoT devices operating on batteries. However, and unlike Sigfox technology, LoRaWAN allows 3 different communications modes for the IoT devices:

- Class A - Lowest power, bi-directional end-devices.
- Class B - Bi-directional end-devices with deterministic downlink latency.
- Class C - Lowest latency, bi-directional end-devices.

Also, unlike Sigfox, LoRaWAN technology is an open standard developed by an industrial alliance: LoRa Alliance. The alliance includes among its members many network operators like Orange, Bouygues Telecom, Swisscom, NTT, etc.

Due to its low data rate, LoRaWAN technology fits very well less "chatty" IoT applications requiring less frequent and smaller data messages (e.g. monitoring of a sensor value).

5.4.4 Other IoT short range networks

5.4.4.1 General

Besides infrastructure-based networks for IoT, other technologies have propelled IoT devices and a large deployment of IoT. These networks are mainly wireless and operate within local areas. Technologies such as Bluetooth and ZigBee are widely used in Smart Home, Smart building, E-Health, Smart Cities, and Wearables verticals. Many of the most used of these network technologies are being developed within IEEE. An overview of IEEE standardization for IoT networks is presented in clause 5.3.4.

5.4.4.2 ZigBee

ZigBee is a wireless communication standard developed by the ZigBee Alliance. It specifies a short-range and low power communication stack for wireless personal networks. The ZigBee protocols stack is based on IEEE 802.15.4 [i.96] that defines the physical and the MAC layers. Among the main characteristics that made the success of ZigBee:

- A low energy consumption.
- An optimal use of channels bandwidth.
- A low-cost devices and deployment.

For these raisons, ZigBee is nowadays present in embedded environments where energy consumption is a selection criterion. ZigBee is also found in smart homes where several sensors and actuators are using ZigBee. E-Health and Smart factory vertical domains are also a field where ZigBee is widely used.

5.4.4.3 Z-Wave

Similar and competitor to ZigBee, Z-Wave is a protocol stack developed by the Z-Wave Alliance. It is also using IEEE 802.15.4 for its physical and MAC layers. Z-Wave is characterized by:

- Mainly targeting the Smart Home domain.
- Relatively secure, compared to ZigBee technology.
- Bidirectional communications; Z-Wave devices can act as both receiver and transmitter.
- Mesh networking: devices can be organized into a mesh network where they can route data packets belonging to other Z-Wave devices.

Z-Wave technology allows the setup of a mesh network of up to 232 nodes which is acceptable for Smart Home applications.

5.4.4.4 EnOcean

The EnOcean alliance provides a standard for interoperable wireless communication, that has been ratified by the IEC, to develop a technology for "energy harvesting" for self-powered monitoring and control systems. These systems are mainly targeted for smart and sustainable building, smart homes, smart transportation, etc.

Thanks to micro energy converters (mechanical movement, light, temperature difference, etc.), EnOcean allows wireless communications between battery-less devices and EnOcean gateways. This technology is very convenient for environments where IoT devices lack a source of energy.

5.4.4.5 ANT/ANT+

ANT/ANT+ is a protocol and a silicon solution for ultra-low power practical wireless networking applications. It facilitates interoperability between ANT+ Alliance (see at https://www.thisisant.com/) member devices and the collection, automatic transfer and tracking of sensor data. Its finds applications in sport, wellness management and home health monitoring. ANT+ defines device profiles that specify data formats, channels parameters and network keys.

5.5 Support of emergency by IoT sensors and platforms

5.5.1 Overview of IoT landscape

From the work of the AIOTI WG03, and later on the works conducted by the STF505 group, it appears that IoT standardization landscape is highly fragmented. Indeed, many SDOs are working on standards related to the IoT technologies. These standards can cover one or multiple verticals domains, and finally the IoT standard can be at different levels of the ISO communication stack or sometime transversal to this stack.

The main IoT vertical domains covered by these studies of IoT standards are:

- **Smart Cities:** modern cities are evolving to become interconnected ecosystems where all components are working together in support of humans. By using IoT, cities are expected to achieve a transition to smart and sustainable cities.
- **Smart Living environments for ageing well (e.g. Smart Home):** IoT is expected to support the population of elderly people in living longer, staying active, etc. together with reducing the cost of care systems and providing a better quality of life.
- **Smart Farming and food security:** IoT is expected to improve the optimization of the overall farming value chain. This will be achieved through the orchestrated automation as well as data gathering, processing and analytics thanks to IoT technologies.
- **Smart Wearables:** Integration of IoT devices into clothes, patches, watches, and other body-mounted devices will provide new opportunities and applications.

- **Smart Mobility (smart transport/smart vehicles/connected cars):** The use of IoT technologies in the mobility domain creates major innovations such as self-driving and connected vehicles, multi-modal transport systems, and intelligent transportation infrastructures (roads, parking garages, etc.).
- **Smart Environment:** IoT is a key technology for environment monitoring and control (air and water quality, atmospheric conditions, etc.).
- **Smart Manufacturing:** Integration of IoT with factories and industrial environments will bring more intelligence. Connected objects provide sensing, measurement, control, power management, and communications.

Besides these vertical domains, IoT standards can be classified with regard to their Knowledge Area (KA). The Knowledge Areas (KA) used in the present document are the ones detailed in STF505 report ETSI TR 103 375 [i.7] on "IoT Standards landscape and future evolution" and based on the initial definitions from AIOTI WG03 report [i.36] on "IoT Landscaping":

- **Communication and Connectivity:** this KA covers specifications of communication protocols at all layers, e.g. PHY, MAC, NWK, Transport, Service, and Application layers. It includes the management associated with the knowledge Area.
- **Integration/Interoperability:** this KA covers specifications of common IoT features required to provide integration (assembly of sub-systems) and interoperability (interoperation of heterogeneous sub-systems) such as technical profiles and testing specifications.
- **Applications:** this KA covers support of the applications lifecycle. This includes development tools, application models, deployment, monitoring and management of the applications. For example, the support methods for installing, starting, updating applications
- **Infrastructure:** this KA covers the design, deployment, and management of computational platforms and infrastructures (e.g. network elements, servers, etc.) that support IoT-based usage scenarios.
- **IoT Architecture:** this KA covers the specification of complete IoT systems, with a focus on architecture descriptions.
- **Devices and sensor technology:** this KA covers mainly device and sensor lifecycle management such as device monitoring, configuration management, etc.
- **Security and Privacy:** this KA covers all security and privacy topics. Examples are: communication security and integrity, access control, AAA management, PII Management, etc.

The study conducted in STF505 included an IoT standards gap analysis, published as ETSI TR 103 376 [i.35]. It has revealed the following gaps:

- Duplication of IoT architectures and models
- Large number of communication protocols addressing different types of communications requirements
- Proprietary data models and mostly specific to vertical domains where they apply
- Lack of harmonization in processing rules and decision-making processes
- Security and privacy are addressed on an isolated basis
- Ambiguity on the data ownership
- Weak acceptance from end-users

5.5.2 Overview of IoT service platforms

An IoT service platform is the intelligent layer between applications, networks and IoT devices (see presentation on IoT Service Platforms [i.37]). It is a coherent set of standardized functionalities. An IoT service platform is considered as an enabler for communication and data interoperability (see ETSI TR 103 376 [i.35]).
An IoT service platform provides a rich set of functionalities for IoT applications developers. Such functionalities include:

- Device management:
  - Device configuration: initial and dynamic configuration of IoT devices.
  - Device provisioning: upload of device programs/firmware/etc.
  - Connectivity monitoring: surveillance of connectivity links of the device (state, performances, etc.).
  - Device supervision: monitoring and control of the IoT device.

  Device management can be achieved remotely and in a bulk fashion (i.e. management of a large group of IoT devices). Device management can be provided directly by the IoT service platform or through the abstraction of dedicated device management protocols. For example, oneM2M service platform relies on OMA DM, OMA LWM2M, and BBF TR.069 for its device management services.
- Messages and data management:
  - Message routing: ability to transmit a data message to its final destination in the whole IoT network.
  - Group management: ability to control or access a group of IoT devices at once.
  - Data storage: Ability of the platform to keep track of the data received from the devices.
  - Notifications management: Ability to provide IoT application (or IoT devices) with updates (asynchronous communications).
  - Access right management: Ability to control who can access a resource (data, device, etc.) and what operation is allowed for this particular user.
- Application management: tooling, SDKs, APIs, rapid application development environments. Ability of the IoT service platform to provide enablers for IoT application development such as high-level abstractions, dedicated programming languages, etc.

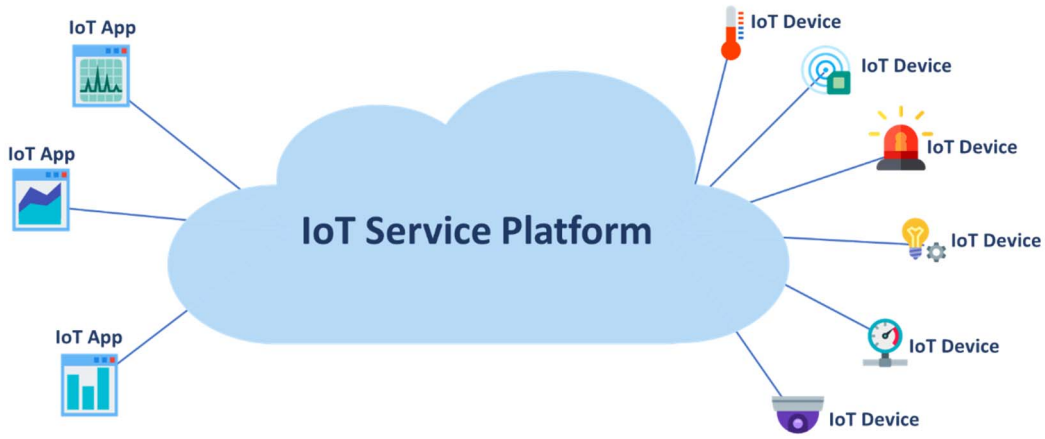


Figure 3: High Level Illustration of an IoT Service Platform

Many IoT service platforms exist on the market. Most of them are proprietary, but few ones are being standardized in SDO and/or industrial alliances. Among these platforms [i.37]:

- **oneM2M platform (from oneM2M Partnership Project) [i.37]:** a generic IoT service platform, designed for multiple vertical domains. Interoperability is at the centre of oneM2M. oneM2M is an interworking framework that provides semantic interoperability and ontologies support, and allows information exchange between heterogeneous devices, networks, services and applications, together with data communication, storage and access control.

- **AllJoyn and IoTivity (from Open Connectivity Foundation) [i.37]:** both are software frameworks that target seamless device-to-device communications in local networks and especially smart home and smart building scenarios. Common networking technologies for the smart home are natively supported such as UPNP, Bluetooth, ZigBee, etc. These platforms can also interwork with other platforms through interoperability features (Gateway agent, Analytics connector, Device system bridge)

- **IPSO Framework (from the IPSO Alliance) [i.37]:** is a set of models/protocols, guidelines and best practices. It offers data interoperability through the support of data semantics, and communication interoperability through bindings to a well-defined communication meta-model.

- **Thread (from the Thread Group) [i.37]:** is a network and transport stack that is open and secure supporting a variety of smart home products (appliances, access control, climate control, energy, safety, etc.). Communications are mainly based on IEEE 802.15.4 and 6lowpan.

A study of these IoT service platforms in the STF505 reveals that oneM2M is a generic IoT service platform designed for multiple verticals while other platforms are mainly targeting smart home/building scenarios.

5.5.3 Drones as special IoT devices

Recently, the use of drones or UAV (Unmanned Aerial Vehicles) has been generalized especially by hobbyists and professionals such as photographers or safety inspectors (roads, railway systems, etc.). They are also trialled for merchandise delivery. Drones can also be used for emergency services. Indeed, drones can provide both contextualized information about an incident area, and act as delivery support such as dropping lifesaving equipment (i.e. medicines, Automatic External Defibrillator or AED, …) for victims in areas reachable with difficulties. The emergency services can and will benefit from the use of drones or RPAS (Remotely Piloted Aircraft System) in different ways. Indeed, drones can be used differently depending on the incident phases (mitigation, preparedness, response, and recovery). Their applications can be classified into: surveillance, reconnaissance, telecommunications, transport, and entertainment.

Drones come in different sizes and types. They can be classified in different ways based on their: use (civilian/military), lift (fixed-wing, multi-rotors), MTOW (Maximum Take-Off Weight), etc. Depending on the drone's performance, drones can be used by emergency services and or disaster management agencies for example to:

- Stream in real-time video and audio from the incident area. Very convenient when the incident area is a large geographic area and/or where the incident area may present considerable risks for the intervention team.

- Transport of technical (people/animal detection device in the case of earthquake or avalanche) and/or medical equipment (medical drugs, emergency blankets/flotation, etc.) from and to the incident area if it is unreachable or accessible with considerable delays.

- Carry or install loud speakers for warning citizens in an affected area (e.g. toxic cloud, tsunami, etc.).

- Monitor large fields and forests during dry spells to reduce the risk of wildfire.

According to the EENA report on "RPAS and the Emergency Services" [i.78], drones can be used differently by different emergency services:

- **Police services** may use drones for: incident control in order to increase/improve situational awareness, crowd observation, aviation security, stolen vehicle search, etc.

- **Emergency medical services** may use drone for: delivery of first aid to an affected area, providing specialist equipment (such as defibrillators) to first responders, providing situational awareness to the HEMS (Helicopter Emergency Medical Service) pilot in advance of landing, etc.

- **Fire and rescue services** may use drones for: obtaining situational awareness information using different sensors (IR cameras, temperature sensors, etc.) to access potential fire risks, inspecting building in advance of fire crew deployment, detecting and reporting hot spots during an intervention, or critical points post fire suppression, assessing potentially dangerous incidents (e.g. presence of hazardous materials), etc.

5.5.4 Existing implementations and trials using IoT sensors for emergency situations

5.5.4.1 Emergency calling

There are several commercially available technologies for fully (direct notification of PSAPs) or semi (a human operator checks the alert for plausibility) automatic emergency calling. Examples include:

- automatic fire detection systems in buildings and industry plants;
- monitoring of Chemical, Biological, Radiological and Nuclear (CBRN) air and water pollutants;
- vehicles which automatically dial 112 in the event of a serious road accident (eCall);
- emergency beacons activated by aircraft and ships;
- surveillance systems for the early detection of forest fires (e.g. product description in https://www.iq-firewatch.com/); and
- water level monitors for flood control and prediction (e.g. product description at https://www.seba-hydrometrie.com/).

5.5.4.2 Mission critical communications

5.5.4.2.1 Based on PMR systems

Apart from status message transmission (based on the "short data service") the TETRA hand/mobile radio terminals are able to send their GNSS coordinates (automatically or on request).

5.5.4.2.2 Proprietary solutions

For local communications in the incident area, proprietary solutions are already being deployed. Examples for such proprietary solutions are given hereafter:

- Vendors offer products for respiratory equipment wearers which communicate the actual status of the wearer (e.g. manual/automatic distress signal, cylinder pressure) to the entry control point. In the opposite direction the entry control point can send withdrawal or evacuation signals.
- Many public safety agencies/organizations use Unmanned Aerial Vehicles (UAV) with live video streams for search and rescue, surveillance, and exploration operations.

Other existing solutions transmit mission critical data on top of public networks. Examples are:

- State-of-the-art vital parameters and electrocardiography monitors for pre-clinical treatment are able to transmit live patient data towards the receiving hospital or remote specialists.
- For management of mass casualty incidents there are a few local/regional approaches based on electronic devices for registration of affected persons and mapping of these persons to transport means and destination hospitals. These solutions are not based on commonly accepted standards.

5.5.4.2.3 Research and trials

Apart from many quasi-stationary sensor/actor IoT applications ongoing research works address simultaneous localization and mapping (SLAM) with different sensor fusion approaches. The general problem statement is both generating a map of an unknown environment and determining the agent's position as accurate as possible at the same time.

In environments without Global Navigation Satellite System (GNSS) reception (e.g. in buildings) other sensor data (e.g. inertial measurement units with human activity recognition, Bluetooth beacons, RFIDs, received signal strength of WLAN access points, electronic compass, barometric altimeters, ultra-wideband transmitters, etc.) and - if available - a priori knowledge (e.g. building plans) can be combined (research approaches see e.g. https://www.dlr.de/kn/desktopdefault.aspx/tabid-12629/admin-1/22033-read-50333/). Cooperative systems combine the information gathered from many agents improving the overall mapping accuracy.

There were several national research projects in the past addressing IT-supported management of mass casualty incidents (e.g. in Germany "e-Triage" and "SOGRO"). The ongoing Horizon 2020 research project TOXI-Triage http://toxi-triage.eu/) extends the scope to CBRN scenarios. Key objectives are:

- accelerated delivery of situational awareness;
- command and control with secure, dynamic and seamless communication;
- traceable point-of-care diagnostic tests with integrated casualty tracking.

5.5.4.3 Public Warning System

Japan and Chile coasts are equipped with an infrastructure to monitor earthquakes and tsunamis, as described in an inventory from researchers in Germany and Austria [i.88]. This inventory has been demonstrated with case studies in both countries.

The French research project RATCOM (2009-2011) [i.89] aimed at developing and confirming the feasibility of an evolved alerting system towards the public safety professionals on one hand and the citizens on the other hand. The project was developed in the Nice area, where small tsunamis can occur due to sub-marine landslides and may have an impact on crowded beached and harbours. The project was organized around two major components: the upstream component and the downstream component. The upstream component aimed to collect and analyse measurements from different sensors located in the harbours and other areas. It was organized around a vigilance network, SECUNET and was responsible to monitor the events occurring at the sea and report the risk level to a Control Centre. The Control Centre then took the decision to generate an alert and forward it to the downstream component, responsible to disseminate the warning within the shortest time frame possible.

At that time, the main method used to broadcast alert messages was by triggering the operation of alert sirens. However, more modern technologies were identified that could help reach a larger quantity of people. The RATCOM downstream component aimed at identifying and setup a network combining these technologies into a single framework. Some of these technologies already operational in 2011 were included in the final project demonstration. To complete this setup, an additional survey paper activity was conducted [i.89] to identify other technologies not yet ready to be included in the demonstrator. Their suitability for inclusion in the project downstream component was analysed and led to the definition of an inventory of technologies and networks not yet operational at that time, but still relevant to be used in the context of future public warning systems.

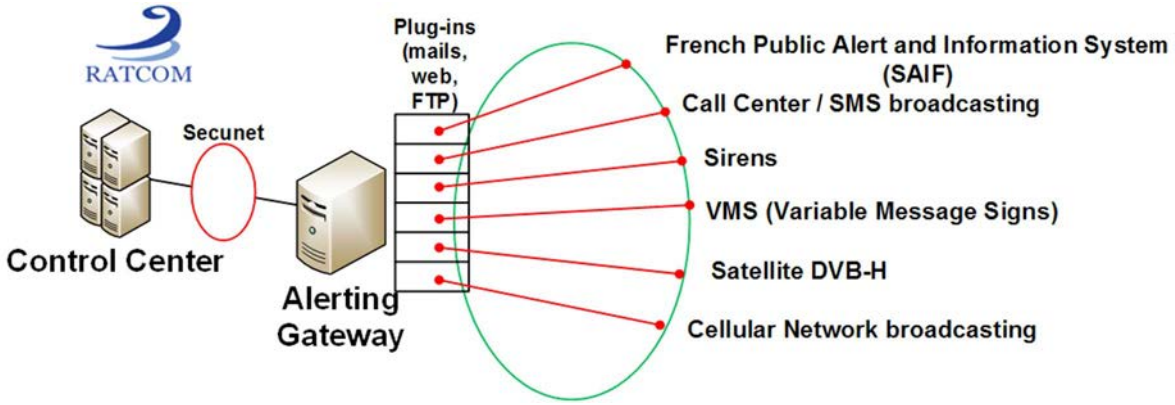


Figure 4: Downstream component of the RATCOM project

5.6 Selection of use cases and existing requirements

5.6.1 Emergency situation handling in oneM2M standard

5.6.1.1 General

oneM2M has identified use cases involving IoT devices. The complete use cases collection can be found in ETSI TR 118 501 [i.6] and ETSI TR 118 526 [i.32]. The study of these use cases resulted in the identification of common requirements and sometimes specific ones that are considered for the definition of oneM2M architecture and protocols. Within the studied use cases, two use cases cope with emergency scenarios:

1) Traffic Accident Information Collection [i.33]; and

2) Information Delivery Service in The Devastated Area [i.34].

These two use cases are described in the following clauses 5.6.1.2 and 5.6.1.3.

NOTE: Additional use cases are under study at oneM2M at the time of writing the present document.

5.6.1.2 oneM2M use case: Traffic Accident Information Collection

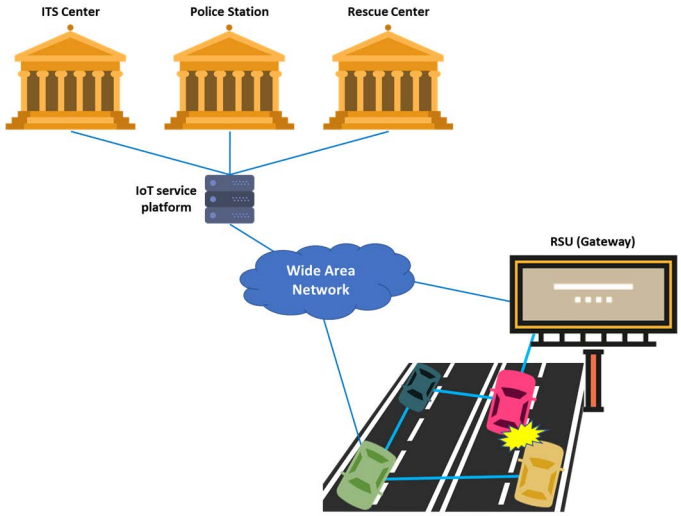


Figure 5: High Level Illustration of The Traffic Accident Information Collection Use Case

In the case of a (vehicle) accident, rescue teams need to go to the exact location of the accident in order to help the victims and the police to ease the resulting traffic jam. A rescue plan can be efficiently and quickly elaborated if the rescue team can have access to real-time information from the accident location. Similarly, the police can efficiently manage the traffic if they can get an overview of the traffic near the accident location. The relevant information can be obtained by the involved ITS stations (i.e. accident and nearby vehicles) or any other sensors (wearables, users' smartphones, roadside sensors, etc.).

5.6.1.3 oneM2M use case: Information Delivery Service in The Devastated Area

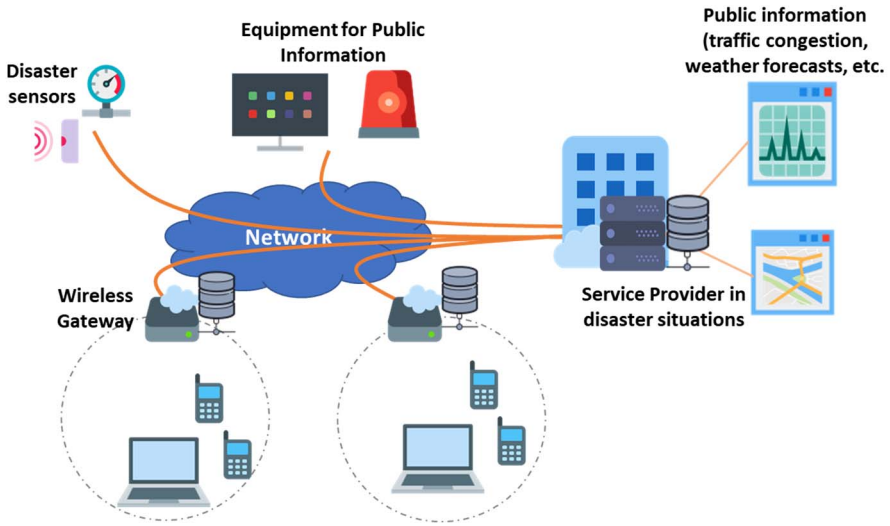


Figure 6: High Level Illustration of The Information Delivery Service in The Devastated Area Use Case

In the case of a disaster, many individuals as well as many organizations require various kinds of information that is difficult to collect immediately and properly. In this use case, an IoT service platform (IoT service provider) needs to transmit information to user devices immediately and automatically (evacuations plan, traffic congestion, hospital locations, etc.). Some localized information needs to be stored and maintained locally (to avoid network congestion) and eventually duplicated in remote location for a wider reachability.

5.6.1.4 Conclusion

From the study of the identified use cases, oneM2M technical working groups have derived a set of requirements that influenced and shaped the oneM2M architecture and protocols. This has resulted in a horizontal platform that suits multiple verticals at the same time. Emergency situations have not been considered as a specific vertical to be tackled separately. However, the consideration of some use cases related to emergency situations makes oneM2M platform capable of supporting such situations. Indeed, some oneM2M features fulfil emergency situations requirements. This includes:

- Distributed nature of the oneM2M platform: an oneM2M platform can be seen as a group of multiple nodes with the same set of capabilities. oneM2M nodes are sets of common services capabilities (CSEs).
- Seamless selection of data storage location: data produced by IoT devices can be stored seamlessly locally or on remote nodes with a powerful routing mechanism in order to access this data.
- Fine-grained access control mechanisms: access control can be set at the data instance level. Such mechanism can be used in order to make some data available based on profiles of data consumers (authorities, individuals, rescue teams, police, etc.).
- Independence from networking technologies and protocols: communications across the oneM2M platform are protocol independent and the communication channels are transparent to the applications. This allows for example a seamless handover from one technology to another in case of network failure.
- Asynchronous communications: oneM2M platform inherently support asynchronous communications through the Notification feature that works following the publish/subscribe paradigm. This is a convenient feature for receiving updates and alarms from the platform whenever a new data is produced, whether it is a physical measure (a value from a sensor) or a virtual measure (data that is generated by an analysis application). This notification will flow to all the entities (devices or applications) that have subscribed to such updates.

Finally, as oneM2M platform relies on the underlying networks, it is subject to the classic QoS issues (congestion, service guarantee, etc.). It is, thus, insufficient to tackle emergency situations without further actions at the network level such as the use of dedicated networks or channels. As part of oneM2M Release 4, oneM2M is working on adding support for Quality of Service enhancements. For example, oneM2M is looking to add the capability for a oneM2M IoT services platform to configure underlying networks (e.g. 3GPP networks) QoS parameters for a given communication session based on the QoS requirements of applications communicating over this session. oneM2M is coordinating with other SDOs (e.g. 3GPP) on this work.

5.6.2 ETSI PPDR 2016 workshop

During the workshop, two presentations addressed possible future public safety scenarios and evolution supported by IoT devices.

The future of Public Safety [i.47]

This presentation provided an overview of the upcoming introduction of data services in public safety operations, in parallel to other vertical domains such as smart city or smart health. Examples applied to public safety are video analytics, sound analytics, situational awareness, video orchestration, road safety systems, flood warning systems, and wearable technologies targeting the personal safety of first responders and firefighters. The new services identified in the presentation include monitoring of first responders' bio-vital parameters, tracking of first responders' positions during incidents, and personal protective equipment. These services bring benefits such as the capability to enhance the visual awareness at the command centre, to manage applications remotely, and to provide/increase the location awareness of first responders.

These use cases cover mainly the "mission critical communications" domain. Data transmission is proposed to be based on a hybrid communication network combining a mobile operated network with a dedicated PPDR component.

Police officers work in this new era of critical communications [i.48]

The presentation introduced new contexts and requirements for mission-critical operations as a huge number of connected devices (sensors and actuators), real-time communications, and context-awareness are now being supported. This domain is expected to evolve from critical communications to "critical intelligence". In particular, IoT devices and wearables could support police activities in the future. Examples for the evolution of policemen equipment are foreseen as follows in the presentation:

- In the 2016-2020 period, a connected policeman is assisted by a smartphone, sensors in her/his specific equipment, biometric wearables, a head-mounted display, a smart watch providing an alternate display, and a location-capable device.
- In the 2020-2030 period, the police officer holds a multi-stream audio virtual partner, biometric wearables, body-worn cameras, augmented reality glasses, and is assisted by a drone and her/his smart car for extended situation awareness.

5.7 Previous studies on IoT in emergency situations

5.7.1 EENA

In March 2016, EENA published a paper on the IoT and emergency services [i.9] that served as one of the triggers for the present study. This paper addresses mainly the 'emergency calling' domain.

The paper introduces the digital transformation of our society and how the IoT is contributing to this evolution, in all domains of our daily existence. It provides a short presentation of the IoT and how it emerged as a new technology, fostered by the arrival of small-scale processors and wearable devices, as well as connectivity capabilities such as WLAN or NFC. Sensors can monitor heat, humidity, light, or perform video surveillance. The corresponding end-to-end communication chain enables the transfer of measurements towards the processing application through a communication network.

This chain is already implemented today, for example for silent alarm buttons which trigger a call to a pre-programmed number at the PSAP. Other scenarios in the paper envision sensors in buildings, personal sensors or robots also connected to the PSAPs.

The paper analyses the impacts of this evolution on Public Safety, from the point of view of technological aspects as well as migration scenarios. The need to build an evolution strategy at Public Safety organizations to adopt these new technologies is highlighted. The paper describes a few use cases related to Public Safety involving IoT technologies, either internally to protect their staff or to enhance a situational insight or more externally to provide additional data (e.g. a patient real-time health data) in case of an emergency call. Drones can be deployed as a monitoring platform for fire protection and prevention. Third-party services can also play a major role in designing solutions that call emergency services (e.g. 112 European number) to signal that a critical situation has been detected by their algorithms.

The paper ends with a discussion on privacy and security requirements and a standardization gaps evaluation.

5.7.2 White paper on technologies for mission critical IoT

5.7.2.1 General

NOTE: Mission-critical in the referenced paper (see Keysight white paper [i.20]), and as reflected in this clause, is equal to emergency calling in the present document (device to third party or within the third-party premises, as a Hospital).

Mission-critical ecosystem that is driven by IoT devices enabling functionalities and delivering efficiencies as performance ultra-high reliability and security, so called Mission-Critical IoT 2.0 and its evolution (see white paper [i.20]).

IoT devices are expanding and entering the industry domains and applications that were never connected before. It is happening already as autonomous vehicles (preventing accidents and reporting accidents autonomously).

Several advantages of recent technologies changing the profile and cost of sensors and IoT devices, these include the high processing power, cloud technologies, support of latest protocols and high-performance radio and all competing for bandwidth as thousands of connections points requiring adequate data rates. Security of data and devices is essential as well as analytics. Policy and regulation may apply in several domains where IoT devices will be used and this is also valid for mission critical IoT.

From the paper (see white paper [i.20]), the mission critical requirements are similar to IoT devices but also specific.

Mission-critical IoT requirements often include some combination of the following:

- robust performance to withstand harsh and/or remote environments;
- precision and accuracy to work in manufacturing processes synchronized to milliseconds;
- low latency to enable real-time communication;
- programmability to support new manufacturing processes;
- scalability to support large-scale networks with tens of thousands+ controllers, robots, machinery, etc.;
- security and resiliency to protect both end-point devices and networks from disruption, and against threats and attacks;
- interoperability to ensure operation with legacy devices and operations; and
- ultra-high reliability so that devices can operate 20-30+ years in harsh environments and remote locations".

Several Challenges are identified for the IoT devices required for such use cases, as:

a) Device Layer:

   - a long lasting battery life to ensure maintenance free for several years;
   - to ensure interoperability with the ecosystem, RF modules of IoT devices need to conform to wireless standards (Bluetooth®, ZigBee, Z-Wave, Wi-Fi, NFC, and LPWA technologies such as NB-IoT, Cat-M1) that are developed to support IoT applications. This is endorsed by passing the wireless certification test before gaining market entry;
   - interference and crosstalk between each of the module's blocks should be identified and eliminated; and

- as large number of IoT devices can co-exist in proximity and operate simultaneously, Electromagnetic Interference (EMI) issues should be identified and dealt with early in the design process to ensure Electromagnetic Compatibility (EMC) compliance.

b) Wireless Communications Layer:

- needs to perform in the presence of multiple users, with different wireless technologies, in the same spectrum. This is mainly impacting the unlicensed 2,4 GHz Industrial, Scientific and Medical (ISM) frequency band that is used beside home appliances, in medical monitoring wearable devices. The various devices operating in this frequency band need to be able to co-exist and operate correctly, that is a challenge; and

- network performance and support of various wireless technologies are important. Support of different access technologies to eliminate the impact of varied locations and availability of the network to the devices is required.

c) Network Layer:

- as it is not ensured that all IoT devices on the market are tested against security, they may behave as maliciously, therefore the network needs to be able to handle such devices and provide the security required to prevent the impact that may even cause the network to go down; and

- quality of service and performance need to be maintained even during the continuous update and upgrade of the network elements and software. This means reliability of the network needs to be ensured.

Essential tools are required to build a strong foundation for IoT, these are design and the test and measurement tools. In the device ecosystem, the best tools of choice during the early research and development stage include:

- Simulation and Design Tools, to understand device operation and performance.

- Battery Drain Analysis, battery consumption in relation to operating mode (protocol, software, etc.).

- Signal Integrity Test, to evaluate high-speed serial interconnect and quickly validate and correlate signal integrity simulation with actual measurement.

- Power Integrity Test, effectiveness of power distribution network from source to load within a system.

- Wireless Conformance Test, for design verification and pre-conformance of the device to the appropriate wireless standard.

- EMI Simulation and Modelling, to simulate the radiated emission of electronic circuits and components to determine whether emissions are within levels specified by common EMC standards, and estimate emission levels before hardware is developed, respectively.

- EMC Compliance Test, to ensure products are compliant to EMC standards.

- Wireless Connectivity Test, for receiver test and troubleshooting during development and to verify, during manufacturing, that wireless IoT devices can interoperate and are able to handle multiple standards concurrently.

- Co-Existence Test, to ensure IoT devices and systems can perform their critical functions in the presence of multiple users, with different wireless technologies in the same spectrum.

- Network Simulation, verifying IOT device compliance to an operator's test plan in the integration, interoperability, and operator acceptance testing phases.

- Network Readiness, high quality service and availability.

- Network Performance Assessment and Monitoring, for verifying, quantifying, and troubleshooting network performance and reliability from pre- to post-deployment.

- Network Infrastructure Performance Test, test the peak network performance and reliability under realistic conditions to get a deeper understanding of its realistic operation under challenging conditions and scaling bottlenecks.

- Network Validation, validate protocol compliance, traffic handling and interoperability.

- Applications and Network Security Test, validate performance of network and devices against security attacks and malwares.

5.7.2.2 Conclusion

The paper provides various requirements related to the emergency communication using IoT devices. These requirements need to be taken into account during the development of the present document. The paper shows that designers, networks operators and service providers alike need to take a pro-active approach in each segment of the ecosystem to ensure the challenges they face are dealt with. The innovation of emergency communications with IoT requires test and measurements to achieve a reliable, robust and secure foundation of device functionality, wireless communication and network infrastructure.

5.7.3 Experiments and Simulations

5.7.3.1 NIST disaster simulation (Philadelphia, USA)

In the case of a disaster, government and non-government agencies responsible for disaster relief are often unprepared for the task. They have to deal with many issues ranging from locating survivors to getting them the necessary aid. In such cases, and depending on the disaster nature, ICT may not operate as it should making the disaster relief operations vulnerable to failure.

During the planned demolition of the Veterans Stadium in Philadelphia, the National Institute Standards and Technology (NIST) seized the opportunity to conduct a large-scale simulation with the help of the authorities. The team chose to study the propagation and detection of radio signals before, during, and after the implosion. They anticipate that the data collected though the study will help develop better communication systems and technologies for disaster recovery efforts. NIST have made publicly available all the reports [i.49].

5.7.3.2 Disaster-ready communication infrastructure (Coral Gables, Florida, USA)

Poor interagency communication during emergency response and recovery operations can have disastrous consequences for a city and its residents. Coral Gables (a city in Florida) officials have learned through experience that they could not depend solely on a terrestrial communication infrastructure due to the destructive nature of tropical storms and hurricanes. Such events can uproot wireless base stations, disconnect vital communication cables, and flood central offices. The old system offered a limited degree of redundancy and lacked interoperability between public safety agencies.

In September 2017, the new system was put under test when Hurricane Irma lashed the city, with many downed power lines, trees and traffic lights. Because of the resilience of the new infrastructure based on IEEE 802 protocols, the system survived the storm and was able to provide digital services and communications to emergency responders during and after the hurricane. The new system developed by the city IT team uses a combination of redundancy layers to ensure uptime and availability [i.50].

6 Use cases for emergency services involving communications with IoT devices

6.1 Introduction

Based on the analysis of existing material and specifications, an exemplary set of use cases has been derived which are described in the following sub-clauses. In clause 7, recommendations for requirements to update existing standards documents, or to create new standards documents, are derived from the analysis of these use cases and identification of potential means to prevent points of failure identified in the present clause 6.

All use cases are described using the same template and with the objective to keep consistency between the different descriptions. First is indicated to which emergency domain, as described in Clause 4, the use case belongs. This is followed by a high-level description of the use case, illustrated by a few examples from real life. The actors involved in the use case are described based on the list found in Table 2 and highlighting potential specificities they may have in the corresponding situation. The flow of the use case is presented, separating the pre-conditions (status before the emergency situation), the use case normal flow which explains the processing of the IoT data, and the post-conditions (status after the emergency has been processed). When relevant, an alternative flow is also described. A high-level illustration shows a possible configuration and the flow of the use case. It should be noted that these pictures are for illustration only and other configurations are possible.

Following its description, each use case is analysed, especially considering possible points of failure in the overall flow that would put safety at risk during the emergency situation. This analysis has been performed in a systematic manner, using the knowledge areas defined in ETSI TR 103 375 [i.7], with availability of data, reliability and quality as additional topics. The analysis for each use case in this clause concludes with the identification of potential means which could help prevent these failures.

To help ensure consistency between descriptions, some common aspects have been recognized in the use cases, especially related to the actors involved and to the pre-conditions which describe the situation and status of the actors involved before the emergency arises.

Three pre-conditions have been identified which are common to all use cases:

- The communication networks and services they provide are deployed and operational.
- The emergency services are established and functional.
- The IoT devices and IoT service platforms are deployed and in operational condition.

The actors involved in the different use cases are illustrated in Figure 7 and presented in Table 2.

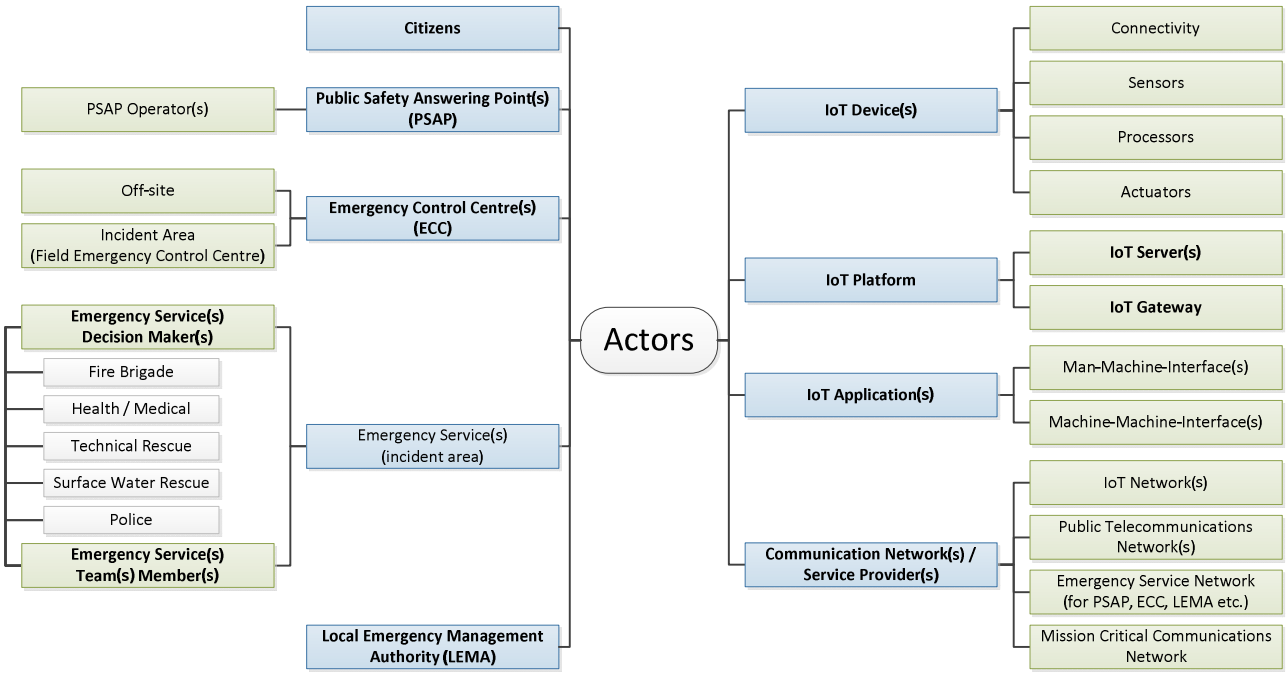
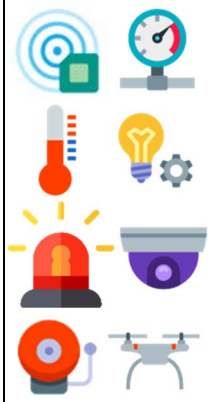
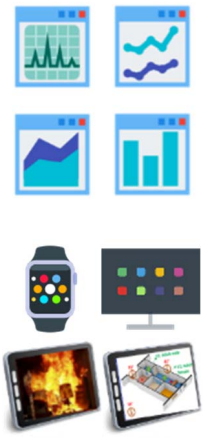
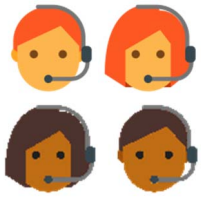


Figure 7: Illustration of the actors involved in the use cases

Table 2: Actors involved in the use cases

Actor	Illustration icon	Presentation
Citizens		Any individual (resident, visitor, passer-by), present in the vicinity of an emergency situation (from the first notice till the complete clearance) and subject to be affected by it, but who has no identified role in the actions of rescue and of restoration of normal conditions. (Source ETSI TS 102 181 [i.1].)
Emergency Services team members		Members of an emergency mission in or near the incident area. Examples include fire crew, police officers, technical and medical staff, etc.
Emergency Services decision maker		An emergency service team member who is managing, coordinating and is responsible for the other members of the team.
Emergency Control Centre (off-site)		ECC: - Facilities required for emergency handling. - Often co-located with PSAP. ECC dispatcher: - Responsible for incident handling in answer to an emergency call and for dispatching of available resources. - Able to analyse received COP data (partly based on IoT data). - Able to take decisions based on COP data. - Able to contribute to COP data.
PSAP		PSAP: - Facilities required for emergency call handling. - Often co-located with ECC. - May be able to differentiate between an emergency call and other types of incoming emergency communications, e.g. voice, data. - May be able to internally route incoming emergency communications differently based on communication type. - Notifies the PSAP operator of incoming emergency communications and make them accessible to the PSAP operator. PSAP operator: - May be human or AI. - Able to analyse received emergency communications. - Able to determine appropriate emergency responder and to share received communication with said responder.

Actor	Illustration icon	Presentation
Local Emergency Management Authority (LEMA)		Local organization within the public services fully or partly responsible for emergency preparedness and handling of incidents (Source: ETSI TS 103 260-2 [i.46]): - Responsible both for emergency preparedness and for the overall command, coordination, and management of response operations; interface to national government. - Able to trigger the sending of a PWS message. - Able to analyse received COP data (partly based on IoT data). - Able to take decisions based on COP data. - Able to contribute to COP data.
IoT device		A non-conventional (i.e. not a computer, server, tablet, or a smartphone. For example, a micro-controller-based embedded systems) and most often resources-limited computing device which includes one or multiple sensors and actuators to interact with its deployment environment. It has communication capabilities through wired or wireless networks. It may operate on batteries. An IoT device is responsible for: - Sensing data for the deployment environment. - Processing raw data and eventually analysing data. - Transmitting data (reports, alerts, etc.). - Receiving commands from remote entities. - Executing the received commands.
IoT server		A computing server hosting the necessary software to: - Store the data collected by the IoT devices. - Analyse the received the data. - Act as a contact point and to expose services for IoT applications. - Control other IoT entities (devices and gateways). The IoT server is typically a high-volume server and is hosted most often on the Cloud.
IoT gateway		A computing device that connects multiple IoT devices to an IoT server or another (high-level) IoT gateway. An IoT gateway may have specific network interfaces (such as ZigBee, Z-Wave, etc.) in order to communicate with the IoT devices. Most often, the IoT gateway is connected to the IoT server(s) through an IP network.
IoT service platform		The set of IoT servers and gateways deployed by an IoT services platform provider that acts as a service layer between the IoT devices and the IoT applications. The composition of the IoT service platform may range from one single IoT server and one single IoT gateway to multiple IoT servers and multiple IoT gateways hierarchically organized.
IoT application		A software application that interacts through a specific API with an IoT service platform in order to access data generated by the IoT devices or to trigger actions on the IoT devices. These applications can be empowered by artificial intelligence/machine learning techniques. IoT application can be autonomous and run as background processes or can have a Man-Machine Interface (MMI) to interact with its users. The goal of this interaction is to allow effective operation and control of the machine/system from the human end, whilst the machine/system simultaneously feeds back information that aids the operators' decision-making process.

Actor	Illustration icon	Presentation
IoT service platform operator		- May be human or AI. - Able to look at the data from IoT device and determine whether there is an emergency. - Able to make an emergency call and to decide when to include additional data from the start, after a delay, on in response to a request from the answering PSAP.
Communication network/service provider		The networked elements required for routing messages from connected IoT devices to other connected users and machines. May comprise: - **IoT networks**: private or public Communication networks able to connect one or more IoT devices to a remote IoT service platform. - **Public telecommunications networks**: capable of routing calls between subscribers of the same network, or between subscribers and gateways connected to other types of communication networks; able to distinguish between emergency and standard calls, and to route emergency calls with high priority to the Emergency Service network. - **Emergency Services networks**: communication networks connecting one or more PSAP networks for conveying emergency service calls and for enabling collaboration between PSAPs and other functional units in emergency services; may be a public network e.g. the Public Switched Telephone Network or a private Emergency Service IP network (ESInet) capable of handling multimedia telephony calls. - **Critical Communications networks**: private communications networks that connects the Emergency Control Centre with emergency responders in the field; may be implemented as a Private Mobile Radio network (PMR) operating in dedicated spectrum, and/or an overlay of a public communication network providing priority to subscribers.

An overview of an IoT service platform and its composing entities is depicted in Figure 8. The different entities are described in Table 2.

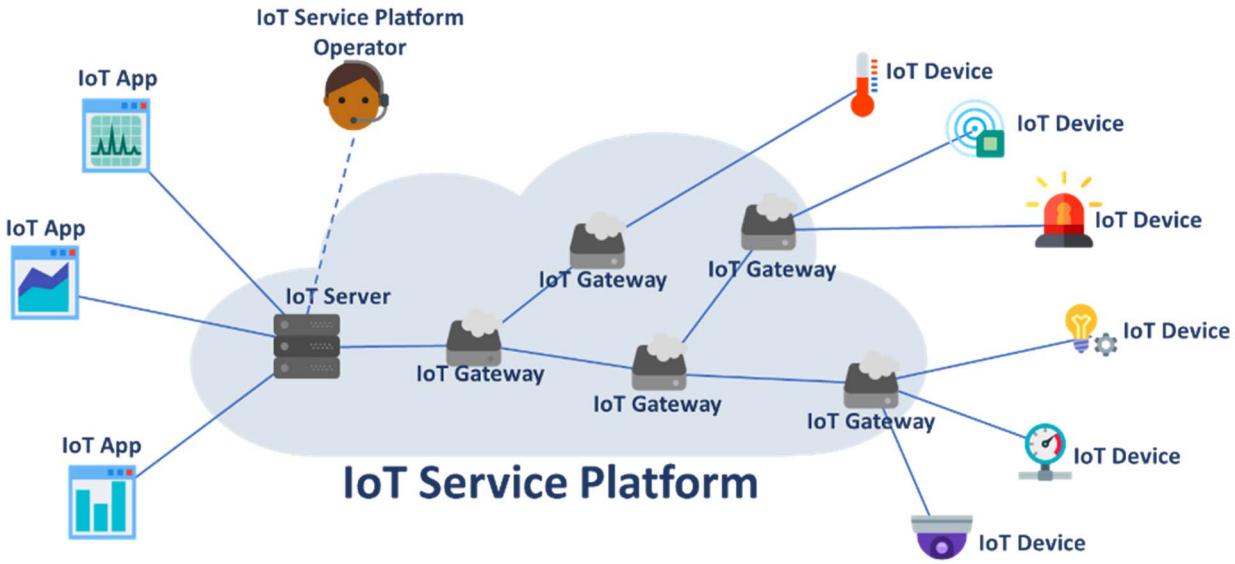


Figure 8: Overview of an IoT service platform bridging IoT applications and IoT devices

6.2 EC1: Automatic direct emergency call from IoT device

6.2.1 Emergency Domain

This use case applies to the emergency domain: Emergency calling.

6.2.2 Description

The following use case could apply e.g. in the case of a smoke detector in a remote location (forest, remote facility, etc.) sending an emergency message in the event of a fire, or in the case of Alternative flow 2 providing real-time emergency video.

The IoT device initiates an emergency data call automatically and directly to the PSAP on detecting an emergency event. The IoT device monitors the local environment, determines that there is an emergency, and creates an emergency message. The IoT device interacts with the communications network to establish an emergency call and sends the emergency message. The communications network routes the emergency call with priority to the most appropriate PSAP (i.e. one that supports emergency data and/or video). The PSAP recognizes that the call is an emergency data call and processes the message accordingly. The PSAP operator reviews the received message and contacts the appropriate emergency responders, making the contents of the emergency message available to the emergency control centre. The emergency control centre dispatches the emergency responders to manage the emergency.

6.2.3 Actors

The IoT device: May comprise one or more sensors, one or more processors, and potentially (for the present use case) one or more network interfaces. The sensor measures environmental parameters to detect specific operational conditions. The processor compares measured values with specified values and creates emergency data messages as required. The network interface transmits emergency data messages via the communication network to emergency authorities.

The communications network: The communication network comprises the Public telecommunications network and the Emergency Service network. The Public telecommunications network routes the call between the IoT device and the Emergency Service network. The Emergency Service network routes emergency data messages to a PSAP. The Emergency Service network may be a circuit switched telephone network or an ESInet capable of handling multimedia telephony calls.

The PSAP: The PSAP provides facilities for emergency call handling. The PSAP can differentiate between an emergency data message and standard emergency call. It may route an incoming emergency data message differently to a standard emergency call depending on the architecture of PSAP.

The PSAP operator: The PSAP operator that handles data messages may be human or a machine (AI). The PSAP operator analyses received emergency messages and contacts appropriate Emergency Control Centre (ECC) based on received emergency messages, sharing the contents of said messages.

The Emergency Control Centre (ECC): E.g. for police, fire fighters, ambulance, etc. The ECC manages reported emergencies, dispatching emergency responders to deal with said emergencies as required.

6.2.4 Pre-conditions

The following conditions exist in addition to the common pre-conditions of clause 6.1:

- The IoT device is capable of making a direct emergency data call.
- The IoT device is armed (emergency calling is enabled).

6.2.5 Triggers

The IoT device detects parameters levels that constitute an emergency event according to its normal configuration.

6.2.6 Normal Flow

In the normal flow, the emergency data is conveyed as a one-shot message between the IoT device and the PSAP. This flow assumes that the Public telecommunications network supports VoIP calling and that an ESInet has been deployed. If additional data needs to be sent, then the IoT device creates another emergency data message and initiates another emergency call to send it:

1) The IoT device detects an emergency event. It creates and emergency data message and packages that for delivery via the communications network. The IoT device initiates an emergency data call and passes the emergency message to the communications network.

2) The Public telecommunications network of the communications network recognizes the call as an emergency data call. It sends it with appropriate priority to the ESInet. The ESInet selects the most suitable PSAP (which may be selected based on proximity to and jurisdiction over the vicinity of the emergency) and routes to the PSAP the emergency data call.

3) The PSAP receives the emergency data call, recognizes it as emergency data and routes it to an appropriate PSAP operator.

4) The PSAP operator retrieves and analyses the message and contacts the Emergency Control Centre.

5) The Emergency Control Centre analyses the emergency message then dispatches suitable resources to manage the emergency.

6) Depending on its configuration, the IoT device may initiate emergency calls to send further emergency data messages to update the situation.

6.2.7 Alternative flow

Alt. 1. The IoT device creates an emergency message as per the normal flow. In this case, the PSAP operator and/or emergency responder is/are able to contact the IoT device and pull further data from it to inform handling of the emergency situation

Alt. 2. The IoT device establishes an emergency data session rather than sending a one-shot 112 data message. In this case, the session remains ongoing with the PSAP and/or connected to the emergency control centre, until it is ended by the PSAP or emergency control. During the session, real time data including video may be sent end to end by the IoT device.

Alt. 3. The IoT device is connected to a circuit switched telephone network. The IoT devices makes an emergency call sending an automated voice message. The data or an URL pointing to the data, is sent in a text message accompanying the automated voice call. E.g. similar to Advanced Mobile Location (AML) in ETSI TR 103 393 [i.77].

Alt. 4. The IoT device creates an emergency message as per the normal flow. In this case, the IoT device details are provided to the emergency responders who make direct contact with the IoT device on site to have immediate direct access to the device's data. This is covered by use case MC3 in clause 6.6.

6.2.8 Post-conditions

The emergency has been dealt with by the appropriate authorities aided by data from the IoT device. The IoT device is reset, tested for correct operation, and resumes monitoring. The full course of actions has been documented and fed back to optimize future operations.

6.2.9 High Level Illustration

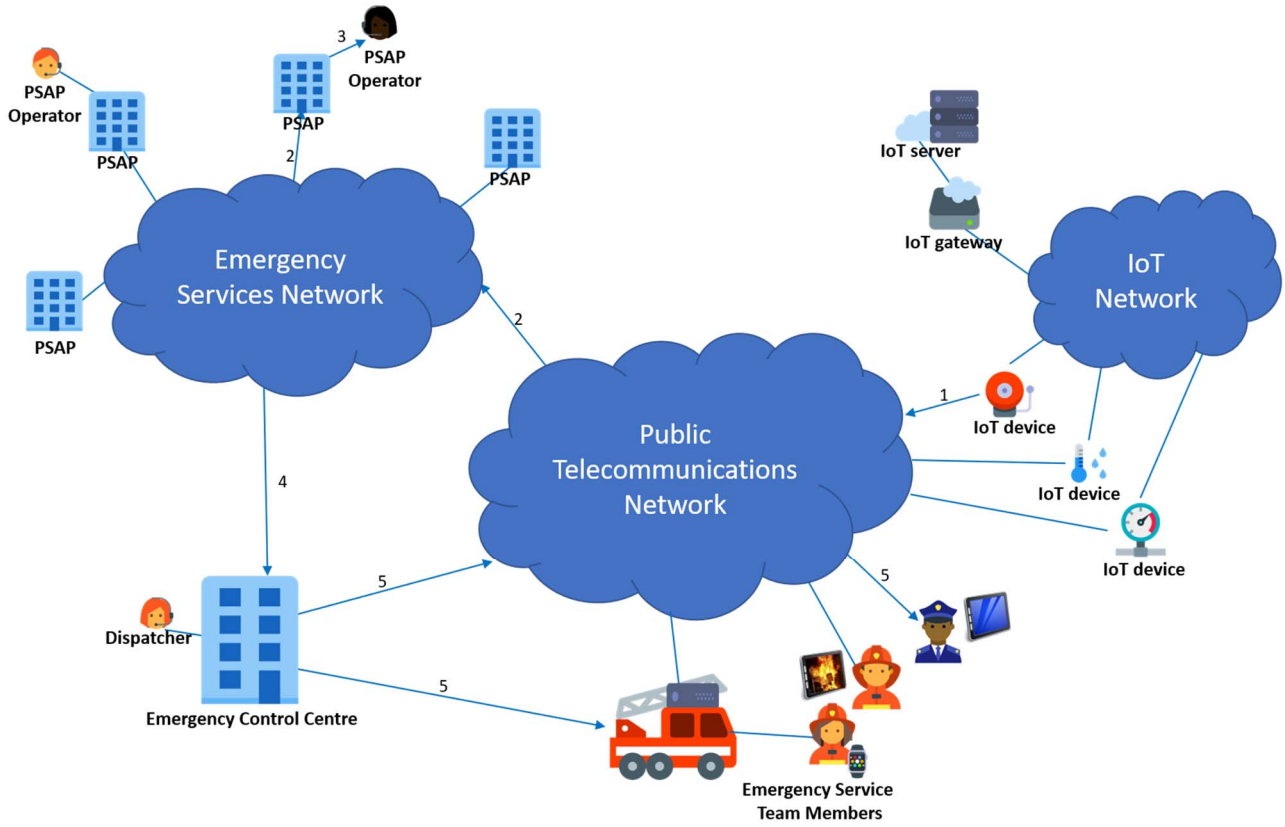


Figure 9: Illustration of automatic direct emergency call from IoT device

6.2.10 Potential points of failure putting safety at risk

- IoT device failure, e.g. battery failure, physical damage.
- Call failure due to network failure and/or congestion.
- Call failure due to protocol incompatibility between IoT device and communication network.
- Call failure due to improper configuration of the IoT device.
- Call failure due to improper PSAP selection, e.g. if the emergency data message is routed to a PSAP that does not support the emergency message feature.
- Call failure because the emergency data call has not been given sufficient priority by the network or at the PSAP, e.g. due to higher priority given to a human initiated emergency call.
- System failure due to IoT device not being emergency enabled as per pre-conditions.
- False alarm call due to IoT device being hacked, this could result in Denial of Service type attacks.
- False alarm call due to IoT device being faulty.
- False alarm call due to unforeseen circumstances, e.g. interpreting unusual environmental parameters as constituting an emergency, this may require some redundancy to determine the veracity of an emergency data message and prevent a large number of false positives from many IoT devices.
- Redundant alarm indication, e.g. due to detection by multiple IoT devices, or a single IoT device sending repeated emergency message.
- System failure due to IoT device data not being decodable/understood.

6.2.11 Potential means to prevent points of failure

- If enabled, IoT devices should be able to support emergency calling as standardized for existing Public Telecommunication Networks.
- If enabled, IoT devices should support the sending of emergency data.
- Public Telecommunications Networks should support emergency data.
- Public Telecommunications networks should route emergency data messages from IoT devices with appropriate priority.
- The PSAP should treat incoming emergency data messages from IoT devices with appropriate priority.

NOTE 1: The relative priority afforded to human versus IoT device-initiated calls is a deployment issue which could be subject to local regulation.

- ESInets should support emergency data from IoT devices.
- ESInets should route the emergency data messages from IoT devices to the most appropriate PSAP, i.e. one that supports emergency data messages, and has jurisdiction over the vicinity of the emergency.
- It should be possible to enable/disabled emergency call features in IoT devices.
- Remote triggering of an emergency call from an IoT device should be prevented other than via its sensor (i.e. no possibility to hack the device and place and emergency call, calls only triggered as a result of processed sensor information).
- The IoT platform should be able to determine the veracity of an alarm indication.

NOTE 2: How to validate an alarm, e.g. through human intervention or through automated means (e.g. data fusion and/or Artificial Intelligence), is a deployment issue beyond the scope of the present document.

NOTE 3: False alarms potentially caused by faulty devices may be prevented by introducing redundancy in the deployment of sensors. It should be possible to prevent an IoT device from sending repeat or redundant emergency data messages.

- PSAPs/ECCs should support the reception of emergency data from IoT devices (no Callback).
- IoT device supporting emergency data should be able to report potential failure conditions (low battery, etc.).
- IoT device supporting emergency data should be remotely manageable.
- A supporting IoT service platform should monitor the status of the IoT device supporting emergency data.
- The configuration of the IoT device supporting emergency data should be properly tested before the start of its operation.

6.3 EC2: IoT device provides additional information to an emergency call

6.3.1 Emergency Domain

This use case applies to the emergency domain: Emergency calling.

6.3.2 Description

The following use case could apply e.g. in the case of a temperature/smoke detector in a remote location (forest, remote facility, etc.) sending an emergency message in the event of a fire.

An emergency call may be initiated by an IoT service platform operator based on detection of an emergency by an IoT device or based on detection of an emergency by the IoT service platform operator herself having viewed information made available by one or more IoT devices. The IoT service platform operator will initiate an emergency call with the communication network. Additional data received from the IoT device may be attached to the call to provide more details of the emergency. This may be done in a way similar to that used for Advanced Mobile Location (AML) for emergency calls (see ETSI TR 103 393 [i.77]). The communication network routes the emergency call with priority to the most appropriate PSAP (i.e. one that supports emergency data and/or video). The PSAP operator answers the emergency call and receives details of the emergency from the caller. The data may be included by default, the emergency caller may offer that there is additional data available, or the PSAP operator may ask if additional data is available. The emergency data from the IoT device may be included in the call from the start or added during the call. When the emergency data arrives, it is reviewed by the PSAP operator. Based on the information from the IoT service platform operator and the IoT device, the PSAP operator contacts the appropriate emergency responders, also sharing with them the emergency data from the IoT device. The Emergency Control Centre dispatches the emergency responders to manage the emergency.

NOTE: The scenario in which an emergency call is made by a citizen who is unaware of the presence of an IoT device that could provide additional data is not within scope of this use case.

6.3.3 Actors

The IoT device: The IoT device may comprise one or more sensors, one or more processors, and potentially even one or more network interfaces. The sensor measures environmental parameters to detect specific operational conditions. The processor takes the measure values and organizes them to provide meaningful data in an operational context. The network interface transmits the data to an IoT service platform operator.

The communications network: The communication network comprises the IoT network, the Public telecommunications network, and the Emergency Service network. The IoT network routes the operational data from IoT devices to an IoT service platform operator. The Public telecommunications network routes the call between the IoT service platform operator and the Emergency Service network. The Emergency Service network routes an emergency call to a PSAP. The Emergency Service network may be a circuit switched telephone network or an IP network (ESInet) capable of handling multimedia telephony calls.

The IoT service platform operator: The IoT service platform operator that processes IoT device communications may be human or a machine (AI). The IoT service platform operator determines whether an emergency has occurred and initiates emergency calls.

The PSAP: The PSAP provides facilities for emergency call handling. It notifies the PSAP operator of emergency calls and makes them accessible for answering.

The PSAP operator: The PSAP operator that handles data messages may be human or a machine (AI). The PSAP operator answer the emergency call, assesses the emergency and contacts appropriate emergency responders based on requirements of the caller and any data provided.

The Emergency Control Centre: E.g. for police, fire fighters, ambulance, etc. the ECC manages reported emergencies, dispatching emergency responders to deal with said emergencies as required.

6.3.4 Pre-conditions

The following condition exists in addition to the common pre-conditions of clause 6.1:

- The IoT service platform operator is able to add data from IoT devices to a call, either from the start of the call or at any time during the call.

6.3.5 Triggers

The IoT service platform operator detects parameters levels from the IoT device that constitute an emergency event.

6.3.6 Normal Flow

In the normal flow, the emergency call is made and emergency data from one or more IoT devices is added by the monitoring operator during the call. This flow assumes that the Public telecommunications network supports VoIP calling and that an ESInet has been deployed:

1) The IoT device sends operational data to the IoT service platform operator either via the IoT network. The data may be flagged as emergency data or not.

2) The IoT service platform operator determines based on the operational data that an emergency is occurring. The IoT service platform operator makes an emergency call.

3) The Public telecommunications network recognizes the call as an emergency call. It sends it with appropriate priority to the ESInet. The ESInet selects the most suitable PSAP (which may be selected based on proximity to and jurisdiction over the vicinity of the emergency) and routes to the PSAP the emergency call.

4) The PSAP operator answers the emergency data call. The IoT service platform operator offers the additional IoT device data or the PSAP operator asks if additional data is available. If agreed by both parties, the IoT service platform operator adds the IoT device data to the emergency call. The PSAP operator views the emergency data. The PSAP operator contacts the ECC and shares the additional data with it.

5) The ECC analyses the available data from the IoT device and dispatches suitable resources to manage the emergency.

6.3.7 Alternative flow

Alt. 1. The flow is as per the normal flow except, the monitoring operator initiates an emergency call that includes from the IoT device data automatically from the start. In this case, the call may be initiated by a machine IoT service platform operator comprising a pre-recorded message that indicates the presence of emergency data.

Alt. 2. The flow is as per the normal flow except, the IoT device creates an emergency message as per EC1, and the operator sends that message separately as soon as the emergency session is established. In this case, the call may be initiated by a machine IoT service platform operator comprising a pre-recorded message that indicates the presence of emergency data.

Alt. 3. The monitoring operator is connected to a circuit switched telephone network. The operator makes an emergency call and the data or an URL pointing to the data is sent in a text message, accompanying the call in a similar way to that for AML as per ETSI TR 103 393 [i.77]. In this case, the call may be initiated by a machine IoT service platform operator comprising a pre-recorded message that indicates the presence of emergency data.

Alt. 4. The IoT service platform operator provides emergency data as per the normal flow. In this case, the IoT device details are provided to the emergency control centre which makes direct contact with the IoT device on site to have immediate direct access to the device's data.

6.3.8 Post-conditions

The emergency is dealt with by the appropriate authorities aided by data from the IoT device. The IoT device is reset, tested for correct operation, and the operator resumes monitoring.

6.3.9 High Level Illustration

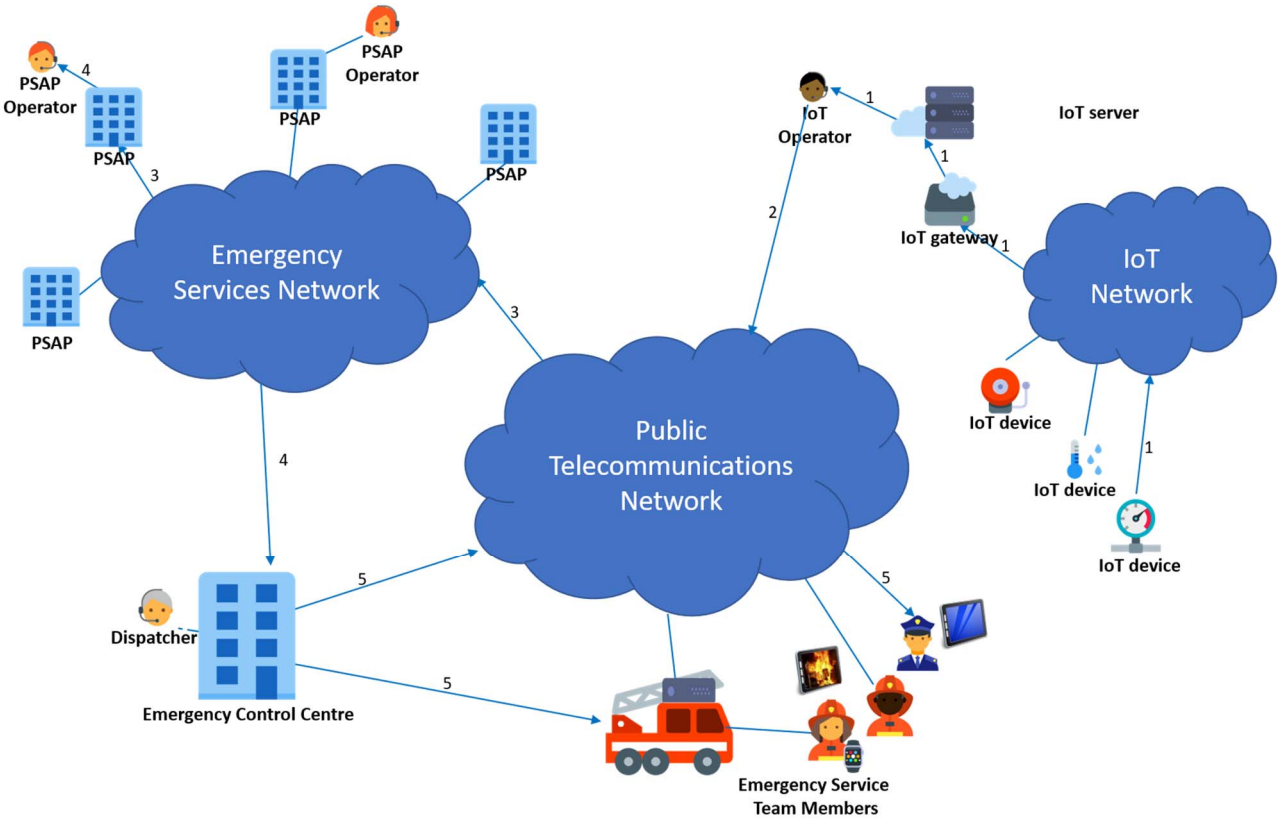


Figure 10: Illustration of the "IoT device provides additional information to an emergency call" use case

6.3.10 Potential points of failure putting safety at risk

- IoT network failure.
- IoT network congestion.
- IoT service platform failure.
- System failure due to inability to add data to call.
- IoT network has insufficient QoS and/or capacity to support the emergency data.
- IoT device failure or improper configuration.
- IoT device emergency data not being decodable/understood.
- IoT device emergency data are inaccurate.
- IoT device emergency data content is unclear.

6.3.11 Potential means to prevent points of failure

- IoT networks should support priority routing of emergency notifications.
- An IoT service platform operator should be able to add data from the start of, or during an ongoing, an emergency session.
- IoT network should provide sufficient QoS and capacity to support the emergency data.

- IoT device emergency data should be in a format that is understandable by the PSAP platform.
- IoT device emergency data should be accurate and reliable.
- IoT device emergency data should be clear and unambiguous.

6.4 MC1: IoT-based mission critical communications

6.4.1 Emergency Domain

This use case applies to emergency domain "mission critical communications".

6.4.2 Description

IoT allows (near) real-time data gathering without human interaction. This is especially important in situations where emergency service team members are busy with critical tasks and additional reporting (e.g. via voice-based radio systems) to the team officer would cause unwanted distraction or delay.

For example, smart clothing, equipped with sensors, can report in real time vital signs and temperature of firefighters involved in hazardous situations. A rescue team officer can thus warn when the situation gets too hazardous or intervene to rescue the firefighter in trouble. Such information can be used to alert other team members in real-time in order to act more carefully.

Another example is emergency service personnel equipped with wearables such as audio and video sensors or supported by a drone. The real-time audio and video transmissions can be used by other team members or the emergency control centre in order to collect more data to assess the situation.

The use case will show how IoT devices can be used in emergency situations in general and for mission critical communications in particular.

6.4.3 Actors

- **Emergency control centre:** manages an emergency mission and coordinates emergency services teams. May be located on-site (field emergency control centre) or off-site with regard to the incident area.
- **IoT service platform:** acts as a middleware between the emergency control centre and the IoT devices. It is responsible for storing and analysing data, managing data subscriptions, notifications, etc.
- **IoT gateway:** A network equipment that is acting as a bridge between the local IoT network and connected to remote IoT server(s) through a wide area network. The IoT gateway can be implemented as part of a handheld device (e.g. cellular transmitter, smartphone, etc.), or mounted on a vehicle (e.g. ambulance, police vehicle, etc.). Data processing tasks of the IoT gateway can be (if needed) offloaded to a nearby Edge Computing nodes (e.g. micro data centres operated by telco operators and placed near cellular base stations).
- **IoT device:** senses, analyses the measured data and transmits it back to the IoT service platform. It is connected to an IoT gateway.
- **Communications networks:**
  - **Emergency service communication network:** a dedicated network to emergency services that may connect the emergency control centre to the IoT service platform.
  - **Critical communication network:** a telecommunication network for routing data flows to the appropriate destination with the ability to differentiate and to prioritize emergency traffic from regular traffic. It is used to connect some IoT devices to the IoT service platform. It is also connecting the emergency control centre to the IoT service platform.
  - **IoT network:** a communication network dedicated to connect some IoT devices; For example, Long Range Low Power IoT networks (Sigfox, LoRaWAN, etc.).

- **Emergency services team member:** Member of an emergency team with an identified role in the actions of rescue and of restoration of normal conditions equipped with IoT devices (e.g. wearables).
- **Emergency services decision maker:** A team officer of an emergency team with responsibility for the team and a legal mandate to take decisions.

6.4.4 Pre-conditions

The general pre-conditions as listed in clause 6.1 are fulfilled.

6.4.5 Triggers

The beginning of the emergency mission.

6.4.6 Normal Flow

1) The emergency service team member starts an emergency mission and activates his/her IoT devices.
2) As the emergency service team members move within the emergency field, the IoT devices continuously send real-time measured data to the IoT service platform through the IoT gateway. This communication goes through the dedicated IoT network. The communication between the IoT gateway and the rest of the IoT service platform will go through the critical communication network or through an emergency service network.
3) The emergency service team decision maker at the emergency control centre receives notifications from the IoT service platform.
4) The received data (from the different sources) at the emergency control centre is used to automatically build an enhanced view of the incident area and to be presented to the emergency service team decision maker. Artificial intelligence and data fusion may be used in that step.
5) The automatically generated data (e.g. by AI) as well as the data that the emergency service team decision maker at the emergency control centre decides to communicate is published on the IoT service platform. Examples include a map with meta information such as temperature values in all parts of the building, location and number of emergency responders or victims, etc. Relying on a "Publish/Subscribe" communication mechanism, all the entities (IoT applications/users) that have subscribed to this "topic" receive the newly published data.
6) Other emergency service team members that are subscribed to MCC services receive notifications from the IoT service platform. The received data is used to gain extra knowledge about the incident area, the other emergency responders, and the citizens that are outside the field of vision.
7) The emergency service team decision maker at the emergency control centre has a precise knowledge of the emergency situation and is updated in real-time. Thus, he/she can manage the emergency mission efficiently.
8) Emergency responders have a better view about the emergency situation while in the field and can carry out the emergency mission successfully.

6.4.7 Alternative flow

In case of networking issues between the IoT gateways deployed in the field and the remote IoT service platform, critical communications may occur locally between IoT devices connected to the same IoT gateway, or between closer IoT gateways. Edge Computing nodes located nearby the incident area can also be envisioned to host data processing tasks:

1) Emergency service team members connect and register automatically to proximity IoT gateways rather than to the remote IoT service platform.
2) Other emergency responders that are subscribed to the IoT service platform, on the proximity IoT gateway, receive notifications. The received data is used to gain a partial knowledge (covered by this IoT gateway) about the incident area, the other emergency responders, and the citizens that are outside the field of vision.

6.4.8 Post-conditions

The emergency situation has been handled efficiently thanks to the precise real-time view provided by the IoT devices to either local and remote emergency service team decision makers.

6.4.9 High Level Illustration

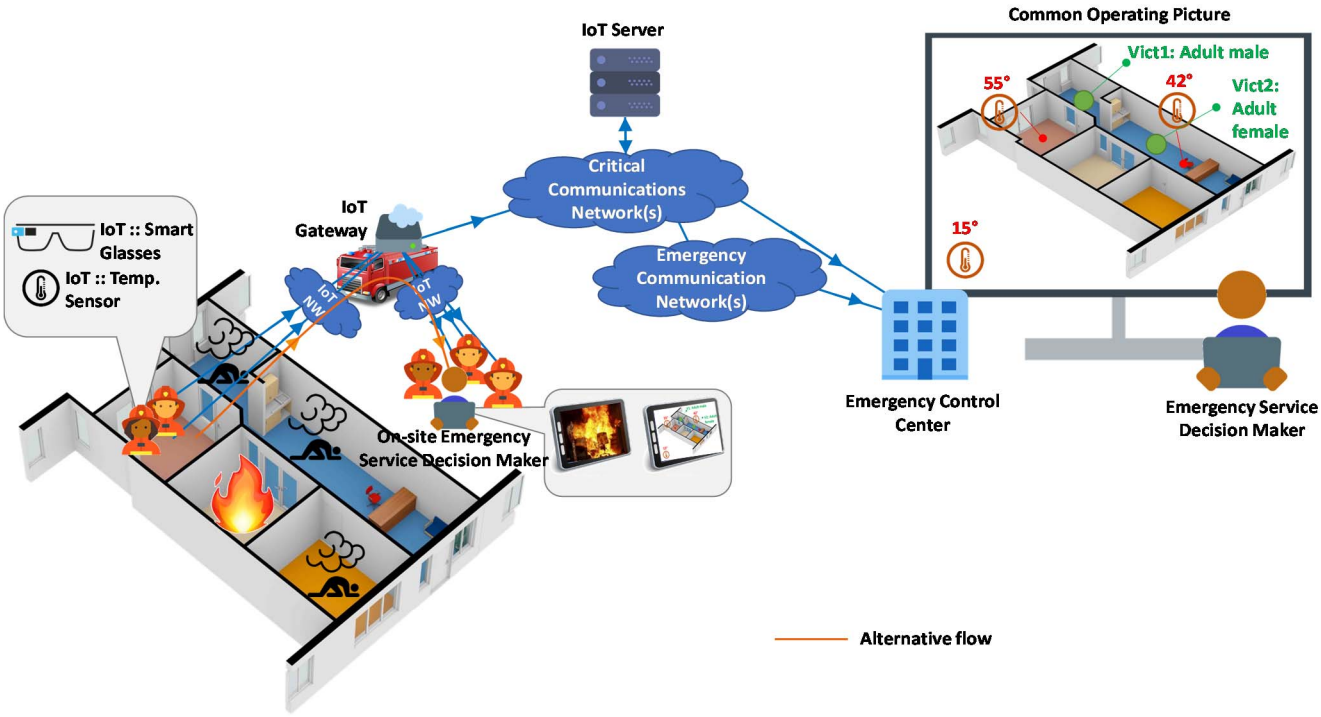


Figure 11: Illustration of "IoT-based mission critical communications" use case

6.4.10 Potential points of failure putting safety at risk

- IoT device failure: e.g. damaged during the emergency mission, battery failure, etc.
- Network congestion: communication networks are under congestion and cannot meet the required QoS anymore.
- Network coverage: in case of multi-hop communications, end-to-end connectivity may not be guaranteed.
- Data accuracy (i.e. precision and correctness of sensor data): IoT devices (sensors) provide inaccurate or false information. For example, a gas sensor did not provide accurate measures that would have led to abort the mission.
- Misconfiguration of IoT device.
- IoT device is not able to exchange data with applications, service platforms because they were produced by different providers (lack of interoperability).
- Communication between IoT device and IoT gateway is hacked.
- IoT device is not usable because it was not updated to the latest version of software.
- IoT device is not usable because its user is not able to authenticate.
- Different emergency services teams are not able to exchange information because their systems are incompatible.

6.4.11 Potential means to prevent points of failure

- Mechanism/techniques to assess data accuracy.
- Guaranteed QoS from the traversed communication networks and the IoT service platform.
- IoT service platform elements (e.g. IoT device, IoT gateway) should be interoperability tested inside and between different emergency services teams.
- IoT entities involved in MC communications should use interoperable protocols and data syntax.
- The IoT service platform should allow point-to-multipoint communications (e.g. from the IoT gateway to all connected IoT devices).
- IoT device communication is ensured (access control, authentication).
- End-to-end connectivity should always be available in case of multi-hop communications.
- A device management service (e.g. firmware update, battery state monitoring, etc.) should be ensured by the IoT service platform for all IoT devices and entities.
- Authentication and authorization to use an IoT device should be provided in a secured and simplified manner to the emergency services team members (e.g. by using an RFID-equipped card).

6.5 MC2: Mission critical logistics support

6.5.1 Emergency Domain

This use case applies to the emergency domain "mission critical communications".

6.5.2 Description

Decisions to be taken by the emergency management entities require a comprehensive situation overview which is known as Common Operating Picture (COP). Data contributing to the COP are typically gathered (see ETSI TS 103 260-2 [i.46]):

- either actively (scouting, polling of IoT sensors, demanding information from other hierarchy levels or other involved organizations, etc.); or
- are obtained passively (e.g. reports from affected citizens, notifications from IoT sensors).

Maintaining a COP and deriving decisions out of it (which will feed into the COP, too) consist of three main tasks:

- Collecting distributed data contributing to the COP from various sources via various communication channels.
- Aggregating distributed data:
  - Categorization (resources vs. demand, hazards, risks, environmental data, other information relevant for decision making).
  - Geo-referencing.
  - Trend analysis, forecasting (if possible).
- COP data distribution to and COP data synchronization between all involved decision makers and stakeholders plus visualization:
  - Timely transmission of important data.
  - Abstraction/visualization/presentation depending on decision makers' functions/roles.

NOTE: COP data transmission and synchronization should take place in near real time in order to allow a short-term prediction of movements (heading, speed). Position updates may be triggered by passed time or distance or other criteria (cell hand-over, emergency, etc.).

In general, both the incident itself and the incident response activities evolve over time, so that the COP has to keep pace with the situation, too:

- Evolving scenario in general (e.g. magnitude, effectiveness of mitigation measures, etc.).
- The emergency management structures evolve over time and adjust to the emergency response tasks. They will never be completely in place before any actual rescue works start.
- Roles of deployed personnel may change over time.
- Personnel and resources may enter (and leave) the scenario at any time. This includes IoT and communication devices.

Without loss of generalization the management of mass casualty incidents (MCI) serves as a use case example for logistics support (see ETSI TS 103 260-2 [i.46]).

6.5.3 Actors

Actor 1: IoT devices attached to affected citizens (casualty IDs, "triage tags")

Tasks:

- Provision of unique, machine-identifiable ID (casualty ID).
- Optional: monitoring of geographical position, monitoring of track along medical evacuation, CBRN sensor functionality, vital parameters, etc.
- Optional: local storage of data in triage tag relevant for treatment or documentation (e.g. medication, sensor data with time stamps, photos, etc.).

Actor 2: IoT devices attached to emergency service teams and equipment (personnel, vehicles, etc.)

Tasks:

- Provision of status and position to COP.

Actor 3: IoT devices deployed along medical evacuation scanning casualty IDs of affected citizens

Tasks:

- Automatic scanning of casualty IDs (triage tags) at Temporary Care Centre (TCC), transport vehicle(s), hospital(s), etc.
- Provision of affected citizens' data (IDs, position, time stamps, etc.) to COP.

Actor 4: IoT applications for emergency service(s) team(s) member(s)

Tasks:

- Scanning of casualty IDs.
- Optional: reading of locally stored data from triage tag.
- Linking of casualty-related data to casualty IDs (e.g. status, position, sensor data, photos, identity, audio files, videos, etc.).
- Optional: local storage of data in triage tag relevant for treatment or documentation (e.g. details of find spot, preliminary diagnosis, medication, sensor data with time stamps, photos, etc.).
- Provision of data to COP.
- Optional: storage of casualty-related data on casualty ID.

Actor 5: IoT applications for emergency service(s) decision maker(s)

Tasks:

- Visualization of COP data for:
  - Emergency Service(s) Decision Maker(s) (on-site and off-site).
  - Emergency Control Centre(s) (off-site).
  - Field Emergency Control Centre(s) (on-site).
  - LEMA.
  - Other stakeholders (e.g. hospitals).
- Mapping decisions (e.g. priority, transport vehicle, destination hospital, etc.) to casualty IDs.
- Provision of data to COP.

6.5.4 Pre-conditions

The following condition exist in addition to the common pre-conditions of clause 6.1:

- Registration of all affected citizens (casualties) with attached machine-identifiable IDs (actor 1) by emergency service(s) team(s) member(s) has started, is ongoing, or has been completed.

6.5.5 Triggers

The scenario starts with an event causing the mass casualty incident and an authorized person (typically an emergency services decision maker) entitled to state the existence of a mass casualty incident and to authorize related procedures.

Each casualty data update (registration, status, position, etc.) and each decision (priority, assigned transport vehicle, transport destination, etc.) feeds into the COP and triggers re-synchronizations of the COP to be visualised among all involved man-machine interfaces (IoT applications).

6.5.6 Normal Flow

1) Emergency service(s) team(s) member(s) assess and register affected citizens (casualties). The registration includes attaching IoT devices (IDs, triage tags) to the affected citizens. Affected citizens' data update the COP.

2) An authorized emergency services decision maker takes for each affected citizen the decision based on the overall COP (i.e. urgency of other patients, availability of transport vehicles, hospital treatment capacity, etc.), if immediate medical evacuation to hospital (which casualty with which transport vehicle to which hospital) or on-site treatment (e.g. at TCC) or transport to other destination. Decisions and casualties' data update the COP.

3) IoT devices attached to emergency service teams and equipment provide their status and position to the COP.

4) Emergency service(s) team(s) member(s) transport casualties. In transport vehicles and at destination update of casualties' data and update of COP.

6.5.7 Alternative flow

No alternative flow involving IoT devices.

6.5.8 Post-conditions

The full course of actions (i.e. the evolution of the COP over time) is available for lessons learnt and police investigations.

After CBRN incidents, routes of casualties and contacts with emergency service personnel can be traced.

6.5.9 High Level Illustration

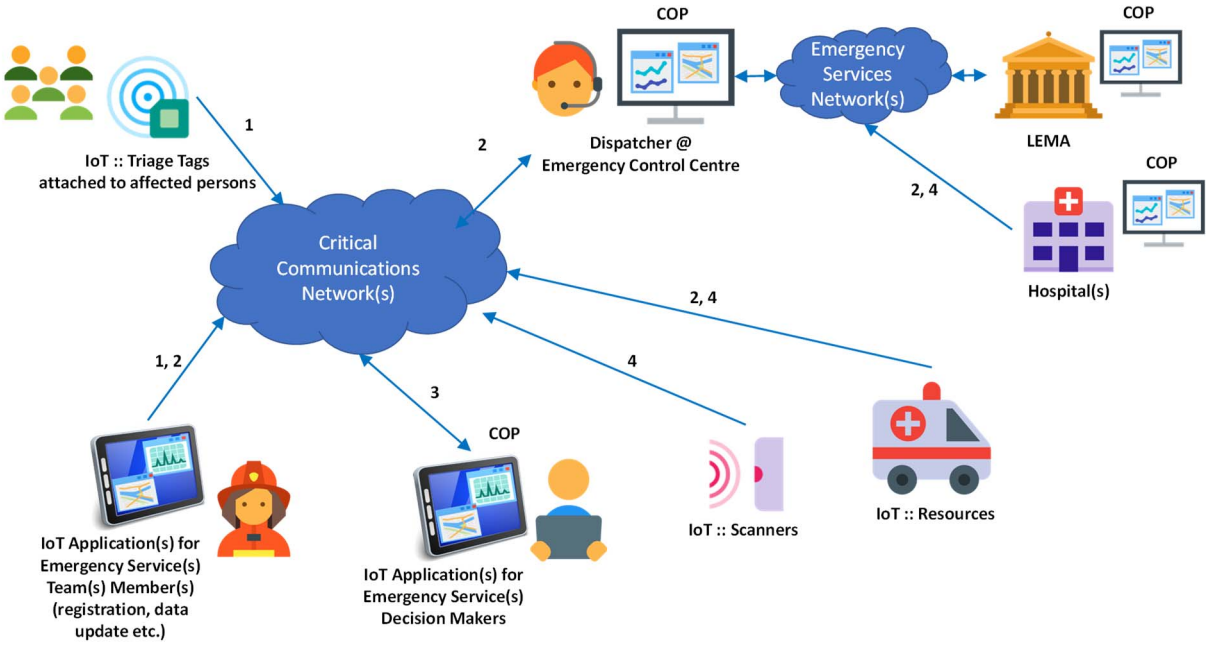


Figure 12: IoT-based management of a mass casualty incident with fully synchronized COP for involved decision makers

6.5.10 Potential points of failure putting safety at risk

- Services (data storage, etc.) may fail.
- All communication and IoT devices (and IoT servers) may enter and leave the scenario at any time.
- All communication and IoT devices (handhelds, scanners, routers, switches, etc.) may fail (especially in scenarios with electromagnetic pulses or with disposal of radioactivity).
- Communication networks may fail (coverage, intended or unintended jamming, etc.).
- Transmission of large amounts of (optional) secondary data (e.g. binary large objects like photos, videos, etc.) may lead to communication network saturation (i.e. key primary data cannot be exchanged).
- There are typical data transmission impairments:
  - Geographical (e.g. size of incident area, coverage of wireless networks).
  - Technical:
    - Link availability (e.g. utilization of wireless communication networks).
    - Availability of communication devices (defects, power outages, etc.).
    - Communications standards including authentication/encryption (e.g. protocols, data syntax and semantics, password management, etc.).
  - Inter-organizational (between different emergency service organizations without common level of hierarchy) and intra-organizational.
- Intentional denial-of-service attacks or jamming.
- Personal data from the COP may be disclosed in an unauthorised manner.

6.5.11 Potential means to prevent points of failure

- The full course of actions (i.e. the evolution of the COP over time) should be available during the incident and for lessons learnt after clearance of the situation (e.g. anonymized data) and police investigations (full access to documentation).
- IoT applications with man-machine-interfaces should provide intuitive man-machine-interfaces for the intended use and should support switching between role-specific man-machine-interfaces (since roles of deployed personnel may change over time. These applications should provide functionalities for daily tasks, too (e.g. emergency medical service documentation and billing).
- All devices should support remote maintenance (software updates, battery and function check, etc.). Software updates should be subject to a certification process.
- Usage of commercial off-the-shelf devices should be possible. Ideally, software should be provided as "stickware" without deep integration in an operating system. If there is a lack of devices this will allow using available third-party hardware.
- Casualty IDs (triage tags) should allow long term storage.
- All IoT devices to be used for mission critical applications should have passed some sort of "interoperability certification" to ensure that devices from different vendors can communicate with each other. This is especially important for large scale incidents requiring the supra-regional and/or cross-national co-ordination of emergency services.
- Syntax and semantics of data contributing to the COP should be standardized. This includes IoT data.
- Interfaces to a COP database should be standardized (ideally based on an open standard with a reference implementation). This is not limited to access for emergency services, but includes external agencies/authorities and social media, too.
- Data exchange should be based on commonly accepted standards for industry and home users. Proprietary solutions are not acceptable.
- The mission critical communications network should support (near) real-time:
  - Point-to-point data transfer.
  - Multi-point-to-point data transfer (e.g. aggregation of casualties' data, respiratory protective equipment data from team members is sent to team officer).
  - (Multi-)point-to-multi-point data transfer (e.g. synchronization of COP data).
  - Unidirectional point-to-point streaming (e.g. IoT device sensor data).
  - Bidirectional point-to-point streaming (e.g. video conferences, real-time telemedicine applications).
  - Multi-point-to-multi-point streaming (e.g. audio/video conference calls).
- The mission critical communications network capabilities should be fully scalable ranging from day-to-day rescue tasks to large scale disasters with potentially damaged infrastructure.
- Mission critical data communication should support both an infrastructure mode (via access points, "on-network") and an ad hoc mode (decentralised wireless network, "off-network").
- All network nodes (IoT devices, communication terminals, etc.) should discover access points (infrastructure mode) or other nodes in ad hoc mode automatically.
- The IoT devices (and communication terminals) should automatically switch between infrastructure mode and ad hoc mode.
- The ad hoc mode should support automatic routing and data transmission via multiple hops (i.e. more than one).

- All (IoT) devices and the network(s) should support time synchronization and should assign time stamps to data when/where appropriate.
- The COP database should support automatically generated and manual data updates. An emergency service decision maker should be able to manually override automatically generated COP data.
- COP data should be automatically synchronized among as many devices as possible ("synchronization composite"), especially in the incident area. New devices arriving at the incident area should automatically (i.e. with as little user interaction as possible) obtain the COP data.
- Physical transport of IoT devices (or simple data carriers) with locally stored data between disjunctive networks (i.e. between different isolated coverage zones) should allow automatic COP data synchronization.
- An emergency service decision maker should be able to merge COP data from two or more incidents.
- Both infrastructure and ad hoc modes should support different data transmission priority classes.
- IoT devices and IoT applications should be able to suggest priority classes to the network(s) for data to be transmitted (important primary data should be transported with priority in comparison to (optional) secondary data).
- IoT devices and IoT applications should buffer data locally during network outages until connectivity is regained. After re-establishing connectivity data should be automatically transferred without user interaction.
- Mission critical (IoT) data exchanges should have priority and pre-emption rights, especially when used on top of public communication networks.
- New devices to be integrated in the IoT/COP synchronization composite should mutually authenticate themselves against all other mission critical devices (or against the synchronization composite).
- IoT data (e.g. vital parameters) and COP data (e.g. patient data, names, diagnosis, addresses, etc.) confidentiality and integrity should be assured at any time. This requires a sound security architecture and a suitable but flexible authorization scheme for the different user functions and roles.
- The authorization scheme should allow mapping of role-specific equipment (which includes man-machine-interfaces and data access rights) to users with as little user interaction as possible. Ideally, authorization should require no user interaction at all.
- The design of the COP framework should enable privacy by design, respecting the GDPR regulation [i.91].

6.6 MC3: Emergency services teams accessing pre-deployed IoT devices

6.6.1 Emergency Domain

This use case applies to the emergency domain "mission critical communications".

6.6.2 Description

IoT devices are very often an integral part of buildings' safety concepts. Examples are smoke/heat detectors, surveillance cameras, but also communication devices in elevator cabins.

For firefighters there are dedicated access points to fire detection systems which allow identifying the origin of an alert. Unless there are control rooms (with personnel operating the technology) emergency services normally do not have access to other IoT devices like surveillance cameras, etc. pre-deployed in a building.

NOTE: The IoT devices in this use case belong to the building administration and management such that only the data they produce are shared on demand with the emergency services. Emergency services normally do not have access to these IoT devices. There is a potential conflict of configuration if two entities have management rights on the same device. This takes place at service/application layer level, and not at network and transport (e.g. MNO) level.

6.6.3 Actors

Actor 1: Emergency service(s) decision maker(s)

A representative of the emergency service with a mandate to access a building's safety system.

Actor 2: Communication network

The network providing connectivity with IoT devices.

Actor 3: IoT service platform

The IoT service platform includes an entity authenticating the emergency service officer and granting access to the safety system. This could be e.g. a remote control centre or an approach based on pre-shared keys. Furthermore, the IoT service platform handles data transport between IoT devices and subscribers (e.g. building managers and emergency services). It is under responsibility of the building manager (e.g. for its configuration and maintenance), but offers the capability to provide data to external bodies such as the emergency services.

Actor 4: IoT devices

Sensors/actuators pre-deployed in the building.

6.6.4 Pre-conditions

The following conditions exist in addition to the common pre-conditions of clause 6.1:

- An emergency in a private or public building or in an area with pre-deployed IoT-based safety systems has occurred.
- There are IoT devices in the building's safety system that can provide additional helpful information to emergency service teams.
- The emergency service team's devices are compatible to network and data provided by the building's safety system.

6.6.5 Triggers

The emergency service decision maker determines that he/she needs the additional information from the building's safety system.

6.6.6 Normal Flow

1) An emergency service decision maker asks the authenticating entity for access to a building's safety system.
2) The authenticating entity grants access.
3) The emergency service decision maker can obtain IoT devices data via the IoT service platform from the building's safety system.

6.6.7 Alternative flow

None available here.

6.6.8 Post-conditions

Termination of the data connection between emergency service team and building safety system.

6.6.9 High Level Illustration

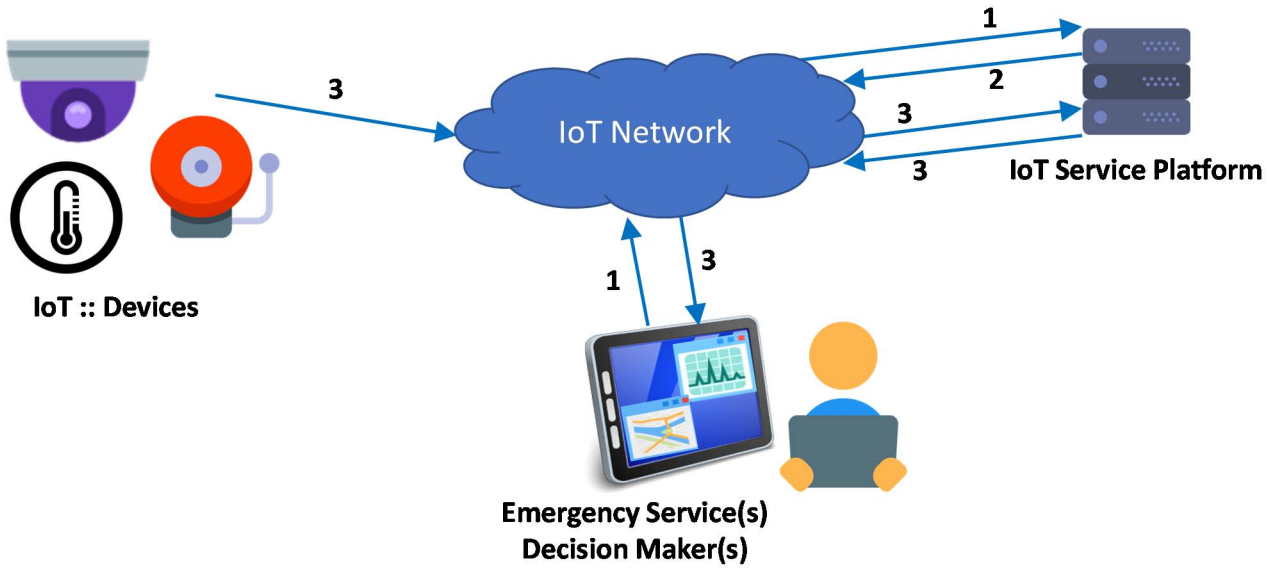


Figure 13: Illustration of an emergency service decision maker requesting access to pre-deployed IoT devices

6.6.10 Potential points of failure putting safety at risk

- Misuse by unauthorised persons.
- Emergency services are not able to obtain the IoT device data because the platforms are not interoperable.
- Emergency services are not able to obtain the IoT device data because the IoT service platform is not available (out of working hours if personnel are mandatory in the process, out of service, etc.).

6.6.11 Potential means to prevent points of failure

- The authentication protocol should be secure and standardized.
- The authentication process should require as little user interaction as possible.
- IoT devices and IoT service platform should mutually authenticate each other before activation.
- IoT devices should be able to trigger other IoT devices via the IoT service platform (e.g. smoke detector turns on camera).
- The emergency service decision maker(s) should be able to obtain IoT device data via the IoT service platform.
- IoT device data should be in a format (syntax and semantics) so as to be understandable by emergency service devices and applications.
- The IoT service platform should be able to manually or automatically adapt IoT device data rates (e.g. scaling of video camera resolution) to available network bandwidth.
- The IoT device data should directly feed into the COP.
- IoT device data should be of sufficient accuracy (i.e. precision and correctness of sensor data).
- IoT devices should be able to provide data on a 7/7 - 24-24 basis if required.

6.7 PWS1: warning sent via IoT device to citizens

6.7.1 Emergency Domain

This use case applies to Public Warning System domain.

6.7.2 Description

When a disaster occurs, the national or local authorities need to provide information to the citizens regarding the impact of the disaster including precautions that need to be taken by the citizens to increase their safety. The information provided by the authorities to the citizens is delivered to the area(s) where the incident happens, that can be limited to a small area(s) and up to the whole country. Means to ensure that the impacted citizens in the designated area are receiving the warning information can include IoT devices. These IoT devices are as described in clause 6.1, for example bus stop displays, displays inside the buses and connected cars, connected billboards/road displays, among others.

A communication network to securely transport the information from the authority centre to the citizens is needed. In case of using the Internet as a means to transfer the PWS information, the communication network needs to prevent spoofing of PWS information and also discover the authority centres, as described in ATOCA charter (see IETF-charter-ietf-atoca-01 [i.86]), that can verify authorization and deliver messages to the intended recipients. This is based on the mechanisms assuring that only those pre-authorized agents can send alerts via ATOCA, through an interface to authorized alert distribution networks. Communications networks may include Mobile Networks, fixed Broadband networks, TV/Radio broadcast, among others.

NOTE: Beyond the IETF ATOCA (Authority-to-Citizen Alert) charter, ATOCA system documentation has not been developed by IETF.

The communication network should be capable to ensure transport of the information efficiently and timely. Also handling of duplicated messages needs to be detected and deleted either in the communication network or the IoT/end device. Massive IoT devices could be connected to IoT service platforms that control these devices and convey the information to the citizens.

The information should be understood by all citizens, thus the ones with hearing and visual impairments should have the means to receive the information as well. Languages, in addition to the local language may be provided to the citizens in general or designated citizens.

The use case reflects how IoT devices are used to convey information provided by the authority to the citizens during emergency situations.

6.7.3 Actors

- **Local Emergency Management Authority (LEMA):** In case of PWS, it specifies the area/location where the information should be sent. The method for communicating the information as language, sound, light, etc. can be provided based on regulatory requirements.
- **Communication network/ service provider:** connecting the authority IoT server capable of transporting the public warning information instantaneously to the IoT devices in the designated areas, ensuring the information needed are up to date and in-line with the regulation and authority preferences, as well as compatibility with the connected communication network and IoT devices. It provides a reliable, consistent and secure means for transporting the information.
- **IoT service platform:** controls the IoT devices as well as distribute the right media to the corresponding IoT device. It is capable of detecting duplicated PWS messages and discarding them.
- **IoT device:** A stand-alone IoT device, or an integrated IoT device in another device, capable of receiving public warning information and presenting it to the citizens. It should be able to convey one or more types of media (text, voice, video, among others). These devices should be known by the IoT service platform via registering to the IoT service platform or to the communication network. The IoT device should be able to save the message for predefined time or action, repeat the message if instructed to and discover duplicated messages and discard them.

6.7.4 Pre-conditions

The following conditions exist in addition to the common pre-conditions of clause 6.1:

- A communication network, capable of transporting the public warning information to the right location, ensuring data integrity, connected to the authority public warning IoT server and to the IoT service Platform.
- IoT devices capable of receiving the public warning information and presenting it to the citizens via one or more supported media.

6.7.5 Triggers

- A disaster situation (earthquake, Tsunami, terror attack, etc.) where the authority needs to inform the citizens with information and instructions to increase their safety.

6.7.6 Normal Flow

The normal flow begins when a disaster happens:

1) Local Emergency Management Authority wants to inform the citizens about the emergency situation/disaster.
2) The authority IoT server(s) connected directly to an IoT network or to a communication network sends the information instantaneously with no delay to the IoT service platforms responsible for the designated areas. These networks ensure secure communications where no intruders can provide false public warning information via the network.
3) The IoT service platform receiving public warning information filters the type of media provided based on the algorithms it supports and the capability of the connected IoT devices, it forwards the information to the IoT devices. The IoT device may translate the received message into other notification formats towards the population to be warned. Examples include the display of the messages on available screens such as a connected TV, public connected screens (billboards, bus stop display, etc.), or even speaks out the message, triggering of alarms/buzzers, blinking of lamp/led, etc.
4) An IoT device receives the public warning information and presents it to the citizens. This could be in the form of text, voice, video, vibration, light, and others. No acknowledgment is required for receiving these messages.

6.7.7 Alternative flow

This could be the same as normal flow, however the IoT service platform is part of the communication network.

6.7.8 Post-conditions

The public warning information is received by the citizens.

6.7.9 High Level Illustration

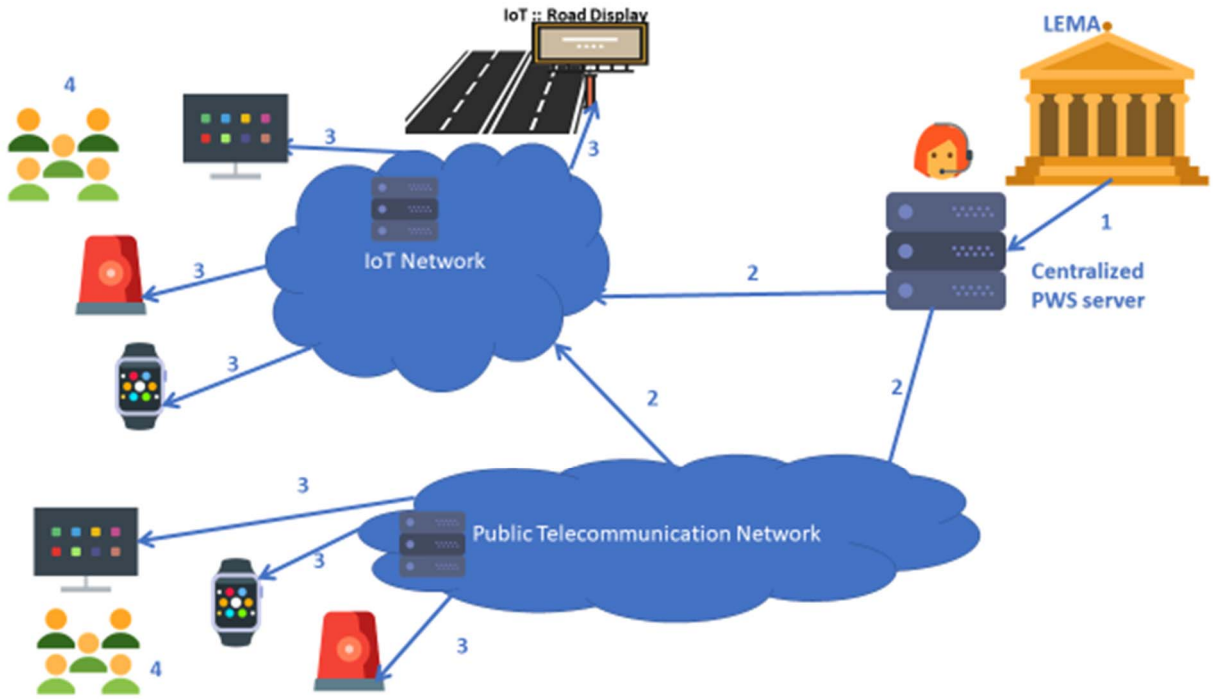


Figure 14: Illustration for warning sent via IoT device to citizens

6.7.10 Potential points of failure putting safety at risk

- IoT device failure or battery life expired.
- PWS Message is not comprehensive or cannot be understood by the IoT device.
- Communication network congestion or failure (totally or partially).
- False alarm due to misconfiguration communication network (e.g. sending the PWS message to the wrong IoT devices/location).
- False alarm due to IoT device being hacked.
- False alarm due to IoT device being misconfigured.
- IoT network failure.
- Failure of the device that is used to present the information to the citizens (e.g. road Variable Message Sign) that is connected to the IoT device.
- Failure in discovering multiple PWS message with the same information. This can be located in the communication network, IoT network or IoT device.

6.7.11 Potential means to prevent points of failure

- PWS message content should be comprehensive; different languages, icons, text, etc., may be required to identify the warning message and to enable the IoT device to take the required action if instructed by the PWS message.
- The IoT service platform and the IoT device should identify PWS message duplication and supress them.
- The IoT service platform and IoT device should forward the PWS, if configured or instructed to do so and if its capability allows.

- To prevent malicious access, i.e. hacking, the communication networks supporting PWS service should ensure that only authorized and authenticated IoT devices are connected to the network.
- The communication networks/service provider should ensure the security, integrity and correctness of the PWS messages to prevent the sending of malicious messages by third parties.
- The IoT service platform and the IoT device should be capable to identify the authenticity of the received PWS message as well as the originator of the PWS message to prevent malicious access, i.e. hacking.
- IoT devices and the whole PWS system should be tested and updated regularly to ensure successful operation.

6.8 AE1: IoT communication with priority handling to prevent emergency situation

6.8.1 Emergency Domain

This use case applies to automated emergency response domain.

NOTE: An automated response to a warning message sent from an IoT device, i.e. before an emergency situation arises, as described in the present clause, is not considered an emergency situation per se. However, it is included below as a useful contribution to ensure a comprehensive coverage of potential requirements.

6.8.2 Description

This use case can be for example when a gas-pipeline that has reached high pressure in a location, and the IoT device informs a remote-control system to regulate the situation to prevent an emergency situation of explosion! This can be seen as a means for utilities to control their networks to prevent emergency situations, through a remote automated closed control system for handling of situations in a faster manner than via human interaction.

This use case describes a critical situation where an IoT device (e.g. industrial control monitor) with a subscription to a priority service needs to send information to a remote server to take action that may include requesting the same or another IoT device to take the action. This IoT device invokes priority service to obtain priority for the data communication session over the communication network.

The priority service requires, in addition to the subscription, an application installed on the IoT device responsible to analyse the data received from the sensors and determine when to invoke the priority service. It can also reset itself/revoke the request without human interaction.

The priority service provider provides secure mechanism to allow access of the IoT device for the use of this service. Hence, the IoT device to trigger establishment of a session that is treated with priority for the information and media flows (all or some). The media could be data, text, others.

6.8.3 Actors

The actors are described in Table 2 with the following additional clarifications:

- IoT device: device comprising one or more sensor(s) that provides data to IoT server via the IoT network;
- IoT application: an application within the IoT device enabling it to invoke a priority service over communication network when discovering an emergency situation based on thresholds of data configured in the device;
- communication network/service provider: A network that can differentiate the IoT devices as priority service based on its subscription. It can provide secure, reliable and instantaneous connection, and is able to prioritize priority connections over others; and
- IoT server: A server that is capable of receiving information from a remote IoT device and reacts by sending back information to the IoT device and/or taking other actions to prevent emergency situations. In this case, it is an automated action where human interference is not required, and very time critical in relation to reacting to the emergency situation.

6.8.4 Pre-conditions

The following conditions exist in addition to the common pre-conditions of clause 6.1:

- IoT device has a subscription for priority service;
- IoT device has a priority service specialized application that allows invocation/revocation of the request of priority service towards the server based on the information received from the sensor(s);
- IoT device has connectivity to the priority service Communication network/service provider;
- the method for invoking data transmission by the specialized application is pre-determined (e.g. use of a server address and media, etc.); and
- a communication network/Service provider that supports priority services and provides prioritized sessions with suitable priority among other communications over the same network, especially in case of congestion.

6.8.5 Triggers

The sensor(s) provides information continuously to the IoT device. Based on the configured information, when the IoT device detects an emergency situation it activates the priority service and sends the information to the designated IoT server for action.

The Communication/service provider triggers the algorithms for checking the security and availability of the network to provide priority for that IoT service and ensure the required Quality of Service (QoS) is met. In case of no available bandwidth, the communication network/service provider may take actions (example; terminating other non-priority sessions, not allowing new non-priority sessions to receive connection) to ensure the requirement for the priority session is met.

The IoT server, once receiving any information from the IoT device, is triggered to take actions accordingly.

6.8.6 Normal Flow

The following describes the sequence of events:

1) the IoT device activates the priority application and invokes the priority service;
2) the IoT device sets a secure connection to the communication network/service provider that provides priority treatment to the affected media flows;
3) the IoT device connects to the remote IoT server over the communication network/service provider;
4) the IoT device sends data to the remote IoT server;
5) the remote IoT server reacts automatically with an action to prevent the emergency situation. The action might be handled locally or sent back to the IoT device, or another IoT device, to handle; and
6) the IoT device indicates the end of the priority service session using a predetermined method.

6.8.7 Alternative flow

The IoT devices are connected to the IoT remote server directly through the public communication network.

6.8.8 Post-conditions

The emergency situation is prevented leading to saving human lives, buildings, resources, etc.

6.8.9 High Level Illustration

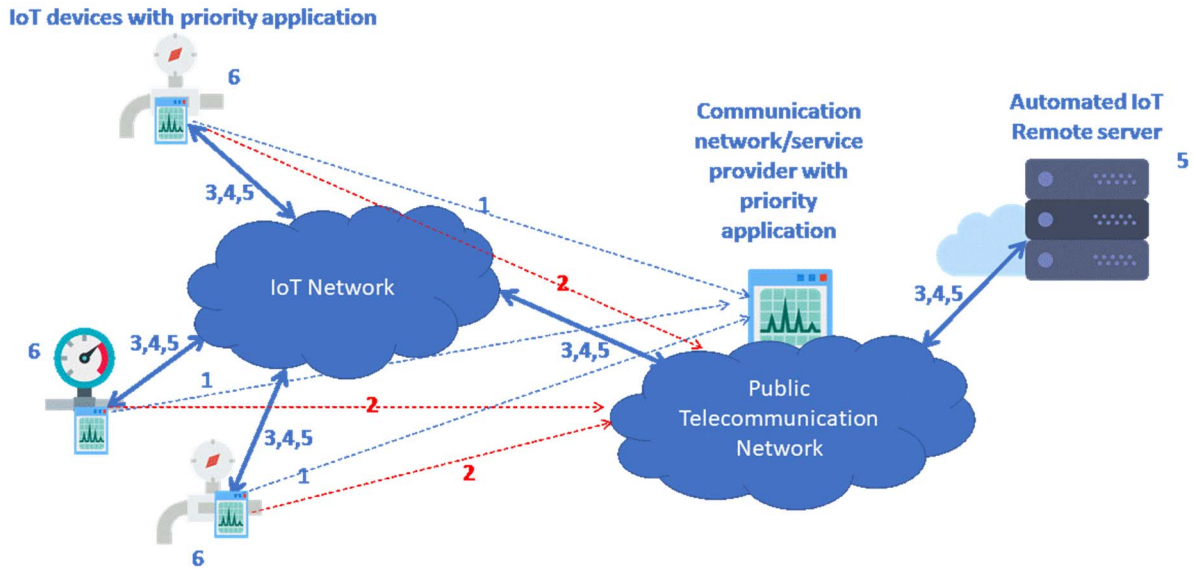


Figure 15: Illustration of IoT communication with priority handling to prevent emergency situation

6.8.10 Potential points of failure putting safety at risk

- IoT device defect, including the sensors, battery, electronics, etc.
- Communication network misconfiguration regarding the priority services and providing the required resources.
- The remote IoT server defect or failure.
- Communication network failure (totally or partially).
- False alarm due to IoT device being faulty, misconfigured, hacked, etc.
- False alarm due to unforeseen circumstances, e.g. sensing wrong parameters that constitutes an emergency. This requires some redundancy to determine the reliability of sent data to the server, at the same time limit the number of IoT devices sending the alarms to prevent a large number of alarms from many IoT devices.

6.8.11 Potential means to prevent points of failure

- The communication network should support means for an IoT device with priority services to initiate a priority session using the application on the IoT device, also to terminate, or revoke the priority session.
- To prevent hacking, the communication network should support means to authenticate and authorize the IoT device and the priority application.
- The communication network should support means to provide the priority function and QoS during congestion when the service is activated by the IoT device, for all requested media. This is to ensure adequate operation of the service.
- The remote server should be able to check the authenticity and the reliability of the information received from the IoT devices, e.g. using secure mechanisms, to prevent hacking as possible.
- IoT devices and the communication network with the priority service should be tested and updated regularly to ensure successful operation.

6.9 AE2: IoT-based action following public warning system message reception

6.9.1 Emergency Domain

This use case applies to emergency domain "automated emergency response".

6.9.2 Description

Public warning systems rely mainly on direct communication (TV, Radio, authorities broadcasting warning message using loudspeakers, sirens, etc.) or telecom services (special text messages). Despite these efforts, individuals may not be aware of these messages. With the wide deployment of IoT devices in the home, city, transportation, etc., public warning systems can benefit from these new "communication vectors" in order to efficiently reach and inform the individuals in emergency situations. Moreover, IoT devices can take action based on the received warning messages.

The use case shows how IoT devices can be used in emergency situations. In particular, IoT devices can be used as a support for a Public Warning System for a wide dissemination of warning messages in the original format but also in other formats. For example, when an earthquake occurs at sea, it may be followed by a tsunami in coastal regions in the following minutes. Public authorities may send PWS messages to the population and in particular towards specific IoT devices such as opening automatic doors' locks in public transportation (subway) allowing users to get out easily, or using connected billboards/road displays to display evacuation plan, etc. In certain scenarios, a PWS message can trigger the transmission of audio/video streams from camera/microphone equipped IoT devices in order to provide contextual information about some areas of interest such as subway accesses, main street, bridges, etc.

In the transportation domain, and in the case of Intelligent Transportation Systems (ITS), a PWS message can be received by a connected/autonomous vehicle and translated to an ITS Decentralized Environment Notification Message (DENM) [i.87] that is relayed in an ad-hoc manner to other vehicles nearby. The message can be then displayed on the driver's dashboard for further actions.

6.9.3 Actors

- Local Emergency Management Authority (LEMA): responsible for sending PWS messages.
- IoT Service Platform: acts as a middleware between the LEMA and the IoT devices that will digest the message. It stores the data, manages subscriptions, triggers notifications, etc.
- IoT device: subscribes to the PWS service on the IoT service platform through an IoT gateway.
- Communications networks:
  - **Emergency service communication network:** a dedicated network to emergency services that may connect the LEMA to the IoT service platform.
  - **Public telecommunication network:** a public telecommunication network for routing data flows to the appropriate destination with the ability to differentiate and to prioritize emergency traffic from regular traffic. It is used to connect some IoT devices to the IoT service platform. It is also connecting the LEMA to the IoT service platform.
  - **IoT network:** a communication network dedicated to connect some IoT devices; For example, Long Range Low Power IoT networks (Sigfox, LoRaWAN, etc.).

6.9.4 Pre-conditions

The following condition exist in addition to the common pre-conditions of clause 6.1:

- Information about a disaster is to be issued to the citizens.

6.9.5 Triggers

The LEMA sends a warning message to a certain group of IoT devices through the IoT service platform.

6.9.6 Normal Flow

1) The decision maker at the LEMA "publishes" PWS messages on the IoT service platform(s). The communication could go through the public telecommunication network or through the emergency network if such network is directly connecting the LEMA to the IoT service platform.

2) The IoT device receives (synchronously or asynchronously) notifications from the IoT service platform. This communication could go through the public telecommunication network or through dedicated IoT networks.

3) The IoT device may translate the received message into other notification formats towards the population to be warned. Examples include the display of the messages on available screens such as a connected TV or even speaks out the message, triggering of alarms/buzzers, blinking of lamp/led, etc.

4) The IoT device acts based on the received warning message. Examples include stopping/deactivating an elevator (e.g. during an earthquake), stopping a subway/tramway or any other controllable vehicle, switching on/off of electrical switches, turning off a gas tap, triggering a temperature/ humidity/ smoke sensor, etc.

5) The IoT service platform can keep track (e.g. for logging purposes) of (some specific) actions that have been taken by the IoT devices.

6.9.7 Alternative flow

None.

6.9.8 Post-conditions

The public warning message reached a wider population and the emergency situation is prevented.

6.9.9 High Level Illustration

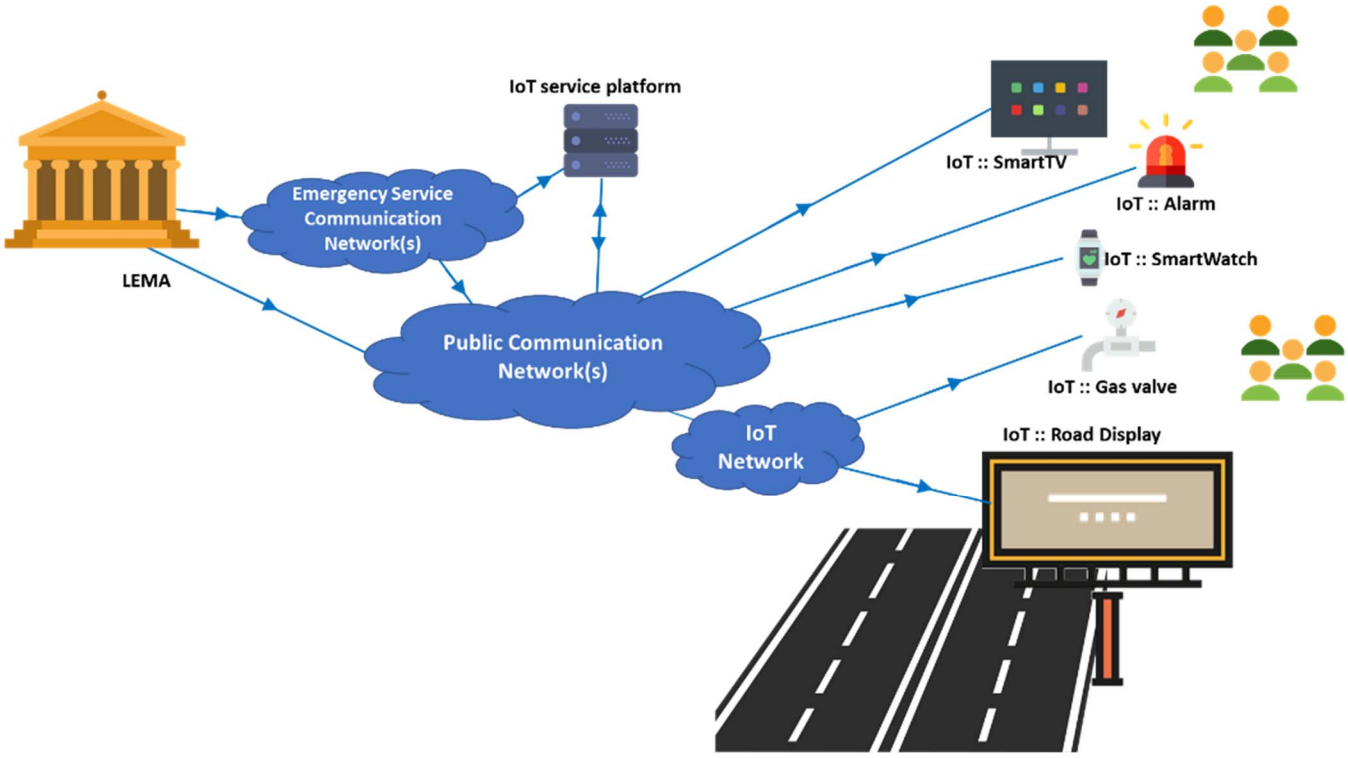


Figure 16: High level illustration of "IoT-based action following PWS message reception" use case

6.9.10 Potential points of failure putting safety at risk

- IoT device failure: e.g. battery failure, etc.
- Network congestion/failure: communication networks are under congestion and/or failure, and cannot convey the PWS message in time or support with a guaranteed QoS the triggered audio/video transmissions.
- Security breach of the IoT device.
- IoT device triggers a false alarm due to improper configuration (understanding of the PWS, affected zone), which leads to an invalid action.
- The PWS message cannot be understood by the IoT device.

6.9.11 Potential means to prevent points of failure

- Guaranteed QoS from the traversed communication networks and from the IoT service platform for the transport of both PWS messages and the eventual (near) real-time data streams.
- IoT networks should be sufficiently robust to withstand local points of failure in the event of an emergency necessitating the transmission of a PWS message.
- In case of network failure, alternate communication paths should be available to route the PWS message, using for example satellite or vehicular communication networks.
- Security (Access control, authentication, authorization, integrity protection, etc.) to prevent a malicious triggering of relay/reaction of non-legitimate PWS.
- The proper operation of an IoT device involved in AE response operation should be monitored and periodically tested.

- IoT device should be kept updated to support the latest versions of PWS.
- Means to enable a shared unambiguous meaning of PWS messages, so that they can be understood unambiguously by IoT devices should be developed, for example encoding of pre-defined messages or the definition of specific semantics and ontology.

6.10 Conclusions

The previous clauses of clause 6 have described a set of use cases where IoT devices are involved in emergency situations. These use cases have been analysed to identify potential failure causes, which could be prevented if the proper measures were taken in the related hardware and software components of the communication system. These measures have been described as potential requirements in the last sub-section of each use case description.

Next clause will consolidate these potential requirements in recommendations for the enhancements of existing or future standard documents.

7 Impact of use cases on specifications

7.1 Introduction

The recommendations of requirements in the present clause 7 do not directly target specific specifications. Rather, they are organized by emergency domain and according to which knowledge area of that domain they apply. Committees responsible for the standardization of emergency communications are therefore encouraged to review all the recommended requirements that follow and are invited to adopt/adapt those that they consider relevant for communication involving IoT devices in emergency situations. Based on the state-of-the-art analysis performed in clause 5, such committees could be, but are not limited to, for example ETSI SC EMTEL (e.g. in ETSI TS 102 181 [i.1] or ETSI TS 102 182 [i.2]), ETSI TC SmartM2M, ETSI TC TTCE, or 3GPP/oneM2M partnership projects.

7.2 Recommendations of requirements for existing domains

7.2.1 Emergency Calling domain

7.2.1.1 Usage & Maintenance

EC_U&M_1: The IoT service platform operator should be able to enable/disable the emergency communication features in an emergency communication capable IoT device.

EC_U&M_2: An IoT device supporting emergency communication functionality should be able to report potential failure conditions (low battery, etc.).

EC_U&M_3: An IoT device supporting emergency communications functionality should be remotely manageable.

EC_U&M_4: A supporting IoT service platform should monitor the status of an IoT device supporting emergency communications functionality.

EC_U&M_5: The configuration of the IoT device supporting emergency communications functionality should be properly tested before the start of its operation.

EC_U&M_6: An IoT service platform operator should be able to add IoT device data at any time to emergency session.

EC_U&M_7: Emergency data from an IoT device should be accurate and reliable.

NOTE 1: Deployment of redundant sensors/IoT devices could enhance the reliability of the IoT device/IoT service platform.

NOTE 2: Artificial Intelligence and fusion of data from multiple sensors could help to guarantee the validity of an alarm in place of human call-out.

EC_U&M_8: Emergency data received from an IoT device should be clear and unambiguous.

EC_U&M_9: The IoT service platform should be able to prevent an IoT device from sending repeated or redundant emergency data messages.

7.2.1.2 Interoperability

EC_I_1: IoT devices operating in safety critical environments should support emergency calling as standardized for existing Public Telecommunication Networks including the sending of video when capable.

EC_I_2: PSAPs/ECCs should support the reception of an emergency data message from an IoT device (i.e. a one-shot emergency data message with no Callback).

EC_I_3: Emergency data from an IoT device should be in a format that is understandable by the PSAP.

7.2.1.3 Networks and connectivity

EC_N_1: Public Telecommunications Networks should support the sending of an emergency data message from an IoT device.

EC_N_2: Public Telecommunication Networks should be able to route an emergency data message from an IoT device with the same priority as other emergency communications.

NOTE 1: The priority given to routing of an emergency data message is a deployment decision potentially subject to regulation.

EC_N_3: ESInets should support the transmission and routing of an emergency data message from an IoT device.

EC_N_4: An IoT service platform should support priority handling of emergency communications from an IoT device.

EC_N_5: An IoT network should provide sufficient QoS and capacity to support the emergency data, including video or other streaming services.

NOTE 2: The impact of false/fake alarms on other user traffic may be exacerbated in networks where such alarms are afforded priority routing. This should be taken into account in future deployments of, and regulation relating to, emergency data messages.

7.2.1.4 Data Exchange at service and application level

EC_DE_1: IoT devices operating in safety critical environments should support the sending of an emergency data message to a PSAP or an IoT service platform monitoring emergencies.

EC_DE_2: PSAPs should prioritize the handling of emergency communications from IoT devices, based on their criticality relative to other calls they receive, for example human-initiated emergency calls.

7.2.1.5 Security

EC_S_1: Remote triggering of an emergency data message from an IoT device should be prevented other than via its sensor (i.e. it should not be possible to hack the device causing it to send an emergency communication that was not triggered as a result of processed sensor information).

EC_S_2: The IoT platform should be able to determine the veracity of an alarm indication, e.g. to prevent a denial of service attack.

7.2.2 Mission Critical Communications domain

7.2.2.1 Usage & Maintenance

MC_U&M_1: All IoT devices involved in MC communications should support remote maintenance (software updates, battery and function check, etc.).

MC_U&M_2: Software updates of IoT entities involved in MC communications should be subject to a certification process.

MC_U&M_3: IoT applications with man-machine-interfaces should provide suitable role-specific access to COP data (e.g. suitable graphical user interface) and should support switching between role-specific man-machine-interfaces (since roles of deployed personnel may change over time).

MC_U&M_4: IoT applications with man-machine interfaces related to the COP should provide functionalities for daily tasks (e.g. emergency medical service documentation and billing).

MC_U&M_5: The authorization scheme should allow mapping of role-specific IoT devices and applications (which includes man-machine-interfaces and data access rights) to users with as little user interaction as possible.

7.2.2.2 Interoperability

MC_I_1: All IoT devices and service platform entities to be used for mission critical applications should have passed some sort of "interoperability certification" to ensure that devices and applications from different vendors can communicate with each other.

MC_I_2: Syntax and semantics of data contributing to the COP should be standardized. This includes IoT data.

MC_I_3: Interfaces to a COP database should be standardized (ideally based on an open standard with a reference implementation).

7.2.2.3 Networks and connectivity

MC_N_1: Data exchanges should be based on commonly accepted standards for professional and home users.

MC_N_2: The mission critical communications network(s) should support (near) real-time (multi-)point-to-(multi-)point data transfer and streaming.

MC_N_3: The mission critical communications networks' capabilities should be fully scalable ranging from day-to-day rescue tasks to large scale disasters with potentially damaged infrastructure.

MC_N_4: Mission critical data communications should support both an infrastructure mode (via access points, "on-network") and an ad hoc mode (decentralised wireless network, "off-network").

NOTE: Networks in ad hoc mode are assumed to be exclusively used by emergency services. Networks in infrastructure mode may be exclusively used by emergency services or may be provided by public communication networks.

MC_N_5: The IoT devices (and communication terminals) should automatically switch between infrastructure mode and ad hoc mode. The IoT devices may support bandwidth sharing among the two modes.

MC_N_6: The ad hoc mode should support routing and data transmission via multiple hops (i.e. one or more hops).

MC_N_7: If possible, the ad hoc mode for MC communications should support end-to-end connectivity for the top transmission priority classes and for streaming applications by using appropriate (re-)routing mechanisms (e.g. switching between alternative routes after link failures, setting up of redundant routes, etc.).

MC_N_8: The ad hoc mode for MC communications should support "store and forward" data transmission for isolated network nodes when compatible with the data transmission priority class.

MC_N_9: Both infrastructure and ad hoc modes should support different transmission priority classes for mission critical data.

MC_N_10: IoT devices and IoT applications should be able to suggest data transmission priority classes to the network(s) for data to be transmitted (important primary data should be transported with priority in comparison to (optional) secondary data).

MC_N_11: IoT devices and IoT applications should buffer data locally during network outages until connectivity is regained. After re-establishing connectivity data should be automatically transferred/synchronized without user interaction starting with top priority class data and tentatively avoiding network congestion.

MC_N_12: Mission critical (IoT) data exchanges (i.e. all mission critical data transmission priority classes) should have appropriate priority and pre-emption rights when used on top of public communication networks.

7.2.2.4 Data Exchange at service and application level

MC_DE_1: All relevant mission critical IoT data should be stored in the COP so that the COP allows tracing the activities during the incident response and forecasts. After clearance of the situation the COP data should be available for lessons learnt and investigations.

MC_DE_2: All (IoT) devices and the network(s) involved in the COP should support time synchronization and should assign time stamps to data when/where appropriate. This applies to isolated operation mode, too. Time synchronization events should be logged, so that all time stamps can be mapped to a common time reference.

MC_DE_3: COP data should automatically be synchronized among as many devices as possible ("synchronization composite" consisting of COP databases), especially in the incident area. New devices arriving at the incident area should automatically discover existing synchronization composites and should automatically (i.e. with as little user interaction as possible) synchronize the COP data. The synchronization composite should be able to handle leaving (or failing) devices, too.

MC_DE_4: COP databases should support remote access to COP data without full COP data synchronization.

MC_DE_5: Physical transport of IoT devices (or simple data carriers) with locally stored COP data between disjunctive networks (e.g. between different isolated coverage zones) should allow automatic COP data synchronization.

MC_DE_6: COP databases should support automatically generated and manual data updates. An emergency service decision maker should be able to manually override data updates.

MC_DE_7: An emergency service decision maker should be able to merge COP data from two or more incidents or should be able to split COP data into two or more incidents.

MC_DE_8: IoT devices should be able to trigger other IoT devices via the IoT service platform (e.g. smoke detector turns on camera).

MC_DE_9: The IoT service platform should be able to manually or automatically adapt IoT device data rates (e.g. scaling of video camera resolution) to available network bandwidth.

MC_DE_10: The IoT service platform should support (near) real-time (multi-)point-to(multi-)point data transfer and streaming at the service level.

MC_DE_11: The IoT service platform should identify mission critical communications priority classes and provide them with a guaranteed quality of service.

MC_DE_12: The IoT service platform should support mission critical communications at the service level in isolated operation mode, i.e. without the need to reach a remote server especially in the case when the communication with this server has failed.

7.2.2.5 Security

MC_S_1: IoT devices and IoT service platform should mutually authenticate each other before activation.

MC_S_2: IoT device data should be of sufficient accuracy (i.e. precision and correctness of sensor data).

MC_S_3: New devices/databases to be integrated in the COP synchronization composite should mutually authenticate themselves against the synchronization composite.

MC_S_4: IoT data (e.g. vital parameters) and COP data (e.g. patient data, names, diagnosis, addresses, etc.) confidentiality and integrity should be assured at any time. This requires a sound security architecture and a suitable but flexible authorization scheme for the different user functions and roles.

MC_S_5: IoT data (e.g. vital parameters) and COP data (e.g. patient data, names, diagnosis, addresses, etc.) storage and processing should be designed to guarantee privacy protection (e.g. GDPR) and prevent any personal data breach.

7.2.3 PWS domain

7.2.3.1 Usage & Maintenance

PWS_U&M_1: The IoT platform operator should have the means to enable/disable the PWS in an IoT device supporting PWS.

PWS_U&M_2: An IoT device supporting PWS should be able to report potential failure conditions (low battery, etc.).

PWS_U&M_3: An IoT device supporting PWS should be remotely manageable.

PWS_U&M_4: An IoT service platform supporting PWS should monitor the battery status and operation of an IoT device supporting PWS.

PWS_U&M_5: The configuration of the IoT device supporting PWS should be properly tested before the start of its operation, and then regularly.

PWS_U&M_6: An IoT device supporting PWS may be connected to another device that can display and communicate the received information to the citizens.

PWS_U&M_7: PWS information sent towards an IoT device supporting PWS should be accurate and reliable.

PWS_U&M_8: Reception of PWS warning messages and information, sent towards an IoT device supporting PWS, across countries' borders depends on national regulations.

7.2.3.2 Interoperability

PWS_I_1: An IoT device supporting PWS should support PWS formats as provided by PWS standards and/or regional regulations.

PWS_I_2: An IoT device supporting PWS should support the format of the connected device (if any) to be able to convey the information (i.e. video, voice, text, etc.).

7.2.3.3 Networks and connectivity

PWS_N_1: Public Telecommunications Networks should support the transmission of PWS messages towards an IoT device supporting PWS.

PWS_N_2: Public Telecommunications Networks should route PWS messages towards the designated IoT device or IoT platform, supporting PWS, with high priority.

PWS_N_3: An IoT service platform supporting PWS should support priority handling of PWS messages towards an IoT device.

7.2.3.4 Data Exchange at service and application level

PWS_DE_1: PWS message content should be comprehensive. This may include different languages, icons, text, etc. Means are required to enable the IoT device to understand the PWS message. Comprehensive PWS message is used to identify the warning message and to enable the IoT device to take the required action if instructed by the PWS message.

PWS_DE_2: The IoT service platform and the IoT device, supporting PWS, should identify PWS message duplication and supress them.

PWS_DE_3: The IoT service platform and IoT device, supporting PWS, should forward the PWS message if instructed to do so and if its capability allows.

PWS_DE_4: The IoT service platform supporting PWS should ensure that the data forwarded to the selected IoT device supporting PWS is compatible with the data type supported by the IoT device.

7.2.3.5 Security

PWS_S_1: The communication networks should ensure that only authorized IoT devices supporting PWS that are communicating the PWS messages to citizens are connected to the network.

PWS_S_2: The communication networks/service provider should ensure the security, integrity and correctness of the PWS messages to prevent the sending of malicious messages by third parties.

PWS_S_3: The IoT service platform and the IoT device, supporting PWS, should be capable to identify the authenticity of the received PWS message.

PWS_S_4: The IoT service platform and the IoT device, supporting PWS, should be capable to identify the authenticity of the sender/originator of the PWS message.

7.3 Recommendations of requirements for new domains

7.3.1 Automated Emergency response domain

7.3.1.1 Usage & Maintenance

AE_U&M_1: The IoT service platform operator and/or the automated emergency response IoT server operator should have the means to enable/disable the automated emergency response IoT device and any running application.

AE_U&M_2: An IoT device supporting automated emergency response should be able to report potential failure conditions (low battery, etc.).

AE_U&M_3: An IoT device supporting automated emergency response should be remotely manageable by the IoT service platform operator and/or the automated emergency response IoT server operator.

AE_U&M_4: A supporting IoT service platform should monitor the status of an IoT device supporting automated emergency response.

AE_U&M_5: The configuration of the IoT device supporting automated emergency response should be properly tested before the start of its operation, and then regularly.

AE_U&M_6: An IoT device for automated emergency response may be connected to another device that can take actions based on the received instruction from a designated remote server.

AE_U&M_7: In Automated emergency response system, the received information from the IoT device and the sent instructions towards an IoT device should be accurate and reliable.

AE_U&M_8: IoT devices and the communication network with the priority service should be tested and updated regularly to ensure successful operation.

7.3.1.2 Interoperability

AE_I_1: An IoT device for automated emergency response should be able to support automated emergency response based on standardized solutions and regulations (if any).

AE_I_2: An IoT device for automated emergency response should be able to support automated emergency response priority service.

AE_I_3: An IoT device for automated emergency response should support the format of the connected device to be able to convey the information received by the designated remote server.

7.3.1.3 Networks and connectivity

AE_N_1: The communication networks should support means for the IoT device used for automated emergency response to operate with priority services and to initiate a priority session using the application on the IoT device, also to terminate, or revoke the priority session.

AE_N_2: The communication networks should support means to provide the priority function and QoS during network congestion when the service is activated by the IoT device for automated emergency response, for all requested media.

7.3.1.4 Data Exchange at service and application level

AE_DE_1: An IoT devices for automated emergency response should support the sending and receiving of the automated emergency response server information.

AE_DE_2: An IoT service platform involved in automated emergency response should support the transmission of emergency data messages through a dedicated service.

AE_DE_3: An IoT service platform involved in automated emergency response should handle emergency data messages at the service level with a guaranteed priority.

AE_DE_4: An IoT service platform involved in automated emergency response should ensure data interoperability between the emergency control centre and the IoT devices, i.e. semantics and ontologies for messages that trigger automated emergency responses should be standardized.

7.3.1.5 Security

AE_S_1: The communication networks should support means to authenticate and authorize the IoT device for automated emergency response and the priority application.

AE_S_2: The remote server used for automated emergency response should be able to check the authenticity and the reliability of the information received from the IoT devices for automated emergency response, e.g. using secure mechanisms.

AE_S_3: Triggering of an automated emergency response message from an IoT device for automated emergency response should be only based on information received from its sensors (i.e. it should not be possible to hack the device causing it to send an emergency communication that was not triggered as a result of processed sensor information).

AE_S_4: The IoT platform for automated emergency response should be able to determine the veracity of an alarm indication.

AE_S_5: The IoT service platform for automated emergency response should be protected against denial of services attacks.

7.4 Concluding recommendations

7.4.1 SC EMTEL recommendations

As stated in clause 7.1, the recommendations of requirements above do not target specific specifications. However, given that they are organized by emergency domains of which three out of four are pre-existing in associated SC EMTEL specifications, it is clear that there will be some relationship between these recommendations and those in existing SC EMTEL specifications. The main SC EMTEL deliverables for the three existing emergency domains covered in the present document and as summarized under clause 5.2 are:

- for Emergency calling - ETSI TR 102 410 [i.3] and ETSI SR 002 180 [i.19];
- for Mission Critical communications - ETSI TS 102 181 [i.1]; and
- for Public Warning Systems - ETSI TS 102 182 [i.2].

As such, SC EMTEL should consider in particular the requirements under clause 7.2.1 in light of their relationship to and potential for inclusion in ETSI ETSI TR 102 410 [i.3]; the requirements under clause 7.2.2 in light of their relationship to and potential for inclusion in ETSI TS 102 181 [i.1]; and the requirements under clause 7.2.3 in light of their relationship and potential for inclusion in ETSI TS 102 182 [i.2].

However, whilst it is clear there will be some relationship between the recommendations for requirements and existing SC EMTEL specifications, it is worth remembering that the focus of existing specifications is very much communication between humans (individuals, emergency service personnel, authority operatives), and not communication with and between IoT devices. SC ETMEL may therefore wish to consider creating new specifications for each domain, referencing the existing specifications where appropriate but focussing specifically on requirements for IoT devices involved in emergency communications.

The fourth emergency domain covering Automated Emergency response is clearly a new domain specific to machine type communications involving IoT devices. It is therefore recommended that SC EMTEL creates a new specification including at least requirements based on those under clause 7.3 of the present document.

7.4.2 Recommendations for IoT service platform specification groups

For oneM2M, as a standardized IoT service platform, potential requirements related to "interoperability" and "data exchange at service and application levels" could be of interest for oneM2M RDM (Requirements and Domain Models) working group. In addition, oneM2M should consider requirements relating to priority communications and include mechanisms to guarantee the required quality of service for such communications. These potential requirements together with "security" potential requirements, are relevant to oneM2M SDS (System Design and Security) working group. In particular, oneM2M should consider these potential requirements for potential inclusion in future releases of:

- ETSI TR 118 501 [i.6] - Use Case Collection
- ETSI TS 118 102 [i.93]- Requirements
- oneM2M TR-0046 [i.94] - Study on Public Warning Service Enabler

When presenting the initial draft of the present document to oneM2M, it was proposed to add to the present document an annex on "How oneM2M service platform complies with the identified potential requirements". Such an annex would have a larger impact in one of the oneM2M deliverables mentioned above, with a reference to the present document, as it would reach more easily the oneM2M community.

The same potential requirements may also be relevant to other IoT service platforms standardization efforts such as Open Connectivity Foundation (OCF). Indeed, all the identified potential requirements are relevant to "Core Technology", "Data Model" and "Security" OCF working groups. OCF should consider these potential requirements for potential inclusion in future releases of:

- OCF Core Specification
- OCF Resource Type Specification
- OCF Device Specification

- OCF Security Specification

7.4.3 Recommendations for network specification groups

For 3GPP related specifications, potential requirements related to "Network Connectivity" are in general relevant to 3GPP working groups (SA1, SA4, SA6), whereas "Security" potential requirements may relate to SA3 work. These recommendations would apply as well to other groups standardizing networking technologies that could be used by IoT devices, e.g. ETSI (TCCE, SES), IETF, ITU-T, IEEE or some specific industrial alliances (ZigBee, Z-Wave, LoRa, etc.).

Annex A:
Use case MC2: MCI logistics and management in detail

Figure A.1 depicts the (idealized) casualty flow during a MCI. Injured casualties are either transported directly to hospitals ("immediate medical evacuation - medevac") or taken to the Temporary Care Centre (TCC). Depending on their health status and depending on available resources these casualties are either handed over to a temporary shelter or transported to hospitals. Non-injured casualties are directly guided to a temporary shelter and then evacuated to shelters outside the incident area.

The main objective of MCI logistics is keeping track of all casualties and mapping casualties to treatment resources in the field, transport vehicles, hospitals (considering type of injury and treatment capacities), and shelters. Rough knowledge of all casualties' current locations is desirable, but detailed movement patterns are normally not required. An overview of remaining casualties in vicinity of the Casualty Collection Point(s) (CCP), patients entering/leaving each Temporary Care Centre (TCC), and patients on their way to or arriving at receiving hospitals is the basis for all MCI management decisions.

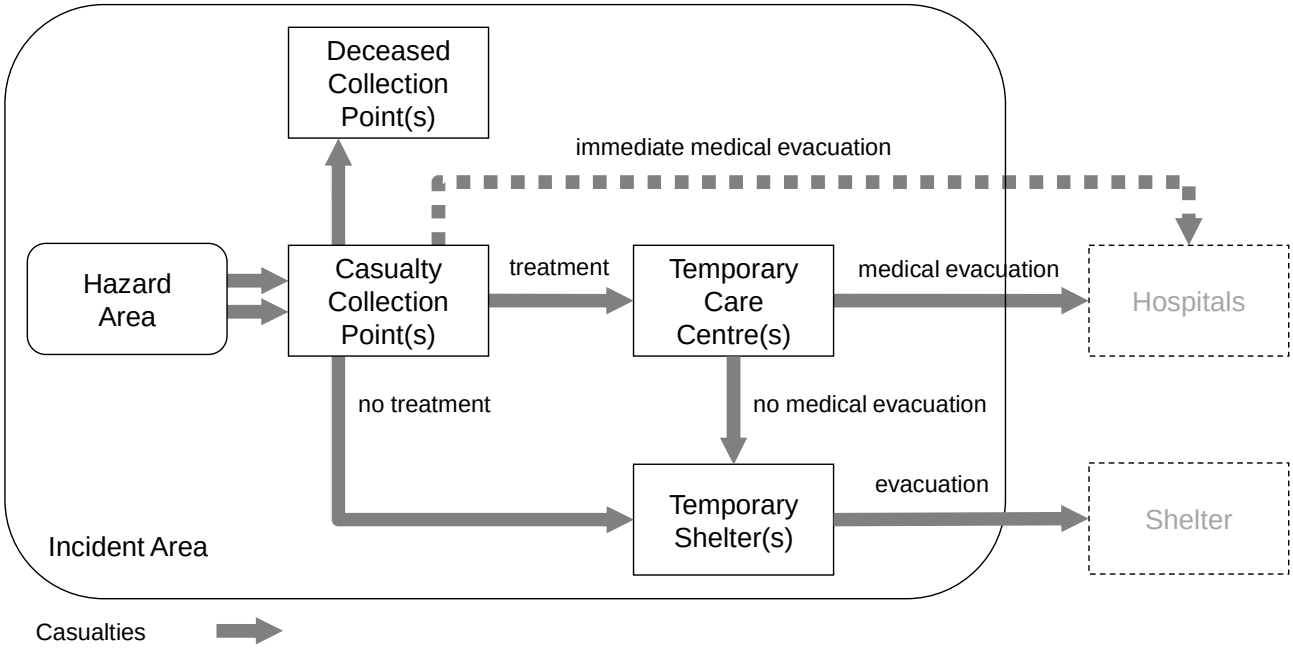


Figure A.1: Casualty flow chart

Figure A.2 depicts the (idealized) MCI process chain from the casualty data perspective. Casualty data is not static which means that all relevant status changes have to be communicated to all SubService ECCs. E.g. if one casualty's triage category changes after the initial assessment, then all decisions regarding treatment and medical evacuation priority of all other casualties will have to be re-evaluated. Likewise, there might be an updated diagnosis affecting medical evacuation priority and the choice of the receiving hospital.

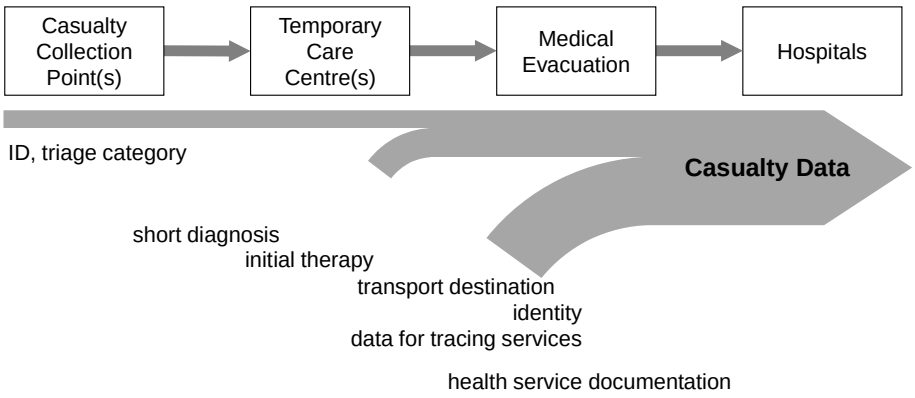


Figure A.2: Casualty data along medical evacuation feeding into the COP

Current approaches for MCI management are mainly based on paper tags which are attached to all casualties during the registration process at the CCP. These tags have unique IDs and are marked with the casualty priority and a short diagnosis as result of a brief medical examination which is typically a standardized triage algorithm checking main vital parameters. Additionally, supplementary information like date, time, or position information can be filled in, too.

IoT devices could help to overcome the disadvantages of this paper-based approach. In principle there are two possibilities:

- Triage tags with passive machine-identifiable IDs (e.g. RFID tag, barcode, etc.), emergency teams with electronic handheld devices, CCP/TCC/transport vehicles/hospitals equipped with readers at entry/exit gates (i.e. IoT sensor devices).

- Triage tags as active IoT devices transmitting their position (and other data, e.g. vital parameters, CBRN measurement results, etc.).

Figure A.3 shows a typical fully deployed management structure for a mass casualty incident. All involved sector/field emergency control centres (SECC/FECC) and the remote emergency control centre (ECC) require a comprehensive overview of all patients, of all transport vehicles for medical evacuation, of all available resources, and of all hospital treatment capacities. Additionally, the roles/responsibilities of deployed teams/commands may change over time (e.g. if there are no patients to be picked up at the casualty collection point any more, then the teams will support the temporary care centres or the medical evacuation). Last but not least the actual legal situation may define different responsible roles at different locations for key decisions to be taken (e.g. mapping of patients to transport vehicles to destination hospitals).

NOTE: Redundant storage of COP data on different devices (e.g. among all decision makers) with automatic re-synchronization seems to be a viable solution.

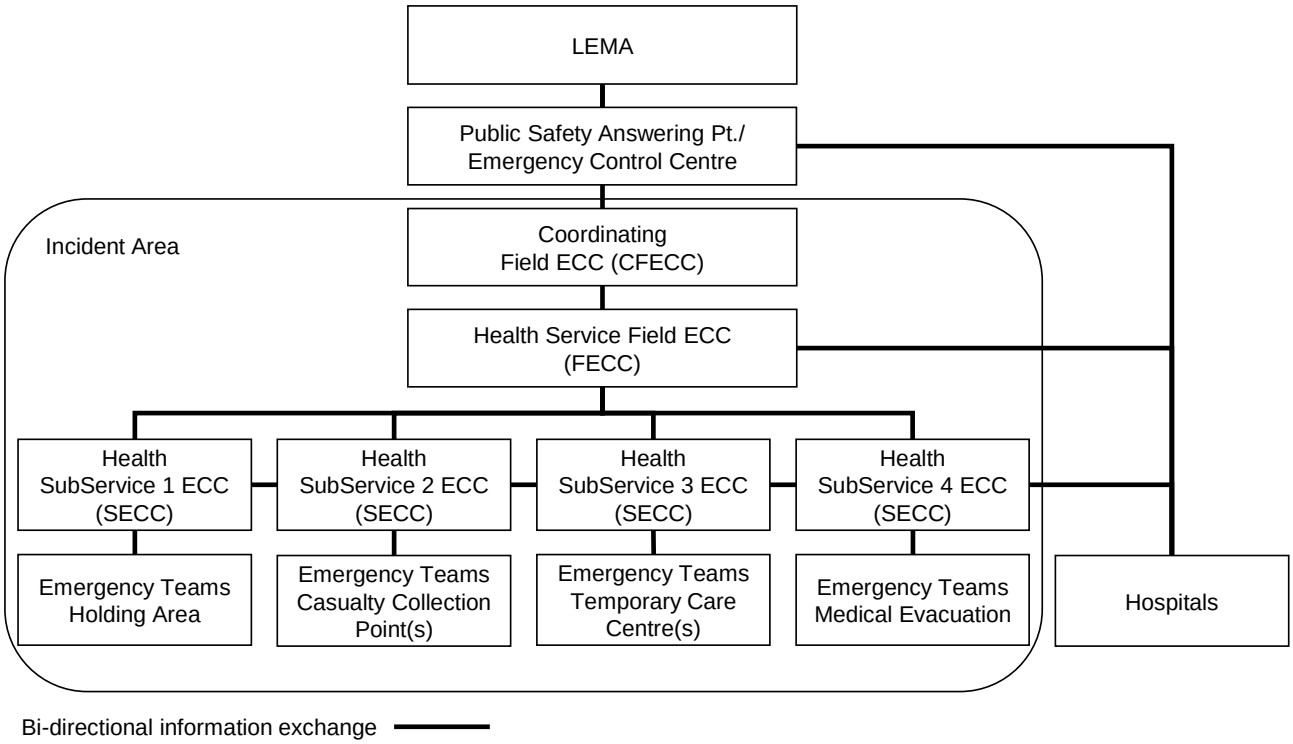


Figure A.3: Health service COP information exchanges

Emergency Control Centre (ECC)

Tasks:

- Remote coordination of involved emergency services

Coordinating Field Emergency Control Centre (CFECC)

Tasks:

- Coordination of involved emergency services in the field
- Reporting to ECC

Health service field Emergency Control Centre (FECC)

Tasks:

- Coordination of involved health emergency services
- Reporting to CFECC

Health SubService 1 Emergency Control Centre (SECC) at holding area

Tasks:

- Assign tasks to emergency teams
- Reporting to health FECC

Health SubService 1 emergency teams at holding area

Tasks:

- Obtain tasks from SubService 1 SECC

Health SubService 2 Emergency Control Centre (SECC) at Casualty Collection Point (CCP)

Tasks:

- Assign tasks to emergency teams
- Reporting to health FECC

Health SubService 2 emergency teams at Casualty Collection Point (CCP)

Tasks:

- Immediate life-saving measures
- Take-over of casualties at CCP(s)
- Search for individuals outside hazard area
- Assessment of all casualties (triage) and registration
- Initial treatment and stabilization, preparation for medical evacuation
- Documentation of findings and reporting (this involves IoT devices)

Health SubService 3 Emergency Control Centre (SECC) at Temporary Care Centre (TCC)

Tasks:

- Assign tasks to emergency teams
- Reporting to health FECC

Health SubService 3 emergency teams at Temporary Care Centre (TCC)

Tasks:

- Assessment of casualties (triage) and registration
- Initial treatment and stabilization, preparation for medical evacuation

Health SubService 4 Emergency Control Centre (SECC) medical evacuation

Tasks:

- Assign tasks to emergency teams
- Reporting to health FECC

Health SubService 4 emergency teams medical evacuation

Tasks:

- Medical evacuation of casualties according to priority. Note: destination hospital has to be chosen according to treatment capacity and type of injury.

Hospital(s)

Tasks:

- Preparations (e.g. increasing treatment capacity) according to COP
- Reporting to health FECC, health Sub-Service 4 emergency control centre, ECC

Annex B: Bibliography

ETSI TS 122 179: "LTE; Mission Critical Push to Talk (MCPTT) over LTE; Stage 1 (3GPP TS 22.179)".

ETSI TS 122 282: "LTE; Mission Critical Data over LTE (3GPP TS 22.282)".

ETSI TS 123 401: "LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401)".

Annex C
Change History

Date	Version	Information about changes
July 2018	0.0.1	Preliminary draft with table of content and scope uploaded to SC EMTEL
September 2018	0.0.2	Initial draft with the result of STF555 Task 2
December 2018	0.3.0	Draft with result from Task 3 for EMTEL rapporteur's meeting
January 2019	0.4.0	First version of the stable draft for EMTEL #44
February 2019	0.5.0	Stable draft with result from Task 4 for EMTEL rapporteur's meeting on Feb 27
March 2019	0.6.0	Pre-final draft for external distribution
April 2019	0.7.0	Final draft delivered for approval to SC EMTEL
May 2019	0.7.1	Final draft including pre-approved editorial comment received during RC

History

Document history		
V1.1.1	July 2019	Publication