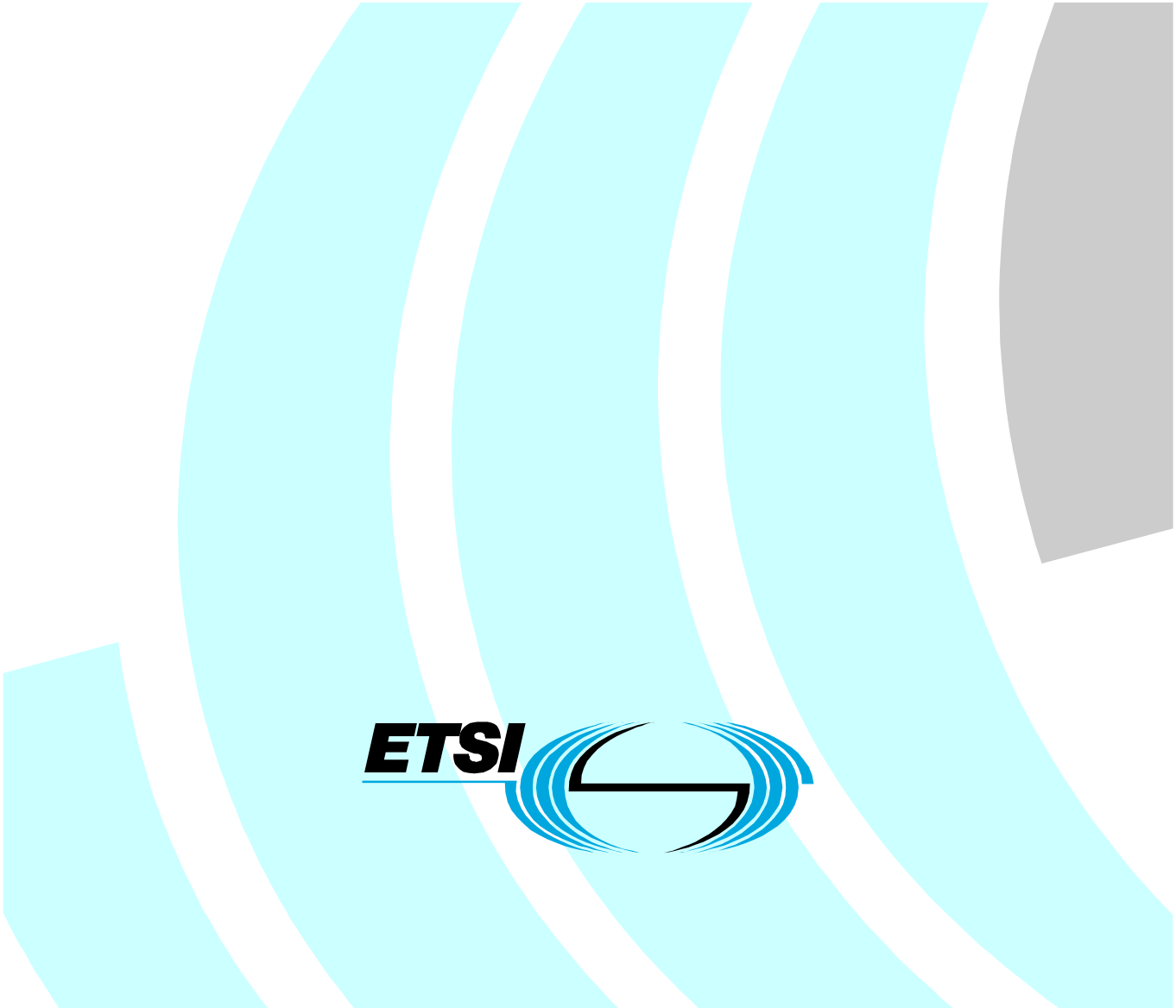
ETSI TR 102 445 V1.1.1 (2006-10)

Technical Report

Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness



Reference
DTR/EMTEL-00005

Keywords
diversity, 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

IPRs essential or potentially essential to the present document 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 (http://webapp.etsi.org/IPR/home.asp).

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.

Foreword

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

Introduction

The concept of Emergency Telecommunications (EMTEL) addresses a broad spectrum of aspects related to the provisioning of telecommunications services in emergency situations.

In emergency situations, efficient and effective communications is critical. The enabling telecommunications technology needs to perform in a robust and reliable manner, providing the requisite functionality to guaranteed service levels. Network resilience and preparedness are critical.

The present document provides an overview of several key technical concepts that can be employed to enhance network resilience. The document then considers the application of these concepts within the different systems that typically integrate to facilitate emergency communications between the public and emergency personnel. The present document concludes by considering network preparedness and the requirement for specialized systems and capabilities in exceptional situations.

1 Scope

The present document presents resilience concepts and considers their application within technical systems enabling emergency communications and also considers network preparedness and requirements for specialized systems and capabilities.

2 References

For the purposes of this Technical Report (TR), the following references apply:

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

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

[2] ETSI TS 102 181: "Requirements for communication between authorities/organizations during emergencies".

[3] ETSI TS 102 182: "Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies".

[4] National Infrastructure Security Co-Ordination Centre (UK): "Telecommunications Resilience".

NOTE: Available at: http://www.niscc.gov.uk/niscc/bestPractice-en.html?yr=2004&mo=5&da=31

[5] British Standards Institute PAS 56: "Guide to Business Continuity Management".

[6] ETSI TR 102 410: "Requirements for communications between individuals and to authorities whilst emergencies are in progress".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in SR 002 180 [1] and the following apply:

preparedness: activities, contingencies and measures taken in advance to ensure an effective response to the impact of hazards

NOTE: Source: United Nations International Strategy for Disaster Reduction;Available at: http://www.unisdr.org/

resilience: concept associated with resisting to the loss of capacity of a failure or foreseen overload, optimizing the availability and quality of service of telecommunications systems and support resources enabling a system to return to a previous normal condition

3.2 Abbreviations

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

DMO	Direct Mode Operation
DR	Disaster Recovery
ECC	Emergency Control Centre
PSAP	Public Safety Answering Point
PSRN	Public Safety Radio Network
RAN	Radio Access Network

4 Resilience concepts

4.1 Overview

Resilience is a concept associated with optimizing the availability and quality of service of telecommunications systems and support resources. The objectives are to maximize Mean Time Between Failure and to minimize Mean Time To Repair.

Resilience applies at all levels in the system hierarchy: at component level and at system level, and within switching systems, transmission systems and end devices.

A short overview of key concepts is provided in the following clauses.

4.2 Component level resilience concept

Component level resilience is the concept of incorporating features into the design of an individual component of equipment to enhance its overall availability.

Such features include:

- Incorporation of multiple redundant modules within the component such as power supplies, processor units and data storage modules.
- Localized storage of information within the component to enable continued operation in the event of failure of higher-level information sources.

4.3 Multiple component operation concept

Multiple Component Operation is the concept of deploying several components to fulfil a particular aspect of system functionality. Components are typically arranged in parallel.

Multiple Component Operation can be arranged in several modes:

- Redundant Mode: In the event of failure of the active component, operation is switched to the standby component. The switchover operation can be range from manual intervention to fully automatic.
- Active Parallel Mode: In the event of failure operation continues but with reduced capacity.

The different modes have differing advantages and disadvantages. Regarding Redundant Mode, design of the application and design of the clustering is simpler and there should be little performance loss in the event of a failure. However the total cost of the system is likely to be higher. Regarding Active Parallel Mode, the opposite arguments will apply: design is more complex and there is performance degradation in the event of a failure, but the total cost of the system will likely be lower in comparison to Redundant Mode.

4.4 Circuit diversity and separacy concepts in line transmission systems

Diversity is the concept of ensuring that specified circuits are not routed over the same transmission circuits. However there may be some common physical network sites and/or equipment within the circuit routings.

Separacy is a more reliable means of ensuring that specified circuits are not routed over the same cables, equipment or transmission systems and also that there are no common physical sites within the circuit routings. Normally, separated routes will even enter a building through separated ports using different service facilities (power etc.). They will only physically combine at the circuit terminal equipment.

It should be noted that separacy guarantees diversity, but diversity does not guarantee separacy.

In theory a single incident affecting one particular circuit should not affect transmission capacity in circuits that are diverse or separate. However, the avoidance of a single point of failure can only be guaranteed in fully separated circuits.

4.5 Diverse routing concepts

Diverse routing concepts relate to the ability to use, select or switch between different circuits to avoid congestion or network failure.

Diverse routing capability is built upon the provision of transmission diversity and separacy. Routing and transmission devices are capable of detecting a reduction in performance on a particular circuit and reroute traffic based on specific rules.

4.6 Fault-tolerant concepts

Fault tolerant systems are devices that are designed and built to correctly operate even in the presence of a software error or failed components. The term is most commonly used to describe computer systems designed to lose little or no time due to issues, either in the hardware or the software running on it.

4.7 Disaster Recovery (DR) concepts

Disaster Recovery (DR) is a coordinated activity to enable the recovery of telecom/IT/business systems due to a disruption. DR can be achieved by restoring telecom/IT/business operations at an alternate location, recovering telecom/IT/business operations using alternate equipment, and/or performing some or all of the affected business processes using manual methods.

4.8 Service diversity

Service diversity is a concept whereby if a particular communications service fails, information (or a subset of information) can be transferred by an alternate communications service. Examples include:

- If a Public TV service fails, Public Radio systems could still broadcast Emergency Messages.
- If a Commercial Cellular Telephone system fails, Commercial Paging systems could still be used for Emergency communications.

5 Emergency communications network resilience

5.1 Overview

The telecommunications networks used to enable emergency communications span a very broad group of systems, technologies and interfaces.

For the purposes of the present document, the arrangement illustrated in SR 002 180 [1] is considered. This is reproduced in annex A.

Consideration of the application of the key resilience concepts to emergency communications is provided in the following clauses. Avoidance of Single Points of Failure is a key concept throughout. Transparency on the end-to-end routing of emergency calls is also critical.

5.2 Local exchange/mobile switch to PSAP

The set-up of the call to a Public Safety Answering Point (PSAP) may take a number of routes originating from a fixed or mobile network or possibly transiting a point of interconnect. In each case an emergency call is given a higher priority than other traffic. The initial stage (customer to PSAP) achieves this based upon analysis of the call destination.

Various resilience techniques are applicable to emergency calls.

Typically emergency calls will have access to additional routes (although not exclusive). This occurs throughout the network, including access to multiple switches that support emergency communications services. It should be noted that the PSAPs themselves are connected to more than one switch.

In times of overload, Restrictive Network Management controls can be applied. Normal calls can be restricted to use a smaller number of circuits than usually available. However, priority calls are made exempt from such restrictions, effectively meaning that certain circuits are protected and made available for priority traffic only in times of overload. In times of normal load, all circuits are available and work normally. Hence this technique may be carried out on newer "Next Generation Networks" but may also be configured on current Circuit Switched networks.

Telecom operators use a number of other techniques to protect the network from the impact of fault conditions and during periods of high traffic. Often public networks can be subject to a large number of short duration very high traffic periods as a result of "phone-ins" to TV and Radio. The impact of these events are controlled by the use of call-gapping to protect the network. This will also restrict emergency calls if a user cannot access a dial tone.

5.3 PSAP

PSAPs typically house "contact centre" technology to enable the efficient and effective handling of emergency calls. In this environment, fault tolerant systems are appropriate to ensure very-high system availability.

The concept of Multiple Component Operation can also be applied. This can enable "load sharing" of emergency calls across different PSAPs. Should a major failure occur at a PSAP, calls can be distributed across other PSAPs.

Alternatively or in addition, Disaster Recovery concepts are appropriate to minimize the impact of any major system failure. These could take the form of a replicated secondary/back-up PSAP.

5.4 ECC

Emergency Control Centres house a number of operational systems, typically including:

- Integrated Communication Control System (ICCS).
- Command and Control (C&C) System.
- Geographical Information System (GIS).
- Private Automatic Branch Exchange (PABX).
- Radio Dispatcher Terminals (RDT).

In this environment, fault tolerant systems are appropriate to maximize the availability of "mission critical" applications.

Also, Disaster Recovery (DR) concepts are appropriate to minimize the impact of any major system failure.

5.5 PSAP/ECC integration/separation

The PSAP function can either be integrated with the ECC function or separated, dependent upon country and emergency response organization. Resilience concepts in these two situations are discussed below.

5.5.1 Integrated PSAP and ECC

In cases where the functions are in the same location, the systems can form an integrated system and there are no public network connections between them.

Positive benefits of this arrangement can include:

- Fewer potential points of failure, notably the transmission systems.
- Ability to share personnel across different functions according to workload and staff availability.

However, negative benefits can include:

- Centralization of systems and resources can represent a more acute single point of failure.

5.5.2 Separated PSAP and ECC

In cases where the functions are in separate locations, communications between PSAPs and ECCs are typically achieved using a dedicated leased line connection from the public network to the ECC.

Several resilience concepts are applicable in this instance:

- Connection of the ECC to more than one public network switch.
- Circuit diversity and separacy applied to the connections from ECC to public switches.
- Separacy and diverse routing capability across the PSAP to ECC circuits, and PSAP to Data Stores.
- Ability to re-route calls to another ECC should the initial target ECC be unavailable/unreachable.

5.6 ECC to emergency service personnel

Communications between an ECC and emergency service personnel are achieved in several ways, including:

- Using mobile radio systems direct to vehicle mounted and hand portable devices.
- Using private networks based on dedicated circuits to fixed devices in operational locations such as fire stations, police stations and ambulance stations.
- Using commercial cellular networks, see clause 6.4.1.
- Using (future) digital mobile broadband technology, see clause 6.4.2.

5.6.1 Mobile radio systems

Mobile radio systems are usually dedicated or prioritized for usage by one or more emergency response organizations. A common term is "Public Safety Radio Network" (PSRN).

There is an ongoing trend for roll-out of new digital PSRNs to replace legacy analogue PSRNs. In either case, there are typically several generic components:

- Radio access - typically radio base stations sited in strategic locations to provide the requisite radio frequency coverage.
- Access and core transmission - transmission systems from the radio base stations to switching systems.

- Switching network - for voice and data call control and routing.
- ECC Transmission - transmission systems from the switching systems to ECCs.
- Network management - support systems to configure and operate the network.

Resilience concepts can be applied to each of these components to achieve a guaranteed level of end-to-end availability for the voice and data applications operating over the PSRN and to avoid single points of failure. These concepts are discussed in more detail below.

5.6.1.1 Redundancy in the Radio Access Network (RAN)

The radio access network will typically provide higher levels of coverage than commercial cellular or commercial Private Mobile Radio systems. Due to the nature of a PSRN, coverage has to be provided over a high proportion of a land area instead of concentrating on a high percentage coverage of populations.

The radio access network itself can offer redundancy in a number of ways:

- Overlapping coverage from multiple cell sites in the same area.
- Redundancy of components on cell sites (e.g. transceivers, site controllers, antennas etc.).
- Redundancy of power supply capability, including battery and generator powered supplies.
- Fallback strategies to allow stand alone operation of sites disconnected from switching sites. In this case trunked communications are possible between terminals connected to the same site.

Radio access network availability is highly dependent on the topology of the transmission network supporting the cell sites, and by the availability of the core network switching components. The availability of the radio access network can be enhanced by:

- Use of multiple transmission links to sites using various topologies including redundant stars and rings.
- Configuration of network such that adjacent sites are connected to different switches: loss of a switch will still allow remaining sites to provide a reduced coverage across the served area if enough overlap in coverage is provided between the cell sites.

In areas where there is insufficient coverage overlap between sites, cell sites typical employ a means of providing communications in the event of network faults that isolate the sites from their switching centres. Where older analogue systems are in place, this communication typically is achieved by forcing the site to perform a stand alone repeater system, whereby the base station transmitter relays all received transmissions, and where different users will typically share the same channels. With the movement to all digital trunked PSRNs, more automation is typical, where the cell site maintains enough intelligence to provide a trunking function, maintaining the automatic allocation of different channels to different user groups.

5.6.1.2 Resilience in the Radio Access Network (RAN)

In addition to the mechanisms employed to provide protection against failures in the radio access network, mechanisms are also employed to provide resilience against interference, both deliberate and accidental.

The strongest protection against deliberate interference is the use of air interface encryption, often together with an authentication process, which protects signalling and traffic from eavesdropping, and also makes it difficult for an attacker to manipulate the air interface by replaying valid traffic or introducing interfering traffic. The encryption process can also be maintained during stand alone operation of a cell site.

Networks can also provide protection against accidental interference by monitoring the quality of the signal link between cell site and mobile device, and assigning different frequencies where interference occurs on a frequency in use.

5.6.1.3 Resilience in the transmission network

The transmission network (also termed Ground Based Network in PSRNs) is usually composed of a number of technologies including:

- Copper based landlines.
- Optical fibre networks.
- Microwave links.

Redundancy can be applied at a link level duplication of equipment supporting a single link, e.g. duplicate microwave transceivers, and duplications of the links themselves. Where links are duplicated, physical separation of routes (separacy) is generally employed to protect against a single physical event interrupting main and backup paths (e.g. severing of cables by digging machinery).

Redundancy can be applied at the network level, whereby the network is designed with multiple node to node links in a mesh configuration, and paths between pairs of nodes can carry traffic between other more distant nodes. Loss of a link or node causes the network to automatically reroute traffic through different nodes and links (diverse routing). This approach is more common with systems employing packet switching techniques, such as IP.

5.6.1.4 Resilience in the switching network

Switching sites are typically constructed using redundant or highly resilient components. The following techniques can be used within a switching site:

- Duplication of system databases, both within a site and between sites, to ensure resilience of user and system configuration.
- Duplication of switching intelligence to ensure mobility and call control functions are maintained in event of failures.
- Duplication of switching components, or more recently adoption of more resilient distributed approaches, typically based on IP, with redundant routing components.
- Redundant Local Area Networks connecting switching components.
- Redundancy in network interfaces connecting each switching site with other switching sites and with cell sites.
- Duplication of power supplies with use of Uninterruptible Power Supplies and back up options using batteries and generators.

In addition, duplicate switching sites can be used, such that a single switching site may be configured and switched into place of any failed switching site, or multiple switching sites employed up to the case that each primary switching site is duplicated. Duplication of switching sites takes place across multiple geographic locations to increase resilience in event of loss through disaster.

5.6.1.5 Resilience outside the network infrastructure

PSRNs usually provide additional means of communication outside the main communications network. This is known as Direct Mode Operation (DMO), as terminals communicate directly rather than via the network. DMO provides another level of resilience, as terminals may operate together locally and maintain communications either during network failures, or in areas where network coverage is not sufficient. Use of DMO can also alleviate traffic loading on the network in high traffic incident situations.

DMO range can also be enhanced by using repeater devices. These can be deployed to the area where communications are required, and can increase the communications range of the individual terminals by virtue of appropriate location and use of appropriate antenna systems.

5.6.2 Private Networks

The connections from ECCs to fixed devices in operational locations may involve wireline and/or wireless technology, and may be routed over public and/or private infrastructure.

Again, resilience concepts can be applied to these arrangements, including:

- Circuit diversity and separacy.
- Alternate means of communicating with the remote operational location (service diversity).

5.7 Planning/enhancing resilience

Resilience does typically require additional expenditure. 100 % guaranteed resilience is not usually affordable. Emergency Response Organizations must balance the risks to their service from a telecom failure against the cost of providing enhanced resilience. One approach for deciding a strategy is to adopt a risk management methodology. Several such risk management methodologies exist.

A number of documents regarding telecoms resilience and preparedness are publicly available. These are listed in clause 2 references [4] and [5].

6 Emergency communications network preparedness

6.1 Overview

In the present document, requirements for emergency communications network preparedness are treated separately from requirements for emergency communications network resilience.

There are a number of differing interpretations of the term "preparedness". For the purposes of the present document, "preparedness" is defined as "activities and measures taken in advance to ensure an effective response to the impact of hazards".

Extending the term to emergency telecommunications, for the purposes of the present document, "emergency communications network preparedness" is then defined as "activities, contingencies and measures taken in advance in relation to emergency communications networks to ensure an effective response to the impact of hazards".

Requirements for emergency communications network preparedness thus means the listing of specific activities and measures taken in advance in relation to emergency communications networks to ensure an effective response to the impact of hazards i.e. a listing of emergency telecommunications facilities that need to be prepared for use in the event of a major emergency/disaster.

6.2 General Requirements

Emergency management is the organization and management of resources and responsibilities for dealing with all aspects of major emergencies/disasters, in particular preparedness, response and rehabilitation.

Emergency management involves plans, structures and arrangements established to engage the normal endeavours of government, voluntary and private agencies in a comprehensive and coordinated way to respond to the whole spectrum of major emergency needs. This is also known as disaster management.

The emergency management process will thus generate a listing of emergency telecommunications facilities that need to be prepared for use in the event of a major emergency/disaster. Different Authorities will generate different requirements according to the specific set of hazards faced.

However, regardless of the specific set of hazards faced, there are several generic areas of requirements. EMTEL has identified the main areas as:

- Communication from individuals to authorities/organizations (emergency calls).
- Communication between authorities/organizations (public safety comms).
- Communication from authorities/organizations to individuals, groups or the general public (warning systems).
- Communication amongst affected individuals during emergencies.

Drawing upon existing EMTEL reports in these areas and expanding as necessary, requirements for emergency telecommunications facilities that need to be prepared for use in the event of a major emergency/disaster are compiled and summarized in the following clauses.

6.3 Communication from individuals to authorities/organizations

In the event of a major emergency/disaster, it should be possible for individuals to communicate with authorities/organizations.

SR 002 180 [1] sets out requirements for communication of individuals with authorities/organizations in case of distress, including in the event of a major disaster.

6.4 Communication between authorities/organizations

In the event of a major emergency/disaster, it should be possible for authorities/organizations to communicate within themselves and with other authorities/organizations.

TS 102 181 [2] sets out requirements for communication between authorities/organizations during emergencies, including in the event of a major disaster. Some further requirements for facilities are set out below.

6.4.1 Commercial cellular networks

The ECC may decide to contact certain emergency services personnel using a commercial cellular network. Certain personnel may not have access to private mobile radio networks for a variety of reasons, such as the person being out of the coverage area of a private network, or perhaps because the person acts in a part-time role or volunteer on-call role.

In the event of a major emergency/disaster, the commercial cellular network may however become congested with traffic, affecting the ability for emergency services personnel to make and receive communications.

In such situations, it should be possible to prioritize the communications for authorized emergency services personnel. Example mechanisms include the use of reserved "Access Class" values set on the GSM SIM cards of authorized emergency services personnel; during times of major incidents and network congestion, specific GSM base stations can be set to only allow users with certain access classes to use radio channels.

6.4.2 Conditions for implementation will be subject to national and regional technical and commercial agreements between Emergency Services Organizations, network operators and other relevant parties.(Future) digital mobile broadband technology

Specifications for digital mobile broadband technology aimed at the sectors of public safety and disaster response are currently in development. Project MESA is producing the specifications for an advanced digital mobile broadband standard. The availability of such technology will contribute to the overall resilience and preparedness of Emergency Communications Networks.

6.5 Communication from authorities/organizations to individuals, groups or the general public

In the event of a major emergency/disaster, it should be possible for authorities/organizations to communicate with individuals, groups or the general public.

TS 102 182 [3] sets out requirements for communications from authorities/organizations to the individuals, groups or the general public during emergencies. Implementation of such systems would contribute towards preparedness.

6.6 Communication amongst individuals during emergencies

In the event of a major emergency/disaster, it should be possible for individuals to communicate with other citizens.

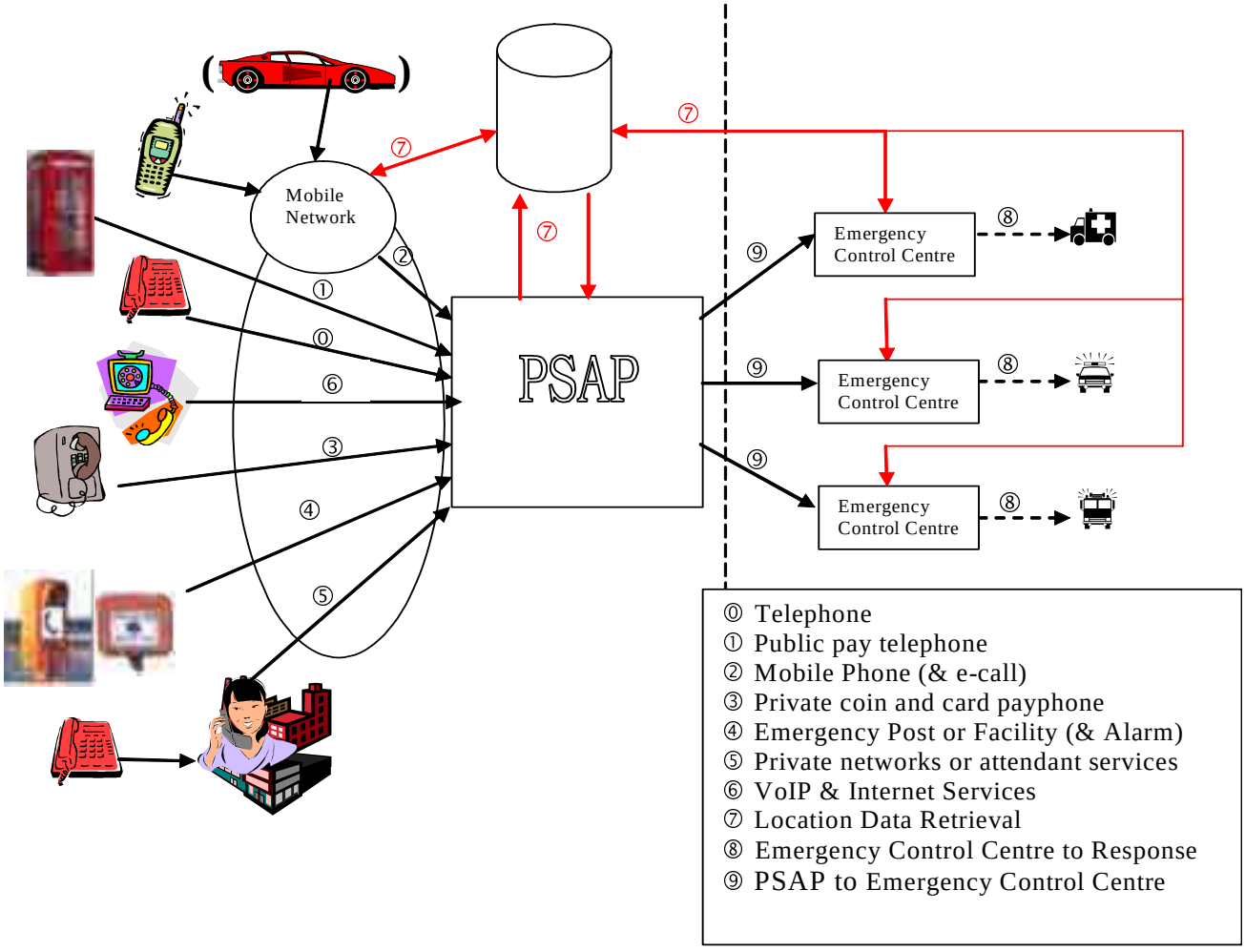
In case of an unforeseen disaster, individuals may have a strong demand to communicate among themselves in order to:

a) coordinate actions of mutual interest.

b) ascertain/learn the state of relatives, property, etc.

TR 102 410 [6] establishes a minimum set of requirements for communications facilities under such circumstances, taking into consideration that the normal infrastructure of country or region in question may be in a very bad state. The document gives recommendations on basic facilities that should be catered for and hints at possible realization.

Annex A:
Basic architecture



NOTE: PSAP can be integrated or separate to ECC.

Figure A.1: Functional architecture

History

Document history		
V1.1.1	October 2006	Publication