ETSI TS 102 181 V1.3.1 (2020-06)

**Emergency Communications (EMTEL);
Requirements for communication between
authorities/organizations during emergencies**

Reference
RTS/EMTEL-00049

Keywords
emergency

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 Specification (TS) has been produced by ETSI Special Committee Emergency Communications (EMTEL).

The present document is one of several deliverables covering the communication needs of citizens and authorities in emergency situations, as identified below:

- ETSI TR 102 180 [i.1]: "Basis of requirements for communication of individuals with authorities/organizations in case of distress (Emergency call handling)";
- **ETSI TS 102 181 (the present document): "Requirements for communication between authorities/organizations during emergencies";**
- ETSI TS 102 182 [i.3]: "Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies";
- ETSI TR 102 410 [i.4]: "Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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

The present document outlines the requirements for communications between emergency authorities, and the need for standardization in this area to support these requirements. These communications are considered of three types:

a) speech communications between emergency staff members;

b) data communications allowing them to exchange information such as pictures, schemas, files, videos; and

c) IoT communications where physical and virtual "things" have identities, physical attributes, virtual representation, use interfaces to be integrated into the information network where they support the actions of the emergency authorities.

Clause 4 describes the relations between authorities in general terms defining each authority. Clause 5 categorizes the emergency services communications requirements. Clause 6 discusses the scalability and priority issues, including the dynamic need to employ resources. Clause 7 outlines the requirements applicable to the network(s) and user services, describing the services and the network features and capabilities. Clause 8 raises a number of security considerations. The annexes describe additional operational considerations, which may be useful as a background but do not constitute part of the communication requirements.

1 Scope

The present document addresses the requirements for communications between the authorized representatives who can be involved in the responses and actions when handling an emergency.

It describes the functional requirements for communications between the authorized representatives involved in the responses and actions when handling an emergency. The level of precision has been chosen to avoid interaction with the specific local, regional or national organizations and diagrams of relations between authorized representatives. It follows from this that adaptations will have to be done when implementing the present document at a local level. Furthermore, the scope of the present document also encompasses various types of services that can bring an added value to this basic scenario or add new scenarios, such as the services brought by other technologies e.g. IoT devices that support communications between authorities during emergencies.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

[1] Void.

[2] Recommendation ITU-T E.409 (05/2004): "Incident organization and security incident handling: Guidelines for telecommunication organizations".

[3] Recommendation ITU-T G.114 (05/2003): "One-way transmission time".

[4] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[5] Void.

[6] Recommendation ITU-T E.106: "International Emergency Preference Scheme (IEPS) for disaster relief operations".

[7] 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.

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

[9] ETSI TS 122 280: "LTE; Mission Critical Services Common Requirements (3GPP TS 22.280)".

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 TR 102 180: "Emergency Communications (EMTEL); Basis of requirements for communication of individuals with authorities/organizations in case of distress (Emergency call handling)".

[i.2] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

[i.3] ETSI TS 102 182: "Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies".

[i.4] 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.5] ETSI TR 103 582: "EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations".

[i.6] ETSI TR 102 299 (V1.4.1): "Emergency Communications (EMTEL); Collection of European Regulatory Texts and orientations".

[i.7] ETSI TS 103 479: "Emergency Communications (EMTEL); Core elements for network independent access to emergency services".

[i.8] C(2003)2657 Commission Recommendation of 25th July 2003 on the processing of caller location information in electronic communications networks for the purpose of location-enhanced emergency call services, published on O.J.E.U. L 189/49 the 29.7.2003.

[i.9] ETSI TS 103 260-1: "Satellite Earth Stations and Systems (SES); Reference scenario for the deployment of emergency communications; Part 1: Earthquake".

[i.10] ETSI TS 103 260-2: "Satellite Earth Stations and Systems (SES); Reference scenario for the deployment of emergency communications; Part 2: Mass casualty incident in public transportation".

[i.11] IETF RFC 3261 (June 2002): "SIP: Session Initiation Protocol", J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler.

[i.12] IETF RFC 7852 (July 2016): "Additional Data Related to an Emergency Call", R. Gellens, B. Rosen, H. Tschofenig, R. Marshall, J. Winterbottom.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 102 180 [i.1], ETSI TR 103 582 [i.5] and the following apply:

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

authorized representative: individual officer or institution authorized by public service (fire, police or health) to play a key role in handling of an emergency case

emergency control centre: facilities used by emergency organizations to handle rescue actions in answer to an emergency call

NOTE: A PSAP forwards emergency communications to the emergency control centres.

emergency number: special short code(s) or number(s) which is used to contact the PSAP to provide emergency services

NOTE: The emergency number is used by the emergency caller to request assistance from the emergency services. There exist two different types of emergency numbers in Europe:

1) **European emergency number, 112:** unique emergency number for pan-European emergency services and used, for example, in EU member-states, Switzerland and other European countries.

2) **National emergency numbers:** each country may also have a specific set of emergency numbers.

emergency response organization: organization providing response to disaster situations, e.g. the police, fire service and emergency medical services

emergency service: service, recognized as such by the member state, that provides immediate and rapid assistance in situations where there is a direct risk to life or limb, individual or public health or safety, to private or public property, or the environment but not necessarily limited to these situations (see Commission Recommendation C(2003)2657 [i.8])

fleetmap: parameter information programmed into the system infrastructure and into the subscriber radios to control how the radios will behave on the system

incident area: area where the incident occurred, and/or the area which needs communication coverage to manage the response implemented

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 (from ETSI TR 103 582 [i.5])

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 or infrequent in transmission. The number of connected IoT devices is set to exceed the number of conventional devices such as computers, tablets and fixed line/cellular phones.

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 or connects to one or multiple sensors and actuators to interact with its deployment environment (from ETSI TR 103 582 [i.5])

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

IoT platform: 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. (from ETSI TR 103 582 [i.5])

NOTE: 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.

location information: data processed in a public mobile network indicating the geographic position of a user's mobile device or of an IoT device, and data in a public fixed network indicating the physical address of the termination point (see Commission Recommendation C(2003)2657 [i.8])

originating network: network from which the emergency communication was originated

3.2 Symbols

Void.

3.3 Abbreviations

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

C&C	Command and Control
CBRN	Chemical, Biological, Radiological or Nuclear
COP	Common Operating Picture
CQI	Call Quality Index
D2D	Device to Device (communication)
DGNA	Dynamic Group Number Assignment
DMO	Direct Mode Operation
DMR	Digital Mobile Radio
EC	European Commission
ECC	Emergency Control Centre
EECC	European Electronic Communications Code
FIFO	First In, First Out
FR	First Responders
GDPR	General Data Protection Regulation
GoS	Grade of Service
GSM	Global System for Mobile telecommunications
GSM-R	GSM-Railway
IEPS	International Emergency Preference Scheme
IoT	Internet of Things
IP	Internet Protocol
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
LEMA	Local Emergency Management Authority
LMR	Land Mobile Radio
MCPTT	Mission Critical Push To Talk
MCX	Mission Critical X

NOTE: With X = PTT / Video / Data.

MTA	Mass Transportation Accident
NCSA	National Communication Security Authority
NGO	Non-Governmental Organization
PLMN	Public Land Mobile Network
PMR	Professional Mobile Radio
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTT	Push To Talk
QoS	Quality of Service
RF	Radio Frequency
RP	Reference Point
SIP	Session Initiation Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
TETRA	TErrestrial Trunk Radio Access
UAV	Unmanned Aerial Vehicle
VHF	Very High Frequency
VoIP	Voice over IP
VPN	Virtual Private Network
VTC	Video TeleConferencing

4 Relations between authorities

4.0 Introduction to the functional architecture

The type and number of the authorized representatives in a given situation usually directly depend on the nature of the emergency. In the most frequent cases, only people on duty have to intervene according to a day-to-day routine, but in some cases, crisis teams or temporary headquarters will be called. In accordance with a plan, the additional resources will organize a mass action gathering and, if needed, include the resources of several centres, or even include in the rescue plan additional levels of administrative authority, private operators and associations. These new authorized representatives will follow instructions or orders from the administrative crisis authority (also called Local Emergency Management Authority); for example, utilities companies (water supply, transport, energy, etc.) may have to stop the provision of service, install priority of service schemes or execute a coordinated schedule for the restoration of the infrastructure and the service, as applicable.

It is recognized that the public authorities keep the responsibility of overall management of actions during the duration of the crisis, establishment of pre-planned scenarios and, in specific locations e.g. tunnels, underground transports, plants with high level of risk, organization of field exercises involving all these authorized representatives.

Figure 1 illustrates the relations (or Reference Points, RP) between these authorities illustrated as functional entities, and shows them when involved in routine and exceptional emergency situations.

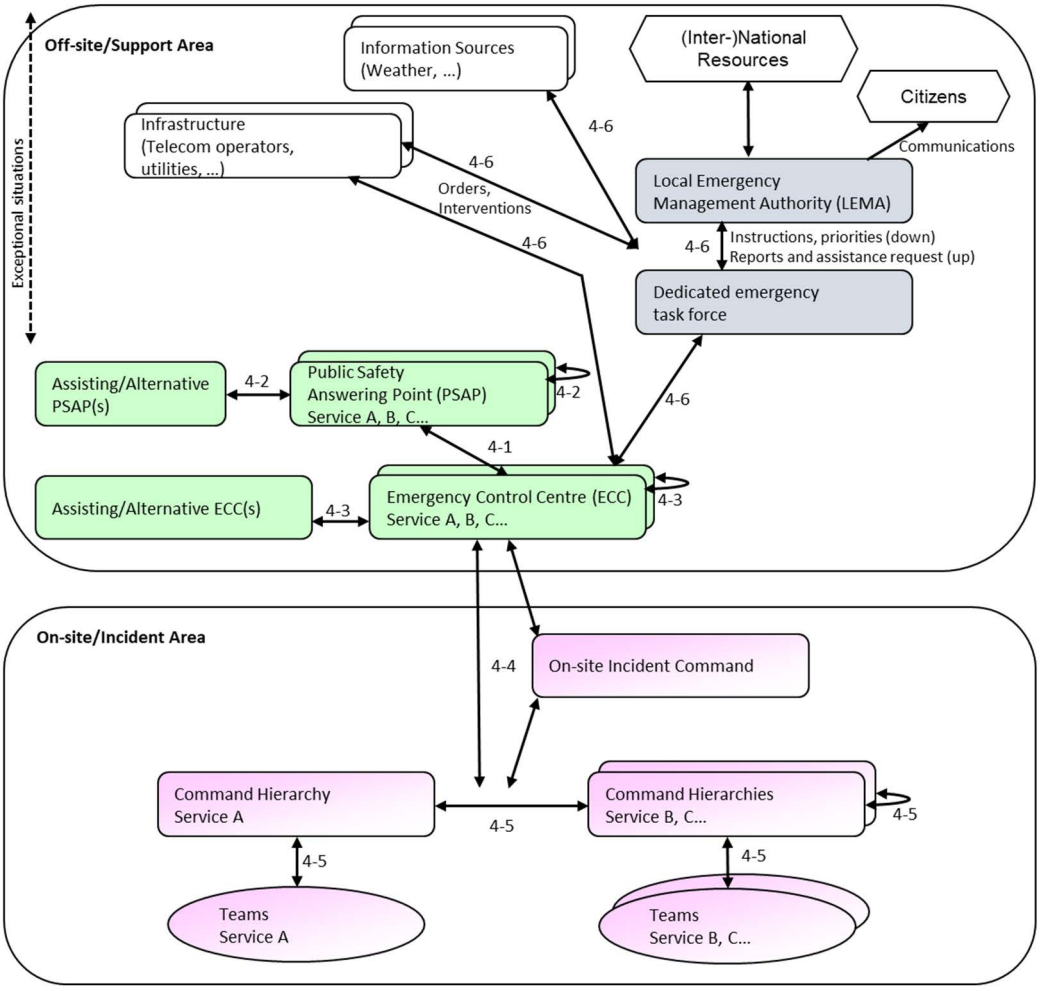

Figure 1: Reference points between functional entities

The description of the type of relations provided in the next clauses relies on the model illustrated in Figure 1. These relations correspond to the requirements from a user point of view. PSAPs/emergency control centres and rescue services (First Responders, FR) in the field may be organized differently in different countries, e.g. in Sweden the PSAP and control centres for medical services and fire are combined, whereas police have their own control centres (to which calls are transferred from the common PSAP).

NOTE: Relations involving the military agencies (described in clause 4.7) are not shown in Figure 1.

The temporary task force for coordination may be a pre-defined group which is activated according to set of criteria, e.g. kind of emergency (landslide, earthquake, etc.), number of casualties, need for resources, etc.

Decisions to be taken by the emergency management entities require a comprehensive situation overview which is known as Common Operating Picture (COP). Enhanced digital technologies such as the Internet of Things (IoT) and drones are also used by authorities to improve their situational awareness, monitoring and response during incidents. The IoT includes physical devices, sensors within or attached to these devices, but also smart services and applications. IoT technologies and drones are thus contributors to the collection, aggregation and distribution of the global COP data. More details can be found in ETSI TR 103 582 [i.5].

Figure 2 shows how and where IoT can support communications between authorities. 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. An example is a FR personnel equipped with wearables such as biometrics, audio and video sensors or supported by a drone. The real-time audio and video transmissions may be used by other team members or by the emergency control centre in order to collect more data to assess the situation.

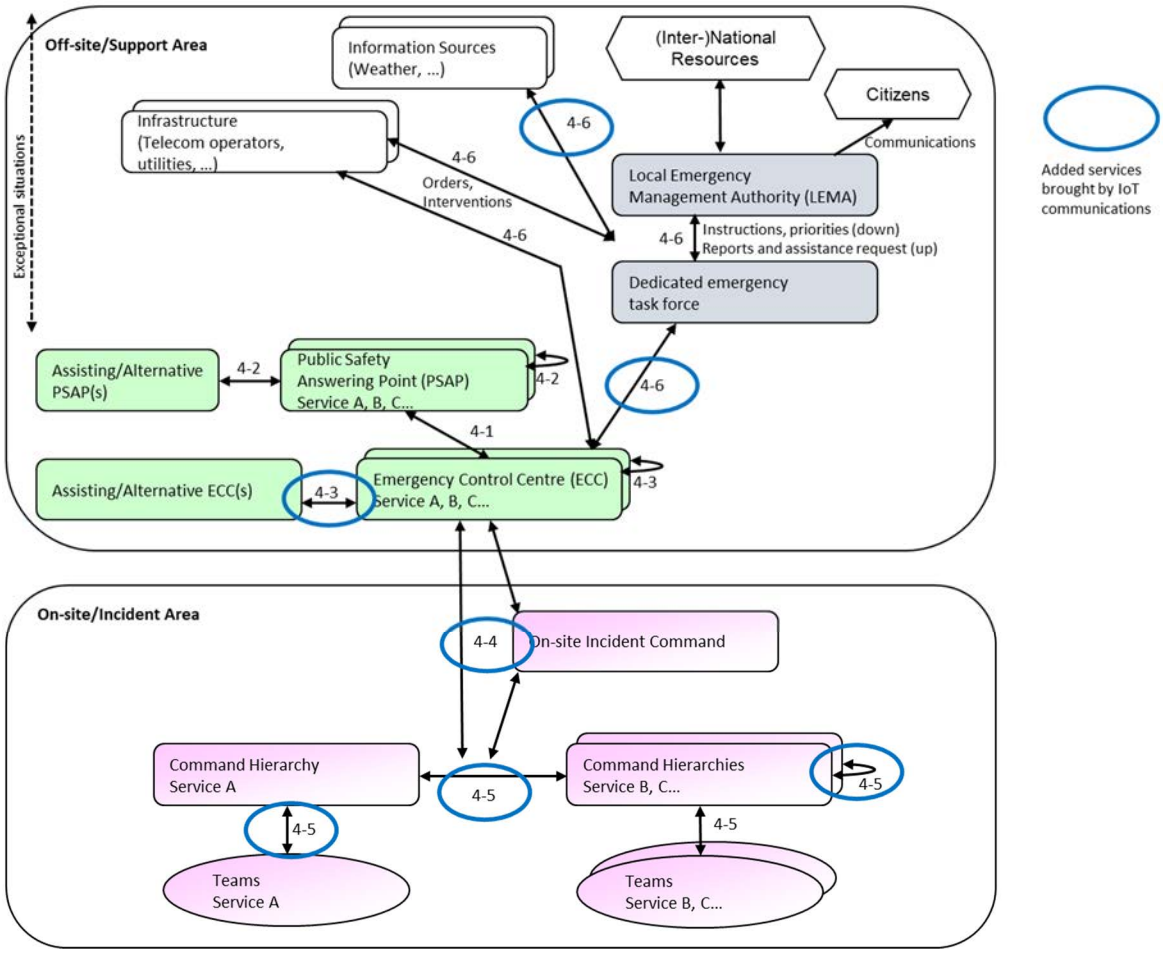

Figure 2: Additional services brought by IoT to functional entities

The requirements in the present document cover both public and private networks. However, the implementation of all the requirements may not be possible in both types of networks.

4.1 Relation between PSAP and Emergency Control Centres

PSAP and emergency control centres are two different functionalities that may or may not be integrated.

The PSAP shall, after reception of an emergency call and without delay, communicate with the competent emergency control centre and transmit the location and nature of the emergency of the calling party, along with any other relevant information that may be available associated with the call.

4.2 Relation between PSAPs

PSAPs normally work independently from each other, however, there are cases where cooperation would be needed between two PSAPs, especially in case of cross-border events. In a single country, PSAPs of different regions can be interconnected. If no operator is available, the communication can be redirected to another PSAP. Across countries, a PSAP may receive an emergency notification for an event happening in a bordering country.

In cases where communications arrive at a PSAP other than the one responsible for the area where the communication originated (e.g. mobile phones in the bordering area between different PSAPs), the communication may be transferred to the other PSAP, together with additional information (e.g. location data).

The requirement depends on operation rules which have been established for these types of situation. Such rules may state that:

- the communication is handled by the receiving PSAP;
- the communication is immediately transferred to the PSAP appropriate for the incident area; in such a scenario the location data shall be made available to the PSAP handling the incident, as for any received communication;
- depending on local procedures, the receiving PSAP may transfer the communication directly to the relevant ECC, possibly together with information about the correct PSAP that the communication has been transferred to.

The PSAPs or their organization shall be responsible to pre-define these rules of procedures.

A PSAP-Directory hosted by CEPT-ECO is available to facilitate inter-PSAP communications in Europe, in compliance with the requirements in the European Electronic Communications Code, EECC) entered into force on 20 December 2018 (see ETSI TR 102 299 [i.6]).

4.3 Relation between Emergency Control Centres

ECCs shall have the facilities to collaborate with other ECCs either within the same service or across services (e.g. fire and health).

Examples of cases where this is needed:

- Communications are forwarded to an inappropriate ECC: The communication shall be transferred to the correct ECC together with additional information (e.g. location data).
- Cases involving more than one ECC, e.g. fires with risks for human lives which typically involve fire, health and police, CBRN incidents (or suspected incidents), terrorism.
- Communication facilities exist to integrate the resources from two or more emergency control centres, in case of a larger emergency situation (see Figure 1).

Communications between ECCs shall be able to:

- Establish communication connections to support a number of services, including speech and (IoT) data.
- Support (video) conference calls including external resources that may be set up and kept over a substantial amount of time. In contingencies, calls to external resources may be required.
- Support exchange of data, such as files, images, video, instant messaging, emails.

- Support the exchange of IoT data, either manually or automatically (see clause 5.3.2.3).

4.4 Relation between Emergency Control Centres and mobile rescue teams/agents

Access to permanent bidirectional connections between Emergency Control Centres (ECCs) and their mobile teams is crucial in the handling of emergencies and shall be available for the duration of the emergency/disaster. The ECC may also be able to receive data information directly from the mobile teams, their supporting IoT devices, or from drones.

The main speech communication needs of the mobile rescue teams, representing the emergency services can be categorized as follows:

- specialized functionality in group communications and dispatching, with instant connection and including appropriate security, dynamic management of talk groups and more generally communication groups, emergency calls, prioritization of communications, etc.;
- call establishment times; voice call set-up time shall be in the range of 0,3 s to 1 s.
- seamless radio coverage throughout the area affected by the incident itself and the areas of operational activities associated to the incident (rescue facilities, hospitals, etc.) - including means to maintain communication during network outage;
- incident capacity; the need for radio capacity increases during major incidents and accidents. Efforts shall be made to ensure as far as possible that sufficient communication facilities are available;
- speech quality sufficient to not impair the understanding of the message;
- controlled access to the network, using functionalities such as assigning priority to potential users, thereby restricting some parties from access to the network under certain circumstances.

The main data communication needs of the mobile rescue teams can be characterized as follows:

- a bandwidth and real-time capability sufficient to proper exchange video streams, VoIP, and different kinds of data, including IoT data;
- the support of group communications to share data in the same manner as for speech;
- the interoperability of the tools used by the mobile teams and the ECC;
- the security and privacy of the communications.

These communications shall facilitate the following aims:

- managing the teams and operational coordination;
- communicating between involved parties (mobile team members, control centre staff, receiving and assisting units/institutions);
- locating and monitoring the attributes of the elements of the mobile teams;
- reassessing on a continuous basis the overall situation and the priority of the missions;
- enabling the reporting from the teams;
- enabling the teams to call for additional support and resources from self and external emergency teams.

The above requirements are fundamental factors for the efficiency, the safety and survival of the victims of the incident as well as for the rescue agents themselves.

These actions remain the responsibility of a variety of public authorities, but it should be mandatory that technical systems provide solutions for all the above requirements. Technology provides tools to improve the effectiveness and efficiency when handling the tasks and procedures. It can never replace the responsibility of the authorities and the correct application of their agreed procedures in the event of an incident.

The need for radio coverage, instant access (network capacity), reliability and specialized communications facilities such as all informed net (group call) and fast communication set-up, is normally considered best served by the use of a solution consisting of a private radio and fixed communications system, shared by several independent authorities. It can also be served by using the relevant features of a PLMN providing MCX (MCPTT/MCData/MCVideo) communications. Risk assessments, together with moves towards cross-services and international collaboration, have led to an emphasis on interoperability between various services. For this collaboration to be efficient, the communication systems in use shall be interoperable. This requirement extends to any other type of data network supporting the needs of the rescue teams.

4.5 Relation between mobile rescue teams/agents

To work efficiently when handling a larger incident, mobile rescue teams need facilities for communication with other mobile rescue teams involved in the same incident. The need is for communication across the services involved, as well as within each service. These communications shall facilitate the following aims:

- managing the teams and operational coordination between teams;
- communicating between team members;
- reassessing on a continuous basis the overall situation and the priority of the missions;
- enabling the reporting within the teams;
- enabling the teams to call for additional support and other resources;
- exchanging information for guidance of the staff involved in the incident and assessment of the injuries and preparation of fixed rescue facilities before arrival of casualties.

Interoperability between the communication systems in use is a pre-requisite for the efficient handling of the emergency. Fallback communication service shall be available to the mobile rescue teams for cases where network service is either unavailable or disturbed due to the nature of the emergency/disaster.

4.6 Relation between Special Task Force/Command Centres and permanent entities in special conditions

For their efficient work in handling emergencies, special task force or command centres and emergency control centres depend on permanent access to bidirectional connections or data communications with the mobile rescue teams and other operational entities. This access shall be available for the duration of the incident/disaster.

There is a basic need for configurable communications to fulfil the needs for handling of potential incidents that are identified. This includes escalations from local incidents to regional/national/international disasters.

4.7 Relation between military authorities and civil authorities

Military forces are routinely used to support emergency services and such involvement may take place in three types of scenario:

a) during major national emergencies where military authorities provide manpower and equipment to supplement public safety resources. These incidents are frequently in response to natural forces e.g. flooding, earthquakes;

b) for pre-planned support to public safety organizations during planned major event e.g. Olympic games;

c) in response to man-made emergencies e.g. terrorist incidents where specialist military skills or equipment are necessary and may form an integral part of the emergency response.

5 Emergency services communication requirements

5.0 Introduction

While the nature of an emergency may vary greatly, the communications services which may be required by authorities is easier to define, although there may still exist disparity in geographical area, scale and the number of authorities involved in any particular emergency (see annex B). This clause describes mandatory communications services, together with other services which may be necessary or beneficial to users in some scenarios.

5.1 Methodology to determine the communication requirements

The great variety of emergency situations and events can be combined with the possible ways of their organizational and technical handling. This results in an extraordinary large number of different scenarios for which baseline requirements are laid down in the present document. However, the associated criticality and probability of occurrence of these scenarios may be very different. Therefore, it is strongly recommended for authorities to carry out a risk analysis of each scenario and define the priority of handling for these scenarios. The procedures and actions required to be taken for handling the scenario shall be measured depending on the associated criticality, risk and probability of the scenario, taking into account the costs and resources required for their realization. When the probability of occurrence of a scenario is marginal, and its criticality is not high, the prescription of mandatory requirements may not be justified.

To present the requirements in the scope of the present document, a methodology has been chosen based on the following steps:

- identification of types of actions to be performed during the handling of the emergency case;
- if applicable, identification of the relations involved for these actions;
- identification of generic telecommunication or information exchange services which can help to perform these actions;
- identification of typical telecommunications services and overlying applications likely to be used in performing these actions;
- tentative combination of the above lists to illustrate a practical application.

It should be noted that the above methodology is not the unique way to handle the subject. It did, however, appear appropriate to prepare a document enabling to approach the variety of situations encountered in reality. It is clear that no unique document can fix the detailed requirements of a given team or entity working in a unique social, geographical, administrative and economic environment.

An alternate methodology would be to examine the historical communication requirements from previous emergencies. While this method is being undertaken to provide a guide of services used, it recognizes that communications between authorities during emergencies in the past was sub-optimal. Similarly, an historical evaluation cannot in itself identify all future requirements.

5.2 Actions that require communications

Communication requirements for emergency services shall be concerned with ensuring that the required information is available to the correct person or organization at the appropriate time.

In essence, communications shall be timely, relevant and accurate for all actions that may be undertaken.

Examples of situations requiring such communications are provided below:

- Mobilization of resources.
- Pre-informing related authorities of the services required from them e.g. informing hospital services of arriving casualties and their needs.

- Relay of command and control information to the incident area, either through voice (speech) calls, instant messaging or video conferencing.
- Request and receipt of information from specialist sources where abnormal hazards are involved e.g. hazardous materials, biological agents, etc.
- Transmission of images (still pictures and video) and sensor data from an incident to a central command point for monitoring purposes.
- Transmission of updated information on the state of the incident and status of actions to the ECC and to other forces at the site of the incident.
- Transmission of control information from ECC to the emergency location. This may involve point to point, point to multi-point (multicast) or broadcast communication services and may directly address IoT actuators.

5.3 Required communications services

5.3.1 Speech and conversational voice services

5.3.1.0 General requirements

Speech and conversational voice services are often the most instinctive and most used communication services in emergencies. This clause does not imply that a particular technology or switching mechanism be employed in the provision of speech services. Speech services may also be brought by VoIP technologies.

For speech services there exist several universal requirements, characterized by:

- **Speech intelligibility:** that received speech is capable of being understood reliably, this is required even in the presence of high levels of background noise and/or when personnel are under stress or exertion.
- **Call setup-time:** short call set-up times enable rapid communication of relevant information. Communication mechanisms which require unacceptably long call set-up times may endanger life, or users may resort to setting up a connection before it is necessary and keeping it connected when not required in order to avoid an unacceptable delay when communication is required.
- **End to end latency:** in addition to the delays noted for call set-up times, it is recognized that where a duplex voice communication system imposes an end to end latency of over 500 ms, there is a degradation in the communicability of the users (Recommendation ITU-T G.114 [3]). ETSI TS 122 179 [8] specifies for the MCPTT service a Mouth-to-ear latency requirement as the time between an utterance by the transmitting user, and the playback of the utterance at the receiving user's speaker.
- **Speech quality:** although the prime attribute for a speech service in most emergencies will be intelligibility, there are cases where high speech quality is desirable. These cases may be when liaising with authorities or organizations unused to public safety communications e.g. external specialists; or where a level of trust is required to be established, e.g. NGOs, community groups.

Speech services may require prioritization and pre-emption of calls. The implementation of such features will be dependent on the technology employed, and the use of such features will be determined by procedure and organizational systems.

Underlaying networks should have the capability to handle prioritized calls correctly, including the capability to pre-empt unprioritized calls. Transit networks should convey priority related signalling in order to support end-to-end priority.

5.3.1.1 Point to point speech services

Point to point duplex voice communications are required for many instances to provide communications, particularly between different authorities e.g. between commanders of different emergency services, or between emergency service staff and external specialists.

5.3.1.2 Group speech services

The use of group speech services of various types is well established in all fields of public safety, although these services are frequently only provided with one service and/or users from one geographical area.

During emergencies the same communication services will be required, but the personnel utilizing them may differ. There will be a requirement in some cases to form groups containing members from multiple services and/or multiple geographic units.

Sufficient interoperability should be provided by systems to support group services across multiple networks, whichever their technology (e.g. TETRA, cellular, MCX, etc.). Group members may be drawn from different services and be issued with different communication terminals. Mechanisms to support dynamic creation of multi-service teams are desirable.

Group services may for example consist of several mobile rescue teams for an unlimited period of time and are required to be in a permanent relationship. Or it may consist of several mobile rescue teams for a limited period of time and require a simple procedure to form a relationship, for as long as it is required.

Each individual may belong to one or more teams. It should be possible for the individual user to identify which group(s) is/are active at any given time. To facilitate this, one or more of the following example services may be utilized:

- **Talk group:** point-to-multipoint (or multicast) communication addressed to a group of individuals, established within a selectable predefined area. The coverage is associated to the group number and may be different from the total coverage. Resources shall be allocated all the time. Any concerned user may enter or leave the talk group at any time.
- **Emergency services call (authority to authority):** on a user action, a status shall be sent by the terminal. Two options shall then be possible (as an operator option):
  - Automatic call set-up of a pre-emptive open channel.
  - Using a pre-emptive priority, a predefined user (e.g. ECC) shall establish a call chosen on an operational basis.

  EXAMPLE: Open channel, ambience listening, individual call.
- **Ambience listening:** this functionality shall enable a dispatch position to switch an individual piece of equipment into transmitting mode without any indications being noticeable at the piece of equipment itself that it is transmitting. The capability to activate this functionality shall be restricted only to an authorized user.
- **Intrusion:** this service shall allow an authorized user to intervene in an ongoing authority-to-authority call.
- **Priority call:** this service shall allow a call to proceed before any other call with lower priority. The priority level can be assigned according to various criteria.
- **Dynamic group number assignment:** this service shall allow a served user or an authorized user to create, modify and delete a group (dynamic regrouping/group merging).

5.3.1.3 Push To Talk (PTT)/Command and Control (C&C) features

Especially in emergency situations it is necessary to avoid network congestion. Even in case of high traffic on the network, communication between individual users (point-to-point) or existing or ad-hoc user groups (point-to-multipoint) PTT has to be enabled. It shall be possible to add and remove users from the communication group dynamically during the session.

Communication should require as little bandwidth as possible. This holds especially for emergency communications characterized by many short speech items transmitted between talk group members over a certain period of time (e.g. giving and receiving instructions in C&C communication).

To facilitate this simplex communication, services like Push To Talk (PTT) can be used. PTT helps to avoid network congestion by transmitting voice over a data channel and thus can be used even in times of high traffic on the communication network. Furthermore, PTT provides flexible management of user groups.

5.3.2 Data services

5.3.2.0 General requirements

Data services are used to provide a large number of applications which can have widely differing requirements in terms of capacity, timeliness and robustness of the data service.

Sufficient data bandwidth, in both fixed and wireless networks, shall be provided to support a wide variety of data applications required for emergency telecommunication purposes. These applications shall benefit from the ubiquitous coverage brought by wireless networks.

Ideally, the data transmission rate shall support the required data throughput and minimize end to end delay, especially for applications such as real time video. Noting the extreme circumstances which may be in force during an emergency, it may be desirable for networks to degrade gracefully when user requirements exceed the agreed levels of service.

Wireless data transmissions may be subject to packet loss when the radio coverage is not of sufficient quality. The quality of the service shall be ensured to guarantee the reliability of the data services.

As authorities may use the data applications under high mobility scenarios, seamless connectivity and real-time capability of data communications shall be ensured to support these services.

Table 1 shows the requirements of diverse data applications. Where data applications share the use of a data transmission capability, provision of sufficient capacity and effective management shall be provided to ensure that application data is communicated appropriately.

Table 1: Requirements on data applications

Service	Throughput	Timeliness	Need for preservation of data integrity
Email	Medium	Low	Low
Imaging	High	Low	Variable
Digital mapping/ Geographical information services	High	Variable	Variable
Location services	Low	High	High
Video (real time)	High	High	Low
Video (slow scan)	Medium	Low	Low
Data base access (remote)	Variable	Variable	High
Data base replication	High	Low	High
Instant messaging	Low	Medium	High
Personnel monitoring (IoT)	Low	High	High
Interactive applications	Variable	High	High
Sharing incident information	Medium	High	High

Throughput: data volume in a given time.

Timeliness: importance of the information arriving within an agreed timeframe.

Preservation of data integrity: how (reliable) free from bit errors the information transmission needs to be.
E.g. a bitmap image with some errors is still useable, a jpg image with some bit errors may be unreadable.

Some applications may be used with dedicated communication assets which will be tuned to the particular needs of that application, although interfaces may be necessary to exchange data from such dedicated systems with other applications e.g. screen capture one frame from dedicated video transmission equipment and email the resulting still image. Where appropriate, such applications should be based on appropriate standards to facilitate information exchange.

Communications between authorities are highly sensitive. Security shall be ensured, more specifically in terms of confidentiality (with encryption for example), authorization, authentication, etc. This is further detailed in clause 8.

Specific applications are listed in the following clauses.

5.3.2.1 Paging Services

Paging services are used by a variety of authorities in order to contact their personnel, and paging services are available from a variety of networks and technologies. The network shall be able to identify the requested authorized emergency agent(s), and then deploy the appropriate technology to contact them. This requirement may encompass different communication network technologies, services and applications such as paging, presence, texting, instant messaging, etc.

5.3.2.2 Video Teleconferencing (VTC)

VTC or conversational video may be required to enable effective coordination between services at a command level or below. VTC services may be utilized to provide reconnaissance information from the incident back to control rooms. VTC communications shall comply with both speech quality and video services requirements.

5.3.2.3 Group video and data communications

Data services such as Instant Messaging or video streaming may be shared as a group service. This allows individuals and teams to work in real time with up-to-date information. Specific requirements for handling these group data services shall match the requirements specified in clause 5.3.1.2 for group speech services.

5.3.2.4 Communications involving IoT devices

Communications involving IoT devices enable status monitoring and include a wide variety of parameters, e.g. breathing air tank levels, accountability monitoring, distress buttons and vital signs monitoring (see ETSI TR 103 582 [i.5]).

Communications involving IoT devices in emergency situations can leverage from the expected benefits of the IoT:

- Data gathering without human interaction.
- Objectivity of IoT data.
- Fast and fail-safe information sharing.
- No translation of human languages required.
- Real-time data transmission.
- Operation in dangerous environments.

Furthermore, emergency services teams may be able to access pre-deployed IoT devices belonging to external bodies such as utilities, building managers, etc. to improve their awareness of the event situation. For example, firefighters may be able to access smoke/heat detectors, surveillance cameras, but also communication devices in elevator cabins.

Communications involving IoT devices have specific challenges, for example potentially a large number of devices, automated data collection, constrained devices, fragmentation of communication standards impacting interoperability when used to exchange information between authorities, which shall be handled when used by emergency service teams.

5.3.2.5 Location services

Location services provide real-time information regarding the position of personnel or vehicles to a command point. These services may also include status information regarding the person or vehicle. They may require frequent transmissions to update position; the amount of data transmitted is likely to be small when location is based on satellite-based solutions, but can be quite extensive when location is to be calculated inside buildings as other technologies may have to be used. Location reporting services may be one-way with no acknowledgement, necessitating a robust communication mechanism. Position information may be considered sensitive in some emergencies and may require security mechanisms to protect the data.

5.3.2.6 Sharing incident information

Emergency calls that are further routed between PSAPs (see clause 4.2) or forwarded to ECCs (see clause 4.1) may convey incident or other additional data that can be shared with emergency authorities and responders. The emergency calls interface is based on the SIP protocol with multimedia capability (see ETSI TS 103 479 [i.7] and IETF RFC 3261 [i.11]) and conveys additional data, by reference or by value, related to the caller, the call or the location as specified by IETF RFC 7852 [i.12].

5.4 Interoperability of communication services

Voice communication services are generally possible across heterogeneous networks, although there may be loss of functionality where special features and services are available (see clause 5.3.1.2). Where different techniques are used for voice encoding there may be additional loss of intelligibility and quality due to the need to decode and re-encode the voice signals.

Data (used by applications in emergency scenarios may originate from multiple sources) needed in emergency situations may be used by multiple applications. Applications need therefore be able to communicate with one another and present data in a format which is understandable and useable by other applications, especially the data semantics.

EXAMPLE: Situational awareness applications may benefit from inputs from other systems e.g. aircraft movement, automatic vehicle location, room temperature, maritime distress systems, etc.

A high level of interoperability between different systems and applications, tested beforehand, allows information to be communicated rapidly, widely and effectively to all relevant parties.

5.5 Example application

The application selected as an example application is the management of several field teams in an emergency situation requiring different expertise's.

The needs are supposed to be limited to one specific area.

They can imply the following relations (see reference points in clause 4.0):

- RP 4-1 (PSAP to ECC);
- RP 4-3 (coordination between different ECCs);
- RP 4-4 (ECCs with rescue teams); and
- RP 4-5 (between different rescue teams).

It may be necessary to have relations of type 4-2 (coordination with other PSAPs) depending on the size or the location of the event.

The type of actions required cover mainly:

- Mobilization of resources.
- Transmission of updated information on the status of the action.
- Pre-informing hospital services etc. of arriving casualties and their needs.
- Transmission of data from an incident to the emergency control centre.
- Real time coordination of actions between the different teams.

The relations-actions matrix can be developed in order to explain what kind of services should be provided through the communications system. Whereas RP 4-1, RP 4-2 and RP 4-3 type of relations may be handled through fixed lines, 4-4 and 4-5 services shall be mobile and on a wireless system.

An example of the full analysis is given hereunder; the resulting matrix can be used in a procurement process as the basis for preparing the terms of reference of the required system. One important point is to provide interoperability between different teams. The obvious solution to have a unique platform may not always be available; teams are then under different systems. The communication will then go through switching, connecting arrangements and data mapping between different systems; which in general reduces or forbids the capability to use a VPN between all actors, losing advantages of an easy interconnection.

Table 2: Relations-Actions matrix in the example application (illustrative)

Actions Relations	Mobilization of resources	Transmission of updated information - status	Pre-informing hospital services, etc.	Transmission of images and data to the ECC	Real time actions between different teams
RP 4-1	Yes	Yes	N/A	Yes	N/A
RP 4-2	Yes	Yes	N/A	N/A	N/A
RP 4-3	Yes	Yes	Yes	Yes	Yes
RP 4-4	Yes	Yes	N/A	Yes	Yes
RP 4-5	Yes	Yes	Yes	N/A	Yes
RP 4-6	N/A	Yes	N/A	Yes	Yes

6 Scalability

6.0 General considerations

Scalability is an important consideration, especially when the communications system (combination of networks) handles the escalation from a case involving e.g. one ambulance and one ECC, up to national involvement of multiple authorities (regional control centres, ministries, municipal authorities as well as local services).

To fulfil this objective, some descriptions may be useful:

- Contingency planning, see annex B.
- Organization of authorities in case of catastrophic event, see annex B.
- Emergency Preference schemes and traffic management, see clause 6.1.

Regarding IoT, one of the main features of IoT deployment is usually the large number of sensors and devices communicating with one another, thus the term often used: "massive IoT". The scalability of IoT devices mostly affects organizational challenges such as deployment, management and maintenance (see annex B).

6.1 Priority and preference schemes and traffic management

6.1.0 Introduction

The objective of rescuing injured or endangered people calls for arbitration of the emergency authority's representatives' access and use of shared, scarce (scarce or privileged) resources. Such schemes can be permanently assigned or activated only when the need arises in connection with the escalation of the disaster and a pre-organized contingency plan.

Additionally, in cases where the crisis event impacts a significant portion of the population, panic and the demand for information may raise the traffic demand on the communication networks to a level where the integrity of the network itself is put at risk. See Recommendation ITU-T E.409 [2] for information on the nature and scales of network resilience security threats and events to be planned against.

Priorities for certain types of calls and access to data services should be described in a comprehensive scheme, that enable priority or essential traffic to be maintained at the risk of allowing other types of traffic to be degraded. Such schemes require contingencies to be described considering a break down for regional or localized eventualities. These plans also require the protection of all essential stakeholders in the planned contingency, including the involvement of public national or regional authorities, representatives or emergency services, operators and secondary support organizations.

The model of an emergency preference scheme should serve as guidelines for the purpose of the foreseen risk, such a scheme may lead to the necessity of traffic management techniques by the network operators, to ensure that spare capacity is maintained to cater for the expected needs that may be foreseen for the continued support of essential and emergency services.

Professional radio communication networks are dedicated to emergency services and as such, traffic is guaranteed by default to the users (emergency teams and authorities) during the emergency.

6.1.1 Traffic management

In general, an emergency situation will not directly affect the infrastructure and the performance of communications networks. Nevertheless, situations may arise where either public networks, private networks, or both, are affected as part of the emergency.

In both cases, the additional bulk of traffic, caused by the crisis, can lead to congestions in the network or part of their networks. It then becomes a vital requirement that the network operator take measures to mitigate against the possible failure of their network. To obviate these consequences and to maintain the access to the network resources required by authorized representatives, in the exceptional time, the operators should be prepared to activate traffic management measures.

In general, such measures, taken for the sake of the interest of emergency communications, will require the decision of the administrative authority, to mitigate the concerns of users who lose access rights, and to nominate those whose traffic involved in the emergency situation is subject to protection.

However, measures to protect the integrity of the network may under normal times of exceptional load be employed by the operators on a purely statistical basis. On such occasions, handling of so-called Emergency Services Calls (see clause 6.1.2.3) may be protected against loss.

By definition, a private radio communication network designed for use in emergencies shall be dimensioned to handle the emergency team's high traffic, particularly in a small area. It shall be possible to dynamically configure the traffic management for the emergency location.

6.1.2 Emergency preference schemes

6.1.2.1 User driven solutions

A public safety 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. The reason why most communications networks have limited physical resources is because the additional cost to increase the size of communications networks to adequately handle abnormal traffic loads in emergencies cannot be justified. As a consequence, compromise solutions are needed.

EXAMPLE: Adaptive traffic management and emergency preference schemes.

Some examples of these user driven solutions for fixed and mobile, public and private, communication networks are given below.

NOTE: This may be used for private network/systems as well.

6.1.2.2 PSTN/cellular solutions

An example of a network access-based call preference scheme has two levels of control:

1) a basic national end-to-end call set-up protection of priority network accesses from restrictive transport and termination controls; and a further;

2) more severe regional protection of priority network accesses from restrictive originating network controls.

The basic functional requirement is for a preference scheme available, but not invoked, on all fixed network accesses to provide an enhanced probability of achieving successful completion of the communication attempt to the destination across all networks, for nominated network accesses of essential users. Normal call unsuccessful conditions permitting (busy, no answer, etc.) the requirement is for the protection of the call set-up and call delivery to the point of termination. This capability shall be available nationally, across all networks on a licensed equitable basis.

The state of network access-based call preference scheme is always available, but under normal conditions not activated. Once activated, the registered network accesses of nominated essential users shall automatically invoke the enhanced network access-based call preference scheme whenever a call is placed. Network management controls shall activate and deactivate the service and register the network accesses of nominated essential users.

The more severe form of control protection of priority network accesses from restrictive originating network controls would be introduced only within parts of the network that are severely affected. This geographic form of control would be applied as a network protection and severe form of a network traffic management measure. However, the case of network failure/disaster cannot be foreseen and clearly may not affect other networks. See Recommendation ITU-T E.409 [2] for information on the nature and scales of network resilience security threats and events to be planned against.

The escalation from an activation of the basic enhanced network access-based call preference scheme to the more severe localized level of the service shall also require network management controls. A procedure shall specify local escalation and de-escalation of the network traffic management measure.

NOTE: The network access-based call preference scheme provides priority service to the essential users nominated network access(es), it is not provided personally to the user themselves, as this adds immediate complexities.

Additionally, a user-based call preference scheme has two features:

1) a protected priority access code; and

2) a user-based validation platform.

The protected priority access code employs similar features to the protection priority of emergency communication access (Directive 2002/22/EC [i.2] on universal service and user's rights relating to electronic communications networks and services, see also ETSI TR 102 299 [i.6]) and the network access base call preference scheme. After subsequent user's request has been validated and authenticated, the terminating leg of the call set up may also employ the protection afforded to the network access base call preference scheme.

See International Emergency Preference Scheme Recommendation ITU-T E.106 [6] and interworking with national schemes.

Cellular systems used by emergency service teams and authorities shall apply similar priority access to network resources to nominated users (see also PMR solutions in clause 6.1.2.3).

6.1.2.3 Professional Mobile Radio (PMR) Networks

Professional radio communication systems, which are dedicated to emergency services, shall be dimensioned to handle the peak of traffic exclusively for them. Yet priority call shall be available to allow authorized users to intervene when needed.

To balance the needs(ed) between acceptable cost, available traffic capacity and an acceptable Grade of Service (GoS) in emergencies, a number of services and facilities are available on PMR networks designed specifically for public safety applications. Although these services and facilities are in fact the solutions used to optimize a network's performance in emergencies, specific names for these solutions have been adopted by the industry and often specified as user requirements, as described below. A large part of these requirements is also specified for the MCX services (see ETSI TS 122 280 [9]). These services are further described in annex D:

- call queuing when busy;
- dynamic traffic management algorithms;
- group call (commonly called "all in formed net" and "talk group call");

- pre-emptive priority call (Emergency Services Call);
- call retention;
- priority call;
- Direct Mode Operation (DMO). Device to Device communication (D2D);
- Dynamic Group Number Assignment (DGNA);
- ambience listening;
- call authorized by dispatcher;
- area selection;
- late entry;
- voice encryption.

Control rooms are expected to handle more than simply radio communication between groups and individuals. They also provide functionality across incident management, call taking, mapping, recording and teamwork, and they are usually composed of elements from multiple providers. They also typically process audio and video at the backend, and perform patching between voice calls, talk group/individual calls and other services. As a matter of fact, control rooms are accessing features and functionality beyond a regular first responder device, therefore, the following core features shall be supported by a control room interface accessing 3GPP MCPTT infrastructure:

- Patching talk groups or individual units from LMR/PMR to MCPTT.
- Combining all selected LMR/PMR and/or MCPTT talk groups into one super-group.
- Tracking locations of LMR/PMR and MCPTT subscriber units.
- Multiselect transmission (a control room transmits to several LMR/PMR and MCPTT talk groups at the same time).
- Viewing talk group participants and their presence.
- Text messaging.
- Recording of voice, data and video.
- Role- and user management functionality such as group combine, multiselect, private call, priority override, affiliation, dynamic group patching, parallel group calls on multiple talk groups, and PTT request queuing.

6.1.3 Interaction with the emergency call service NG112

Once the severe category of this enhanced network access-based call preference scheme has been activated, all network accesses should still provide access to emergency services NG112 (see ETSI TS 103 479 [i.7]). The network access-based call preference scheme will allow essential and non-essential users the ability to make NG112 calls and to access whatever parts of the network are still available.

The nominated network accesses of essential users will not get access to reserved resources, e.g. trunk reservation, as is the case of the emergency services themselves. This implies no additional network management overhead. Therefore, within the network access-based call preference scheme, network accesses will get a priority service handled similarly to the emergency services NG112, without access to reserved resources, but with the ability to terminate to any destination.

NOTE: The level of priority could therefore be seen as lower than that of the essential emergency services e112 themselves.

7 Requirements applicable to the network and user services, (services to support) and the network features and capabilities

7.1 Recognition and treatment of emergency services from the view of the service

7.1.1 Transmission quality

Apart from defining an appropriate minimum bandwidth that is needed to provide a specific emergency service, one of the most crucial problems that have to be solved is assuring a sufficient transmission quality. Depending on which communication channels are used and which services have to be provided, the requirements will vary widely between different systems.

Some of the most important quality parameters for connectivity and their significance for different communication services are discussed in the following.

High availability and reliability are desirable for any kind of connection (but are especially important for applications where the stability of the connection is crucial, such as continuous cardiac monitoring for rescue workers). In any case the restoration time (i.e. the time needed to restore the required QoS after a service disruption) of the connection should be kept as short as possible.

Though a low error rate is always desirable, for transmission of speech or data that is highly redundant or can be interpolated (like video streaming) the acceptable error rate can be considerably higher than for more sensitive data. However, for applications like cardiac monitoring, a very low error rate shall be guaranteed.

The time it takes to get information across a network (latency) is a parameter that is relevant to nearly all applications that use network connections, as high latency implies that the user will have to wait for the application to react to his actions. Voice calls may be considered special, as the latency itself is annoying but not necessarily a crucial problem. Human actors are fault tolerant and can deal with a certain degree of delay. However, the variation of latency for transmitted data packets (jitter) is particularly disruptive for voice calls as well as for other real-time applications like video monitoring or video conferencing as it will disturb the transmission of the data stream.

The dropping of data (packet loss) might cause a temporary failure of the transmission. Compared to data traffic, video streaming and voice traffic are quite robust to loss ratio. However, in data-oriented traffic (e.g. network connections using TCP/IP) the fact that some data packets did not reach their destination might cause the protocol to terminate the connection.

For speech transmission in emergency situations, there is often a trade-off between connectivity and call quality (that can be measured e.g. through the Call Quality Index (CQI)). Connectivity is often the more important factor as long as a certain minimum (baseline) call quality is provided.

EXAMPLE: Whenever a lot of users are trying to make voice calls in parallel (which is most likely to happen in case of an emergency), it will be more preferable to enable most of them to make calls below the baseline quality normally offered to them than to give high quality connections to a few of them while shutting out the others.

Human actors can deal with low quality speech e.g. by repeating their messages whenever they notice that the connection quality gets to poor.

For critical transmission, channels asking for best-effort services is definitely not enough. Especially real-time applications like video-streaming or voice over IP need a minimum QoS to be fully functional. For every communication service used by the authorities, it will be necessary to define a minimum transmission quality for speech and/or data that has to be available to ensure that the service can be provided properly.

NOTE: This may be used for private network/systems.

7.1.2 Ensuring conveyance of communications

Network operators shall make every reasonable effort to ensure the answering, inter-network forwarding and termination of inter-authority communications, including in exceptional circumstances such as crises, catastrophes, etc. Recommendation ITU-T E.409 [2] provides information on the nature and scales of network resilience security threats and events to be planned against.

Network operators should assign privileges to traffic according to decisions from proper authorities. Network management and QoS mechanisms shall ensure that inter-authority communications are not delayed nor disturbed due to network congestion.

Networks should have the capability to handle prioritized calls correctly, including the capability to pre-empt unprioritized calls. Transit networks should convey priority related signalling in order to support end-to-end priority.

7.1.3 Assignment of inter-authority communications to the appropriate authority

A fleetmap structure makes it possible for different groups of personnel to access department specific and common group structures.

Common groups across different authorities should be available to improve interactions in common operations.

Common groups should be able to include users from different networks, in order to facilitate both cross border operations and country specific operations.

All users shall be able to communicate with their respective ECCs and with each other. The ECCs should communicate with all users regardless of their position within the network by means of:

- Group calls.
- Individual calls.
- All kinds of mode of voice and data communication.
- Simultaneous voice and data.

Users from other departments and authorities should be able to access specific groups based on case-by-case admission authorized by their respective emergency centre. It should be possible to define groups limited to a geographical area.

An authority should be able to create and maintain dynamic groups, e.g. by "drag and drop" users in to the dynamic group and to distribute this information to selected users.

7.1.4 Preventing effects of discrepancies in coverage

7.1.4.1 PSAP routing in mobile networks

Due to physical uncertainty and variations of radio coverage limits, there are border effects where an Emergency Services Call is routed to the wrong PSAP. Attention should be given to all parties involved, and more specifically operators, when designing the network to limit the occurrence of such cases. Where these cases occur, cooperation of PSAPs/ECCs should be applied and organized as appropriate.

7.1.4.2 International cooperation

A situation similar to that described in clause 7.1.4.1 may appear near country borders: cross-border Emergency Services Call handling requires international cooperation between all involved parties.

7.1.4.3 Private networks technologies

Situation similar to those described in clauses 7.1.4.1 and 7.1.4.2 may be applicable as well to private networks that are connected through fixed-line networks.

7.1.4.4 Interworking of technologies

Different authorities and organizations may rely on different communication technologies for their field actions (e.g. analogue PMR, TETRA, Tetrapol, GSM-R, VHF Maritime frequencies, DMR and MCX). Attention should be given to ensure proper interoperability between such systems, not restricting the efficient cooperation between field personnel and the emergency centre in charge.

7.2 Recognition and treatment of emergency services by the originating network

7.2.0 Virtual network consideration

If a virtual network is established for emergency work, with subscribers in different networks, this may be an issue for consideration.

7.2.1 Communication-related information

7.2.1.0 Information forwarding

Information from the Emergency Services Call shall be forwarded along with the Emergency Services Call to any authority representative. Communication related information originated by an authority representative shall be transmitted on inter authority communications.

7.2.1.1 Indication of the (emergency) caller's location

Location information from the Emergency Services Call shall be forwarded along with the Emergency Services Call to any authority representative. Communication related location information originated by an authority representative shall be transmitted on inter-authority communications.

7.2.1.2 Identification of the mobile terminal equipment/subscription

Mobile terminal equipment/subscription identity information from the Emergency Services Call shall be forwarded along with the Emergency Services Call to any authority representative. Communication related mobile terminal equipment identity information originated by an authority representative shall be transmitted on inter authority communications.

7.2.1.3 Interworking of Technologies

Communication related data originated by any authority representative shall be transmitted on inter authority communications independent of the use of differing technologies, e.g. location information.

7.2.2 Network identification

Network identification information from the Emergency Services Call shall be forwarded along with the Emergency Services Call to any authority representative. Also, network identification information originated by an authority representative shall be transmitted on inter-authority communications.

7.2.3 Minimum power supply for authority representative user accesses

If feasible, fixed network operators should provide a minimum power supply at their network termination points. This minimum power supply should enable telephone terminal equipment connected to the network termination point to be operational in the case of a local power failure.

NOTE: Emergency authorities should establish their own policies for guaranteeing electricity supply for terminals, generators battery back-up, etc.

7.3 Requirements on call handling between networks

7.3.1 Handling of inter-authority calls between networks

Handling of inter-authority calls between networks shall be conveyed with the associated call priority information to alleviate the call from restrictive network management controls, as specified in clause 6.

7.3.2 Interworking with carrier selection/carrier preselection codes

Interworking with carrier selection/carrier preselection codes needs to be considered as authorities may choose to change supplier. This change shall not have an impact on the service operation and shall work in accordance to the applicable numbering plan.

NOTE: Recommendation ITU-T E.106 [6] Carrier selection may be overridden for international preference schemes.

7.3.3 Inter-authority communications from other countries

International assistance treaties commonly exist across local borders land/sea, e.g. France/Switzerland in the area around Geneva, UK/France in the Channel, UK/Norway in the North Sea, etc.

Call handling between international networks shall have the following functionalities:

- Integration into foreign talk groups.
- Contact with own dispatching unit (ECC).
- Emergency Services Call handling in foreign networks.
- Data transmission for status messages and automatic vehicle location.
- Individual call and phone call.

For call handling from other countries, the network shall provide the following services:

- The display on the handset showing the active network.
- Selection of the preferential network.
- Identification of group members.
- Use of DMO (Direct Mode Operation).

7.4 Providing termination of inter-authority calls for the relevant authorities

Any network directly connecting points of access to authorities should deliver the Emergency Services Call to the authority together with any related data, without undue delay or modification.

If the appropriate authority is not reachable, the call shall be forwarded to the alternative nominated authority.

Terminating networks to authorities should, if possible, meet the functional requirements as agreed, to ensure the continuity of the access to the authority, call diversion deflection, load balancing, etc.

The network operator shall protect the integrity and ensure the survivability of their network, according to nationally agreed objectives. This may be achieved by preventing any single point of failure within their network equipment. Recommendation ITU-T E.409 [2] provides information on the nature and scales of network resilience security threats and events to be planned against.

It is also required, where possible and agreed in the service level agreement, to guarantee that the access required by nominated authorities can have an enhanced survivability in the case of load or disaster. This may be achieved by preventing any single point of failure.

7.5 Requirements on IoT communications

7.5.1 Networks and connectivity

NOTE 1: Due to the renumbering of clauses in V1.3.1, the former clause 7.5 has been moved after the present clause and renumbered clause 7.6.

IoT communications are often made of a massive number of small amounts of data. One of the main challenges of IoT communications is the large number of communication standards as well as proprietary solutions which result in market fragmentation. When used to support emergency service teams and authorities, IoT data exchanges should be based on commonly accepted standards for professional and home users. Furthermore, when relevant, IoT communications shall support real-time services to deliver the collected data on the fly.

IoT devices and IoT applications should be able to suggest data transmission priority classes to the network(s) (important primary data should be transported with priority in comparison to (optional) secondary data). IoT data exchanges shall have appropriate priority and pre-emption rights when used on top of public communication networks, in a similar manner as what is described in clause 6.1.2.

As the global connectivity may be broken in case of disasters, IoT data communications should support both an infrastructure mode (via access points, "on-network") and an ad hoc mode (decentralised wireless network, "off-network").

NOTE 2: 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.

The IoT devices provisioned for emergency services (and communication terminals) should be able to automatically switch between infrastructure mode and ad hoc mode. They may support bandwidth sharing among the two modes. When it is used, the ad hoc mode should support routing and data transmission via multiple hops (i.e. one or more hops). When QoS is a needed differentiating factor, both infrastructure and ad hoc modes should support different transmission priority classes for IoT data. If possible, the ad hoc mode 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 connection failures, setting up of redundant routes, etc.).

IoT devices and IoT applications shall buffer data locally during network outages until connectivity is regained. After re-establishing connectivity, data shall be automatically transferred/synchronized without user interaction starting with top priority class data and tentatively avoiding network congestion. When available, the ad hoc mode should support "store and forward" data transmission for isolated network nodes when compatible with the data transmission priority class.

Drones (also called Unmanned Aerial Vehicle, UAV) are part of the IoT devices used by authorities to monitor and share information about emergency situations. To support the usage of drones, networks shall provide reliable communications in the vertical dimension, up to the altitude agreed in their service level contract.

7.5.2 Interoperability

All IoT devices and service platform entities to be used for emergency applications shall ensure that devices and applications from different vendors can communicate with each other. This may occur at connectivity level and if not possible, at service level. Semantic interoperability works as an abstraction entity that enables interoperability of different platforms at service level, without requiring connectivity interoperability. Accordingly, syntax and semantics of IoT data used for emergency situations shall be standardized but are out of scope of the present document. The interfaces to a database or servers handling the Common Operating Picture (COP) should be standardized as well and are out of scope of the present document.

7.5.3 Data exchange at service and application level

Data are exchanged between services and applications through the communication network. IoT service platforms are the entities supporting this exchange.

To enable all types of services, the IoT service platform shall support (near) real-time (multi-)point-to(multi-)point data transfer and streaming at the service level. A platform shall be able to manually or automatically adapt IoT device data rates (e.g. scaling of video camera resolution) to available network bandwidth. When relevant, it shall identify emergency communications priority classes and provide them with a guaranteed quality of service. The IoT service platform shall also support emergency communications at the service level in isolated operation mode, i.e. without the need to reach a remote server especially in the case where the communication with the server has failed.

To avoid false alarms and misled actions, the data quality shall be guaranteed by all IoT devices involved with the IoT service platform. The IoT device data shall be of sufficient accuracy (i.e. precision and correctness of sensor data).

IoT devices can be sensors or actuators. There are cases when they are able to react faster than individuals and protect the safety of mobile teams. In this case, an IoT device planned for such a task shall be able to trigger other IoT devices via the IoT service platform (e.g. smoke detector turns on a camera).

7.5.4 Contribution to the Common Operating Picture (COP) service

IoT data contribute to the construction of the COP. All relevant emergency IoT data shall be stored in the Common Operating Picture (COP) so that the COP allows tracing the activities during the incident response and forecasts. After clearance of the situation the COP data shall be available for lessons learnt and investigations, still respecting the GDPR requirements [7]. IoT applications with man-machine-interfaces shall 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). IoT applications with man-machine interfaces related to the COP should provide functionalities for daily tasks (e.g. emergency medical service documentation and billing). The authorization scheme shall 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.

All IoT devices and the network(s) involved in the COP shall support time synchronization and shall assign timestamps to data when/where appropriate. This applies to isolated operation mode, too. Time synchronization events shall be logged, so that all timestamps can be mapped to a common time reference. COP databases should support automatically generated and manual data updates. An emergency service decision maker should be able to manually override data updates. 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.

COP data shall 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 shall automatically discover existing synchronization composites and shall automatically (i.e. with as little user interaction as possible) synchronize the COP data. The synchronization composite shall be able to handle leaving (or failing) devices, too. However, COP databases should support remote access to COP data without full COP data synchronization. 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.

7.6 Network management support functions for delivery of inter-authority calls

7.6.1 Priority of inter-authority emergency communication

Inter-authority communications should be afforded preference status as nominated for their use in a call preference scheme (see clause 6.1.2) in times of disaster. This preference should be accorded across public telecommunications networks.

7.6.2 Monitoring of the communications availability of the authority

Communication channels over which emergency communication services are connected should be available without restriction. The terminating network permanently monitors the functionality and transmission quality of the communication channels. Technical modifications and maintenance should not impair emergency connections to the authority. If the quality falls below a minimum threshold, the network and authority should deactivate the access and check the availability and quality of the connection. Any such deactivation should not affect any communication in progress.

7.6.3 Diversion of inter-authority calls

If a network access to an authority is deactivated or out of order the network shall be able to divert incoming Emergency Services Calls to back-up/alternate equipment, connections, network access, if required by the authority. The authority shall inform the network operator on requested reconfigurations.

7.6.4 High or resilient availability

Subject to the nationally agreed service level agreements, network operators should use network management measures to ensure end-to-end inter-authority communications.

7.6.5 Security provisions at the access to authorities

The network operator should make reasonable provisions to mitigate against the impact of attack, either deliberate or accidental, to the access and core networks to which authorities and IoT devices are connected.

8 Security and privacy

8.1 Role of National Communication Security Authorities (NCSA)

For many governmental organizations including public safety, responsibility for communication security lies with a National Communication Security Authority (NCSA). Any mechanisms employed in communication systems used by such organizations shall meet the specific requirements laid down by such national authorities. International coordination exists between many NCSAs, embodied in the Common Criteria ISO/IEC 15408 [4] and the ITSEC arrangements which are accepted by most national governments within Europe and the European Commission.

Users, equipment manufacturers and service providers should contact the relevant national authorities in order to establish the relevant security requirements for particular communication services.

8.2 General security issues

For all emergency communication, the organizations involved shall ensure 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 authorized persons (see GDPR, [7]). In the context of emergency communication several security requirements have to be discussed:

- Confidentiality of data: Whenever confidential data is transmitted it is necessary for each party involved that they can rely on the fact that no eavesdropper gets hold of it. According to the degree of its confidentiality the data shall be transmitted via secure channels and protected by encryption during transmission and storage.
- Protection of signalling information, to prevent denial of service attacks or traffic analysis.
- Authentication of persons or devices: All persons (and devices, if necessary) involved in critical communication shall be provided with means to authenticate themselves. It should be possible for them to do so without having to trust or even know each other, especially in scenarios where ad-hoc communication has to be provided to parties that cannot communicate via secure channels established in advance.

- Authorization: Access to confidential information and critical systems is restricted to persons with appropriate entitlement.
- Integrity of data: Each of the parties has to be able to control if the data he gets is complete and correct and if it was altered during transmission.
- Non-repudiation: None of the parties involved in the communication should be able to subsequently deny that they took part in the information exchange and the commitments they made during the communication.
- Logging: Records of communications should be available to protect users. This information may also assist with subsequent assessment of the emergency, but should be discarded when not useful anymore.
- Privacy: Call and video data (e.g. images and videos collected by drones), IoT data (e.g. biometrics, vital parameters) and COP data (e.g. patient data, names, diagnosis, addresses, etc.) storage and processing should be designed to guarantee privacy protection (see GDPR [7]) and prevent any personal data breach.
- Consent: Individuals monitored by IoT devices have to be in the position to give their consent to the processing of their personal data either by a statement or by a clear affirmative action. This also applies to emergency service teams.

Many public safety services already possess some degree of security to prevent eavesdropping and denial of service. Some systems will only operate with security mechanisms being in place. However, it is essential that in an emergency, appropriate security mechanisms are supported without detracting from the usability.

8.3 Interconnection of secure communication systems

As communication systems employed by many public safety organizations operate in conformance with security requirements issued by NCSAs, there may be significant difficulties in supporting interoperability between systems. Ad-hoc solutions to these problems are generally unsatisfactory and result either in a loss of security as all users fall back to operating in non-secure mode, or in the loss of all but basic services as interconnection is proved only through "red gateways" or "swivel chair interoperability" (where a single user is provided with terminals for multiple systems).

Significant pre-planning and co-ordination of security solutions shall be established as necessary in order to support interoperable secure voice and data services between different user communities and across different networks.

These requirements can be fulfilled by a variety of security mechanisms, as described in annex C.

Annex A (normative): Basic architecture

Figure A-1 represents the basic architecture and the interfaces between authorities where the Rx are the numbered reference points for identification and showing the interfaces.

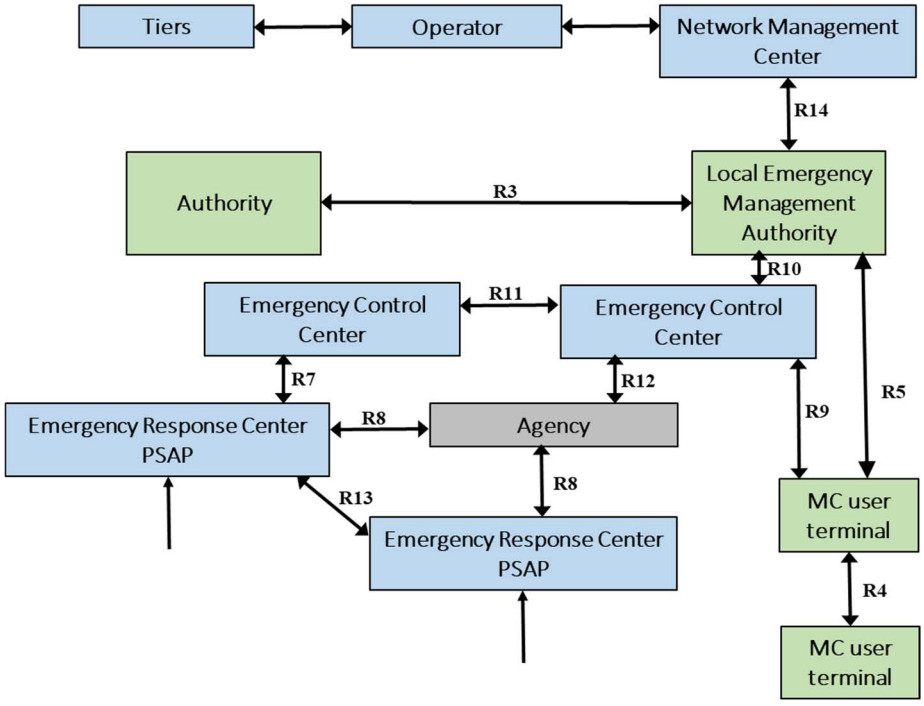

Figure A-1: Basic Architecture

Information about the reference points illustrated in Figure A.1 can be found in the following clauses:

- RP R3: clauses 4.3, 4.6, 7.3;
- RP R4: clauses 4.5, 6.1.2;
- RP R5: clause 6.1.2;
- RP R7: clause 4.1;
- RP R8: clause 4.1;
- RP R9: clauses 4.4, 6.1.2;
- RP R10: clause 4.6;
- RP R11: clause 4.3;
- RP R12: clause 4.1;
- RP R13: clause 4.2, 7.3, 7.4;
- RP R14: clauses 4.6, 7.6.

Figure A-2 represents the same architecture, additionally showing the different IoT entities supporting that architecture.

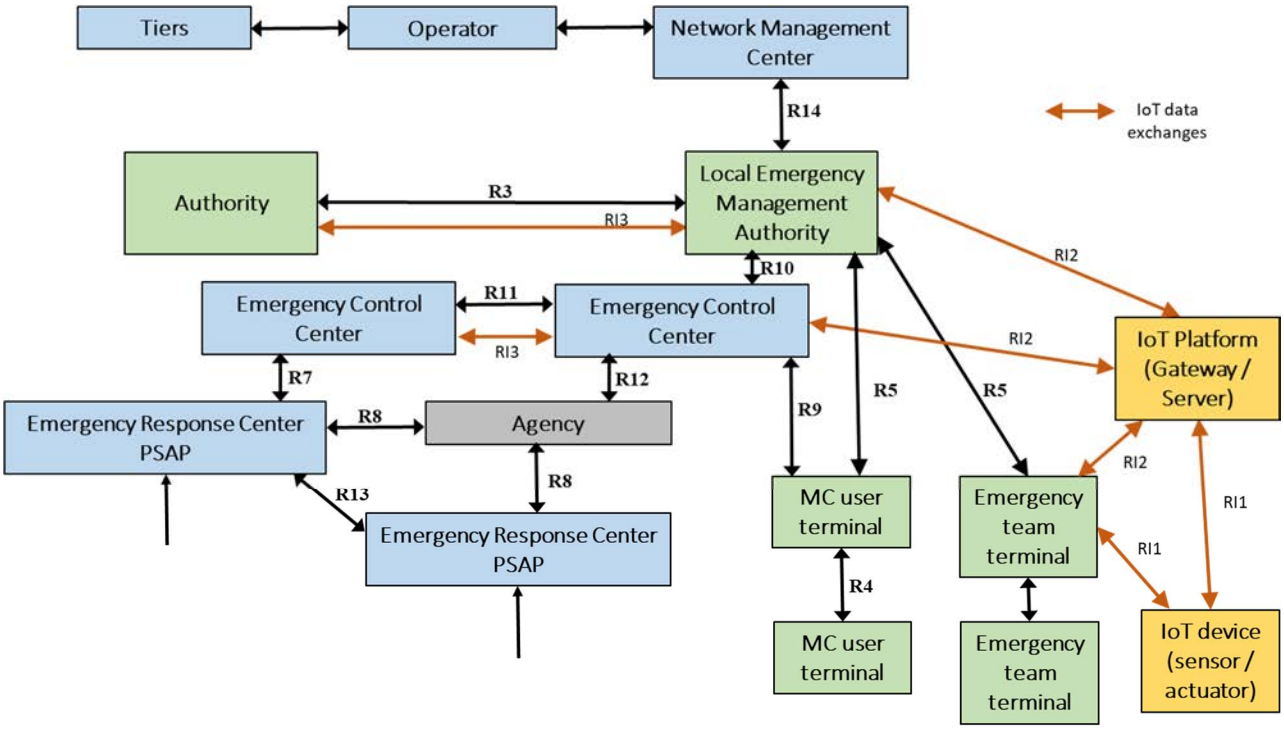

Figure A-2: Basic Architecture showing IoT data exchanges

Information about the additional IoT reference points illustrated in Figure A.2 can be found in the following clauses:

- RP RI1: clauses 4.4, 4.5, 7.5;
- RP RI2: clauses 4.4, 7.5;
- RP RI3: clauses 4.1, 4.3, 7.5.

Annex B (informative): Organizational related issues for authorities to solve

B.0 Introduction

Telecommunications systems or operator services cannot cover all emergency communication needs. In the present document attention of public authorities are drawn to some situations where a fair level of performance can only be reached if organizational decisions are taken by the authorities themselves.

As supporting documents to this annex, ETSI TS 103 260-1 [i.9] and ETSI TS 103 260-2 [i.10] respectively define reference scenarios for an earthquake disaster and a mass-transportation accident (MTA) in a rural environment. Both scenarios include the definition of the responders involved and their gross communication needs. They also define the topology modelling of the responders involved, in terms of their disposition in the incident area, their time evolution and their movements (if any). These scenarios are not generic in the sense of representing all emergencies of each type, but they are intended to be "typical" examples, and thus a reference in order to allow evaluation and dimensioning of required overall emergency telecommunications.

B.1 Handling of foreign languages

In the case of communications between authorities (often between neighbouring countries and a good probability to have on both sides bilingual people), and compared to the case of receiving the emergency calls, the problem may be simpler than with general public. But in general, the solution cannot rely on a statistical hypothesis and involves a minimum training of staff and specific agreed procedures or definition of contacts points for example.

B.2 Mitigating consequences of radio coverage discrepancies

One possible consequence is that some calls may arrive on a wrong destination (presumably in a neighbouring area). Staff in this situation should be informed and know how to act to transfer the call or answer to the caller without delay.

B.3 Definition of priorities (list of beneficiaries, levels, conditions of effective implementation)

The policy in priorities is clearly a national or regional issue. It can be expressed through lists or plans. For a given area, the preparation of such plans should be made in a collaborative way with the operators and users (rescue services), initiated and coordinated by the concerned administrative authority. An International Emergency Preference Scheme (IEPS) is defined in the Recommendation ITU-T E.106 [6].

B.4 Contingency planning

The entities and relations special task force, temporary headquarters and administrative entities or secondary response organizations will be mobilized in disaster situations as soon as the events have reached a predefined level of importance.

This may not be just a question of the regional coverage or a disaster event or of number of casualties, but the need to call on other organizations to perform secondary tasks (e.g. cut the water or gas supply to avoid a risk in the vicinity of an accident with specific conditions); some of the situations require only a normal means of communicating between the emergency control centres and corresponding technical operation centres.

It is, however, clear that all authority representatives should be ready to face dramatic events, where the normal PSAP/ECC will be overloaded with calls and tasks to prioritize.

The prerequisite for facing this sort of situation relies in the hand of the national or local authorities who have the power and the responsibility for fixing the frame of adequate plans, obtain or impose agreement from all authority representatives and make available contingency resources. Also, they will often take the decision of declaring a crisis status, condition for activating the exceptional plan.

The cases where ECCs should invoke a contingency plan depend on a lot of factors, for example: the need for extra resources, simultaneous actions of various disciplines (fire and medical, road traffic, fire, etc.), general organization, geographical distribution of resources, etc.

As a result, relations between authorities, and their need for communications can be based on a regular and daily routine, but may be required to escalate to cater for exceptional cases, and specially faced to dramatic events.

In the case of dramatic events, it is advisable to have plans pre-defined in order to be activated on request of one of the ECCs or on demand on an administrative body. In general, the plan will include several actors outside the ECCs themselves (private companies of ambulances, private doctors, technical services of companies operating facility services, etc.).

Such plans may consist of:

- lists of designated contacts and their co-ordinates;
- basic organization scheme;
- priority schemes (categories of priority, list of people authorized according to each category);
- procedures for requesting the activation of priorities towards the telecom operator (s);
- procedures for updating and change of the previous information;
- procedures for cancellation of the exceptional situation, end of the plan and return to normal.

B.5 Organization of authorities in case of catastrophic event

Most countries have a concept of levels of authority and assistance that can be called on in major catastrophes. In normal emergencies, the primary authorities and organizations can be relied upon to react to the situation. In more serious emergencies three general effects take place. First mobile ECCs are created. This enables the resources of the primary authorities to be concentrated and managed closer to the disaster. The second effect is the escalation toward greater administrative control. In which case contingency plans exist for the local/regional/central government to provide resources, evacuation, planning of transport, food etc. Thirdly, secondary assistance can be called on where commercial organizations that provide essential services are called on under special legal conditions to restore water, electricity, repair roads, communications, etc.

The definitions of the primary authorities, the emergency responsibilities of national or regional authorities, the legal mandates on secondary organizations in an emergency situation vary between countries. But the general concepts remain true. These differences are not the aim of the present document.

The communication needs for the escalation are paramount to the present document. The provisions of communications to primary authorities should be considered in the context of the need where an emergency can rapidly escalate and a rescue team and/or ECC is required. In these cases, a mobile ECC is a means of concentrating resource. Hence it may be seen as subsidiary to a fixed ECC. A mobile ECC has greater communication needs than a normal response unit.

EXAMPLE: A mobile hospital may have needs for video relay of consulting to other hospitals for advice on treatment, operations, radiology, etc.

The requirement for guaranteed QoS data services is therefore much greater in this context. Communications for emergency services should be scalable in terms of numbers of users and bandwidth.

The communication needs for mobile emergency unit and/or control centres are:

- Guaranteed QoS data services.
- Priority access to other peer level and supply organizations.
- Ability to call on recognized experts (doctors, midwives, chemical experts, etc.) and equip them with intuitive communications.

The communication needs for local/regional/central government control and planning during disasters are:

- Priority access to other governmental, primary, secondary and supply organizations.
- International communication for cross-border assistance, e.g. a ship sunk in a common international sea-lane.

The communication needs for secondary assistance organizations that provide essential services are:

- Priority access to governmental, primary, other secondary and supply organizations.
- Access to the emergency communications features of the primary authorities during the repair/crisis.

In addition, the following communication needs may also be present:

- International communication for cross-border assistance.
- Temporary authorization as an authorized emergency organization, electronic authorization.
- Compatible communications equipment and personnel when called on to assist across national borders, e.g. authorized UK electricians assisting the repair of the French electricity network after a hurricane.

B.6 Communication between civil authorities and Non-Governmental Organizations (NGOs)

NGOs are frequently closely involved in the response to emergencies. While this involvement may not take place in the hours immediately after an incident, they may form a vital part of the response to an incident. It is essential to coordinate with NGOs, both for protection of NGO staff and for effective liaison and sharing of information between NGO and authorities.

B.7 Communication between civil authorities and press organizations

Emergencies make the news. Although this is not a high priority, communications support to emergencies should plan to support some degree of communications with the press organizations. Procedures should be in place to ensure that the channel used to press organizations involves checks on the suitability to release information.

B.8 Maintenance of IoT devices and platforms

As further described in ETSI TR 103 582 [i.5], the maintenance of IoT devices and service platforms plays an important role for their correct operation when they are needed. It happens too often that the failure of an IoT device at a critical moment hinders the work of emergency services. The main points addressed here are that all IoT devices involved in emergency communications should support remote maintenance (software updates, battery and function check, etc.). It is also highly recommended that a certification process and adequate security measures are applied to software updates of IoT entities involved in emergency communications.

Regarding scalability, taking into account the large number of IoT devices that may be involved, methods and approaches for large scale firmware and software deployment are needed. Device Management platforms should adapt to the new volume of connected devices. To that end, "campaign management" tools allow to define operations for large numbers of devices using pre-defined rules. In addition to reactive operations, pro-active operations may be required, for instance when a vulnerability is detected on a family of devices, requiring a prompt firmware upgrade. Rollout tools will trigger maintenance operations on devices following specific strategies balancing the operational and functional risks, with either the device pool divided in sub-groups or through a more direct approach with simultaneous upgrades in the case of a serious security crisis.

Annex C (informative): Security mechanisms

C.0 Introduction

The following techniques may be utilized in order to provide security features described in clause 8.2.

C.1 Symmetric encryption schemes

Two parties A and B agree on a secret encryption key either during a personal meeting or by communication on a secure channel. A message one of the parties encrypted using this secret key can only be decrypted by the second party. If their secret key is compromised, A and B should agree on a new key. Symmetric encryption schemes run much faster than asymmetric schemes but they do not allow spontaneous interaction between parties who do not know each other. Another restriction that occurs with symmetric encryption is key management, as every pair of participants in the scheme has to find a way to agree on different keys and store all those keys safely.

It is a common characteristic of emergency communications that typical communication channels for standard situations will be known prior to the real emergency case, so secret keys can be exchanged before an emergency occurs. Thus, symmetric encryption is the preferable method, especially for real-time communication such as voice calls that would suffer from any decrease in performance.

C.2 Asymmetric encryption schemes

Party A chooses a pair consisting of a private key it keeps secret and a public key it publishes for everyone to know, for example in some public directory on the internet. It is not possible for anyone to compute A's private key from the public key. If Party B wants to encrypt a message to A, it gets the public key and does so. Nobody but A (who knows the private key) can decrypt this message. Every participant in the scheme needs only one pair of keys. The key management, however, has some difficulties and requires some kind of public key infrastructure. To link a key to its identity, Party A has to have the key signed by a certification authority. Anyone who trusts this authority can check the signature by using the authority's public key that is generally known. Problems can occur, if there is no third party that both A and B trust. Asymmetric encryption schemes allow spontaneous secure communication between strangers as everyone, who wants to send a message to A, can get the appropriate public key and use it for encryption. A disadvantage of the publishing of the key occurs when A's private key is lost or compromised and has to be changed. A cannot know for sure who got the old public key and warn these persons, not to use it anymore. All A can do is publish the key on a revocation list and hope that B will look into it before encrypting a message with the compromised key.

It will be necessary to use asymmetric encryption if non-standard situations occur during the escalation of an emergency, e.g. if parties from different countries have to exchange information without having had the chance to establish secure communication channels in advance.

C.3 Hybrid encryption schemes

To enjoy both the benefits of symmetric encryption (e.g. better performance) and those of asymmetric encryption (e.g. spontaneous confidential communication between parties that have not had the chance to agree on a shared secret key prior to their communication) a hybrid scheme could be used. This means that the involved parties use asymmetric encryption to agree upon or exchange secret keys in a setup phase of the communication after which they will be able to continue their information exchange using symmetric encryption.

Hybrid schemes will be helpful in situations that require spontaneous information interchange as well as excellent performance and where asymmetric schemes would have to be used otherwise.

C.4 Digital signatures

Party A signs a message by creating a hash value of it, to which it applies an asymmetric encryption algorithm involving its private key afterwards. The result of this process is a digital signature of the message that A can send to B or publish along with the original data. Everyone can use A's public key to verify both that the signature is valid i.e. that the message was really signed by A and that the content of the message has not been altered after the signature has been made. In addition, A cannot repudiate the message afterwards, as a valid signature can only be created with A's private key. Thus, digital signatures are a means to ensure non-repudiation as well as sender integrity and data integrity.

C.5 Authentication methods

Depending on the criticality and sensitivity of the concerned data and communication, various means of authentication could be used. The simplest method providing a basic security level is having the users identify themselves with a username and password. For stronger authentication one-time passwords or certificates stored in software or on smartcards are the preferable means of authentication. The use of digital certificates issued by trusted organizations also provides the advantage of spontaneous authentication between parties that have not been in contact before.

C.6 Authorization schemes

For all critical systems and resources as well as for all sensitive data there should be strict rules defined as to who is allowed to use, change and delete them. This ensures that only authorized entities can log into the system and only work with the data and use the resources they have been explicitly allowed to access. The most efficient way to handle authorization is to assign access rights to the role a group of persons are playing in the organization rather than to the persons themselves. This makes the management of rights easier and allows a quick replacement of people in case of illness, vacation or termination of the work contract of a role bearer. Every role should only be assigned only the minimum rights that are needed to fulfil its tasks. Accounts should not be shared between several people so it will be possible to identify who exactly is responsible for which actions.

C.7 Logging

Logging mechanisms do not prevent attacks or access to data without permission, but do at least store these events. Thus, it is possible to identify attacks or attempts of attacks (and hopefully stop them before too much harm is done) and use this information to prevent further disruption of the system.

C.8 Virtual Private Networks (VPNs)

A Virtual Private Network (VPN) can be used to facilitate joint or co-operative actions; this may be deployed on a permanent basis between entities acting within a common area, especially if there are not collocated.

However, a VPN may be required for temporary situations where an ad hoc co-ordination levels may have been created, e.g. Between PSAPs, and emergency control centres a permanent VPN can be established to facilitate the relationship. A temporary VPN may be established between emergency control centres and a mobile co-ordination centre of an emergency, this may then be extended to individual emergency service personal.

VPNs provide services such as closed user group, on-net/off-net, on-net authentication, on-net encryption, on-net priority and pre-emption, authorization to intrude/pre-empt, authorization to not be able to intrude/pre-empt, place priority calls on-net/off-net. Secured long tail access, service integrity, secure data services, encrypted data services, high integrity data services, etc.

Annex D (informative): Mobile Radio Services

This annex describes the mobile radio services listed in clause 6.1.2.3.

Call queuing when busy

To prevent unnecessary user frustration when a network is busy, call queuing is provided in "First In First Out" (FIFO) and/or access priority order. This means that users trying to gain access to the network are informed that the network is busy, and are automatically called back when they get to the top of the queue and their called party communication is being initiated.

Dynamic traffic management algorithms

To optimize GoS and capacity during busy periods a dynamic means of managing different types of calls is required. For example, the use of dynamic call duration timers with "time out timer" warnings on "one to one" calls, preferred site operation for group calls, restricting wide area group calls to base station sites where the majority of group members are registered and/or allowing wide area group calls to proceed only on sites at which preferred users in the group are registered.

Group call (commonly called "all in formed net" and "talk group call")

- Use simple "push to talk" operation to provide fast call set-up group communications.
- Be operated and managed in particular ways to optimize network loading, some examples being:
  - Simplex operation.
  - Preferred site operation.
  - Area selection.
- Have a very reliable call-set up signalling protocol to ensure all users in a group are connected together when a call is first initiated (call acknowledgment signalling is impractical for group calls).
- Have priority mechanisms to ensure that specified users in a wide area group call (spanning multiple base station sites) are connected together when a network is busy.

Pre-emptive priority call

This call service, commonly known as Emergency Services Call, provides the highest uplink priority and highest priority access to network resources. If a network is busy, the lowest priority communication is dropped to handle the Emergency Services Call. Unlike 911, 112 or 999 initiated public network emergency calls, a PMR Emergency Services Call can be initiated by using a dedicated switch located on the terminal. Activating the Emergency Services Call automatically alerts the affiliated control room dispatcher and other terminal users in that person's talk group.

Call retention

This service protects selected radio terminal users from being forced off the network as a result of pre-emptive calls (Emergency Services Calls) during busy periods. When Emergency Services Calls are supported in a network, it is essential that only a small number of radio terminal users are provided with this facility as the objective of retaining important calls during busy periods could be lost.

Priority call

During network busy periods, that service allows access to network resources in order of user terminals call priority status. As there are multiple levels of priority, this service is very useful in providing different GoS levels (and tariff structures) during busy periods.

EXAMPLE: Front line officers would be provided with the highest priority levels in a public safety network to maintain the highest level of service access whilst routine users would be provided with lower priority levels.

Direct Mode Operation (DMO)

DMO provides the ability for radio terminals to communicate directly with each other independently of the fixed network infrastructure. DMO has been a facility mandated and used by many traditional PMR user organizations for several decades. The primary requirement for DMO has been brought about by the need to balance the RF coverage, GoS and reliability of a network with that of the network's overall cost. This capability is called device to device communication (D2D) in cellular networks. It may be completed by the capability to establish transportable and standalone base stations, able to operate locally and independently from the network infrastructure.

Dynamic Group Number Assignment (DGNA)

This service allows the creation of unique groups of users to handle different communication needs and may also be used to group participants in an ongoing call. This service is considered by many public safety organizations to be extremely useful in setting up a common talk group for incident communications.

EXAMPLE: Selected users from the police, fire and ambulance could be brought together to manage a major emergency where close coordination between the three emergency services is required.

Similarly, DGNA is also considered useful for managing incidents with other user organizations such as utilities and transportation.

Ambience listening

A dispatcher may place a radio terminal into ambience listening mode without any indication being provided to the radio terminal user. This remote-controlled action allows the dispatcher to listen to background noises and conversations within range of the radio terminal's microphone. This is an important service to utilize for those persons transporting important, valuable and/or sensitive material that could be "high jack" targets. Similarly, this is a useful service to implement in public service vehicles where a driver's health and safety could be at risk.

The number of user applications for the ambience listening service are numerous and, in many cases, application specific. However, it is important to note that many users feel that this service invades a person's privacy and for this reason only those users who need ambience listening as part of their work duties should be provided with this service.

Call authorized by dispatcher

A dispatcher verifies call requests before calls are allowed to proceed. This is a useful service to utilize when radio user discipline needs to be maintained. This service also reduces the amount of radio traffic on a network as only essential work-related calls are permitted. However, the frequent need for all informed net group communications between terminal users and time delay experienced in authorizing calls can make this service unacceptable for some user organizations.

Area selection

Areas can be chosen on a "call by call" basis. This service simulates the ability for a dispatcher to select different base stations to make a call, as was possible in conventional networks. This service also helps to improve network load and overall spectrum efficiency by restricting the area of operation for selected group calls.

Late entry

This service provides continuous "call in progress" updates on trunked radio network control channels to allow latecomers to join a communication channel. This is not a service but an air interface feature that allows a trunked radio terminal to behave in a manner similar to conventional PMR terminals.

EXAMPLE 1: If a user turns on his terminal and a call is already in progress, the control channel will automatically divert the user's terminal to the talk group call.

Similar feature applies if the user's terminal has been outside of radio coverage.

EXAMPLE 2: In a tunnel, the control channel will also divert the user's terminal to a talk group call if a call is already in progress.

Voice encryption

To prevent eavesdropping by unauthorized users, PMR technologies used by public safety organizations require high levels of voice encryption with multiple keys and over the air re-keying. These wireless technologies should also support "end to end" encryption using a variety of encryption algorithms as deemed necessary by national security organizations.

History

Document history		
V1.1.1	December 2005	Publication
V1.2.1	February 2008	Publication
V1.3.1	June 2020	Publication