ETSI TR 102 197 V1.1.1 (2003-10)

Technical Report

Services and Protocols for Advanced Networks (SPAN); Preliminary analysis of EMTEL and Local Emergency Service requirements for IP networks and Next Generation Networks

Reference

DTR/SPAN-130318

Keywords

analysis, 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

Important notice

Copyright Notification

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 Technical Committee Services and Protocols for Advanced Networks (SPAN).

Introduction

The present document gives a preliminary analysis of the technical requirements for the support of EMTEL and localization service for Emergency and Priority services within the PSTN/ISDN/IP signalling transport services in Europe.

When Emergency communications is talked about there is a great deal of confusion of what is meant by an emergency. The present document separates the telecommunication requirements arising from disaster situations (natural (e.g. flood, earthquake), or manmade (e.g. terrorist attacks)) from the emergency (e.g. those requiring police ambulance and fire brigade on an individual basis).

The point at which an emergency situation becomes a disaster situation has been defined by the impact upon telecommunications networks.

The present document has been separated into three main clauses.

Clause 4 investigates the emergency calls scenarios where the service has been enhanced to include the location information of the caller.

Clause 5 deals with a disaster scenario that has an adverse impact upon the network.

Clause 6 outlines some of the requirements to support EMTEL on the next generation network (NGN) that is based upon IP technology.

These clauses do have a relationship but the situation and therefore the requirements expected of the networks are different.

1 Scope

The present document gives a preliminary analysis of technical requirements for the support of EMTEL and location services for emergency and priority services within the PSTN/ISDN/IP signalling transport services in Europe, to progress toward the enhancement signalling transport protocol standards documentation.

2 References

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

[1] CGALIES: CGALIES Final Report V1.0.

[2] LOCUS: Final Report D6.

[3] ETSI TS 102 164: "Services and Protocols for Advanced Networks (SPAN); Emergency Location Protocols".

[4] WERT FINAL REPORT for the September 11, 2001 New York City World Trade Centre Terrorist Attack.

[5] Project MESA; Service Specification Group Services and Applications; Statement of Requirements.

[6] ETSI TIPHON STF 225 report.

[7] ITU-T Workshop on Telecommunications for Disaster Relief, Geneva 17 - 19 February 2003; http://www.itu.int/ITU-T/worksem/ets/index.html.

[8] ETSI Workshop on Emergency Telecommunications, Sophia Antipolis 26 - -27 February 2002; http://www.emtel.etsi.org/Workshop/workshop.htm.

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

3 Abbreviations

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

3GPP	3rd Generation Partnership Project
ATM	Asynchronous Transfer Mode
CGALIES	Co-ordination Group on Access to Location Information for Emergency Services
CLI	Calling Line Identity
CPC	Calling Party Category
DECT	Digital Enhanced Cordless Telecommunications
EMTEL	EMergency TELecommunications
ETS	Emergency Telecommunications Service
EU	European Union
GMLC	Gateway Mobile Location Centre
GPS	Global Positioning Satellite
GSM	Global System for Mobile communications
GTS	Global Telematics protocol System
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IP	Internet Protocol
LAN	Local Area Network
LIF	Location Interoperability Forum
LOCUS	LOcation of Cellular Users for emergency Services
MLP	Mobile Location Protocol

NGN	Next Generation Network
PSTN	Public Switched Telephone Network
PSAP	Public Safety Answering Points
SCN	Switched Circuit Network
SMLC	Serving Mobile Location Centre
SMS	Short Message Service
SS7	Signalling System No 7
TDR	Telecommunications for Disaster Relief
TETRA	TErrestrial Trunked RAdio
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WERT	Wireless Emergency Response Team
WLAN	Wireless LAN

4 Enhanced emergency call for assistance

The need for and means of improved telecommunication services for disaster relief communications and emergency call handling was debated in ITU and ETSI workshops [7], [8].

The requirements for the Enhanced 112 (E112) service are contained in the CGALIES report [1] and in the LOCUS reports [2] which outline the regulatory and technical feasibility for the introduction of location information to the Public Service Answering Point PSAP. Thence this location information can then be passed on to the appropriate emergency service operator/dispatcher.

A collection of various national requirements for the purpose of taking them into account in the standardization work of ETSI is contained in draft ETSI SR 002 180 Requirements for communication of citizens with authorities/organizations in case of distress (emergency call handling) (for V0.2.0 2003-06) see [9] http://docbox.etsi.org/ocg/OCG_EMTEL/EMTEL03_Jun2003_Sophia/

4.1 Protocol interfaces

Figure 1 indicates how the location information of the caller is passed to the appropriate emergency service. The caller has been categorized into four basic types, a mobile user, a fixed line user, a data packet user, and an automatic alarm user. These protocol interfaces are marked ③②①④.

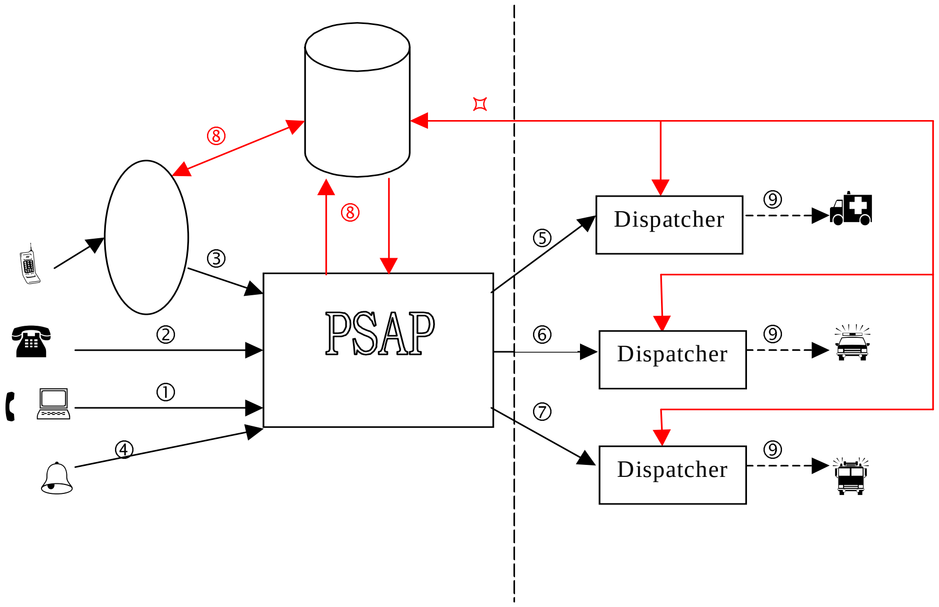

Figure 1: E112 Emergency service functional architecture

It should be noted that the dotted line denotes a notional interface, as the PSAP may also be the dispatcher to the particular emergency service. They are separated here as they represent two separate functionalities.

Interfaces ⑤, ⑥, and ⑦ are not currently standardized. This could be an area that ETSI/EU would want to be standardized as this could be an impediment to cross border co-operation between emergency services (see clause 4.2). In national and cross-border cases all communications from the PSAP to a dispatcher or another PSAP will be priority calls in order to bypass network congestion, failure etc. It should also be noted that for the case where the PSAP and dispatcher are the same person then the national and cross border communications will be via the interface ⑨.

Figure 1 shows location information being requested and delivered to the database across interface ⑧⑧ for the case of mobile networks. Although it should be noted that this protocol may not be standardized it is currently out for vote within ETSI SPAN as TS 102 164 [3].

Figure 1 also shows that the location information is requested and delivered to the emergency dispatcher, this scenario may not be valid for all implementations of emergency services. In some implementations the PSAP and dispatcher are one, in others they are separated as shown so that both the PSAP and the dispatchers have direct access to the location database. Whilst the PSAP is able to retrieve the emergency location in terms of a broad region the dispatchers is able to retrieve all available information about the exact emergency location.

Nevertheless the dispatcher will receive the location information and send it to the appropriate emergency vehicle across interface ⑨ by radio This interface ⑨ is shown as being one interface and one protocol to all the emergency services whereas it should be noted that this may not be the case, as it may be possible that one service uses TETRA another uses GSM technology or a proprietary system.

4.1.1 Fixed line user

This user includes the normal telephony user that dials for emergency assistance using the pan European emergency number 112, or national specific emergency number. As well as the voice telephony service other data services such as SMS or telemetry, may be used to alert the PSAP (or are configured such that an alert can be sent directly to the appropriate emergency service). The latter service may also include "panic button" type services used by elderly and infirm persons at home using radio type technology.

The main protocol deployed at interface ② internationally for this service is ISUP and there are many national variants of this as well as other SS No7 (SS7) protocols.

The location of the caller is derived from the CLI, which in the fixed network gives a very high probability that the emergency service is sent to the correct address/location. It should be noted that fixed networks start supporting SMS and that a short message includes the CLI.

The CLI is used to interrogate a database from which the correct address/location of the network access point can be obtained. This database can be a centrally maintained and funded by all operators or each operator will run its own database. In the decentralized case the PSAP and dispatcher need to be aware of which CLI belongs to which operator, this needs to be maintained to cover the number portability service. A network identifier indicating the database to interrogate and provided in association with the emergency call could be advantageous for the decentralized scenario.

The transaction ⑧ between the fixed network and the database is not required because a database update is required infrequently at network access installation time or after number portability since the network access is fixed. The transactions 8 between the PSAP/dispatcher and the database are required.

4.1.2 Mobile user

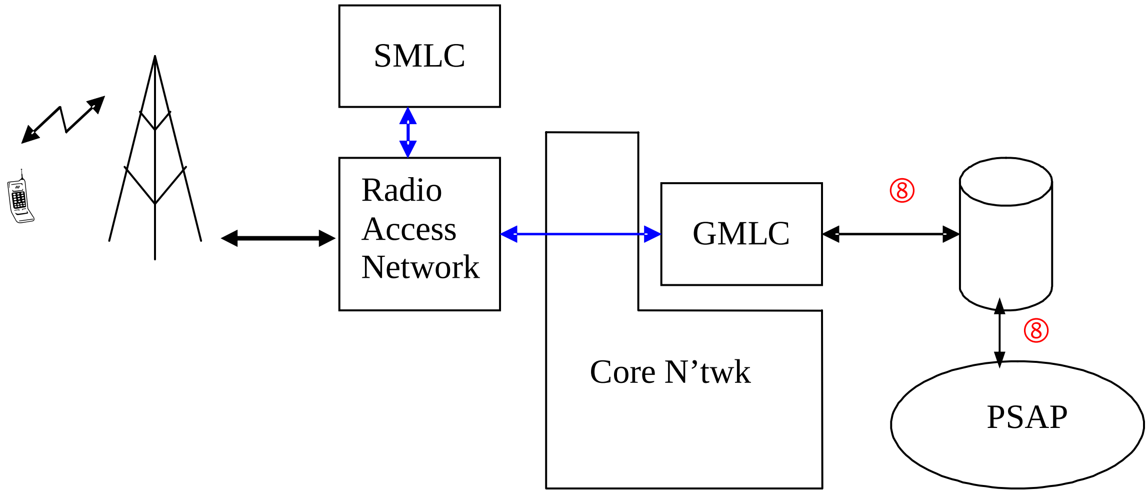

Figure 2: Mobile users with location information functional architecture

Figure 2 shows how for a GSM customer that dials for emergency assistance, using the pan European emergency number 112 or national specific emergency number, location information is made available to a database from where it can be retrieved by the PSAP/dispatcher. Today in most networks the CLI information is transported by means of signalling to the PSAP, the PSAP then can obtain the location information from the database using this CLI. The Serving Mobile Location Centre (SMLC) collects the estimated location information for this mobile. The location information is then passed to the Gateway Mobile Location Centre (GMLC) and the GMLC is responsible for the interworking to the protocol ⑧ and also performs other tasks such as authorization and privacy functionality.

The CLI is used to interrogate a database from which the correct location of the mobile can be obtained. This database can be a centrally maintained and funded by all operators or each operator will run its own database. In the decentralized case the PSAP and dispatcher need to be aware of which CLI belongs to which operator, this needs to be maintained to cover the number portability service. A network identifier indicating the database to interrogate and provided in association with the emergency call could be advantageous for the decentralized scenario.

Users of the next generation of mobile technologies, 3GPP UMTS should also be included in this category of caller. UMTS emergency calls will be fully backward compatible to the GSM emergency calls. For the GSM and analogue mobile (if any left) users the call to the PSAP is interworked to the protocols that are deployed in the fixed network. So as far as the signalling to the PSAP is concerned ③ is the same as ② for a call, and as already been stated the transport of the location information from the mobile network to the database ⑧ has been specified.

The GSM network also has the SMS, which may be used to contact the PSAP, however a one shot message does not provide the location information that can be obtained by the GSM voice call. It may be worthwhile for ETSI to investigate the possibility of obtaining the location information from a SMS message as well as looking into the impact of the use of non real time services, e.g. SMS and email, on an emergency call.

The EU commission project E-MERGE investigates and proposes a technology that enables a driver in a vehicle to contact the Home Call Centre in case of an emergency. The E-MERGE call can be generated automatically or is manually enabled by the driver. The E-MERGE call makes use of GSM and GPS technology to send a GTS protocol message carrying GPS location data plus other vehicle related information to the Home Call Centre.

It is not clear how this GTS protocol information which includes a chain of recent location information would be carried by the signalling networks (if required) or by the bearer channels, or how the GPS information is interworked to the database information carried in the protocol ⑧.

This car device can also make a voice call to the PSAP via GSM technology. ETSI would need to ensure that the telephony service is compatible with the standardized technologies and may have to write the protocol to support this project.

4.1.3 Data network user

4.1.3.1 Data based users

Included in this clause, is a description how location information could be obtained and verified. At present this cannot be done in the present IP protocol set of standards. How is this information then interworked so that the information is available in the location database?

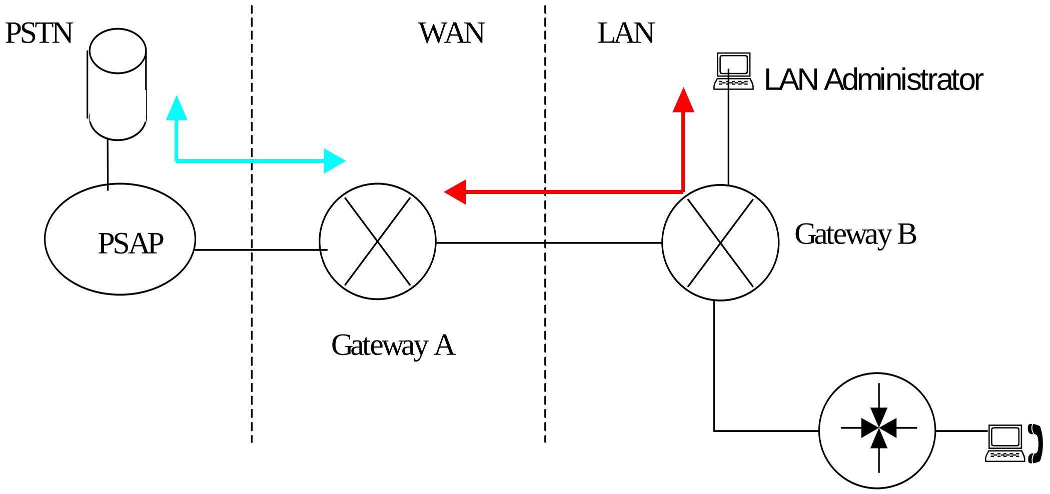

Figure 3: Possible architecture for location information from an IP based network

Figure 3 shows how the location information could be obtained from interrogating the LAN administrator who should have details of the subnet port number, which would equate to a physical location. This of course does not apply to wireless LANs, where the physical location of the aerial could be obtained but not necessarily the physical location of the VoIP caller. Now the procedure for this to be applied does not at this moment exist as far as the author is aware. Therefore (a) all LAN administrators should have the functionality to provide location information on emergency calls if they are enabling public telecommunications services and (b) the protocol from the PSAP location database and the information supplied from the LAN administrator in the IP protocol that has to be interworked at the Gateway A needs to be defined.

Voice over IP can be achieved with a number of differing protocol technologies which sit on top of the IP protocol transport layer itself, RTP, MPLS, SCTP and SIP, being some of them. Work needs to be done in ETSI to verify that these technologies can deliver the location information or is this achieved from the IP transport protocol itself?

VoIP needs to be defined for ETSI as far as a public telephony service is concerned as this term is being used for voice calls over the Internet, from one computer to another, or for telephony over the Internet, or for telephony on a managed IP network which is about to replace the current telecommunications networks.

A problem has been identified in that at present the User Agent on the callers terminal generates the CLI information that is received from the IP network for the VoIP service. This means that this should be considered to be a user provider not verified number not a network number that is generated from the PSTN/ISDN networks. For SIP technology a p-asserted identity should be utilized to provide the network number to enable the CLI services to be correctly applied. For non-SIP VoIP services then the CLI services cannot be guaranteed which renders this to be unsuitable for public telephony services, unless appropriate mechanisms are developed.

A further problem is outlined below in figure 4 where a user has tunnelled a connection from LAN B to LAN A, a scenario that is common as ETSI delegates tunnel from ETSI LAN back to a respective company LAN. So from the LAN administrator's view in LAN A the location information may not reflect the true location of the mobile data user but only the point of ingress to LAN A.

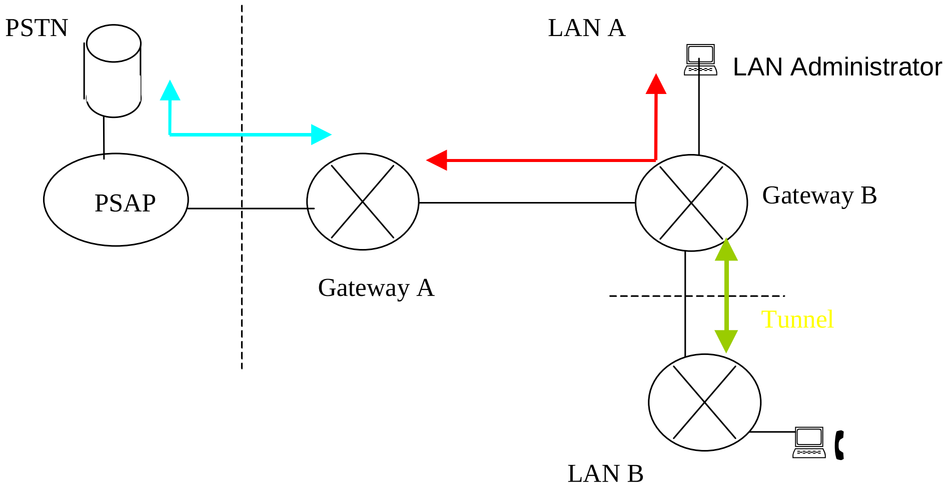

Figure 4: Problem of location information from LAN administrator

So for VoIP type calls the location information of the caller to the PSAP is in need of being standardized.

With Voice over ATM networks this is dependant on how the protocols have been built. Employing ISUP/BICC on an ATM network will give the same information as an ISUP/BICC network on a switched circuit network (SCN). So the CLI can be network generated and deliver the same level of location information that is delivered by a SCN today.

However if there is a VoIP service that is using the ATM transport, to deliver the required QoS for voice, then the problems identified for IP networks above will also apply here.

It should be noted that the TIPHON technical report [6] deals with the Authority-to-Authority scenario and so does not cover the citizen to the Authority scenario.

4.1.3.2 Message data based users

Data, fixed and mobile networks are also capable of delivering data as well as voice to the PSAP, in the form of email and SMS messages respectively. This form of contact suffers from the problem that the location cannot be confirmed in real time by the caller as is done by voice communication, provided the caller is capable of speaking or speaks the same language as the PSAP operator. Since a SMS message includes the CLI a distinction has to be made between a short message sent from a fixed network access and a short message sent from a mobile network access.

Text from Email to the PSAP has all the problems outlined by SMS messaging to the PSAP and has the same problems as the VoIP scenario as well.

4.1.4 Alarm data users

This has been investigated by this STF and it is believed that there are no problems for ETSI SPAN as alarm devices are fixed in the network therefore location information rarely changes.

4.2 Multiple PSAP and cross border protocol interfaces

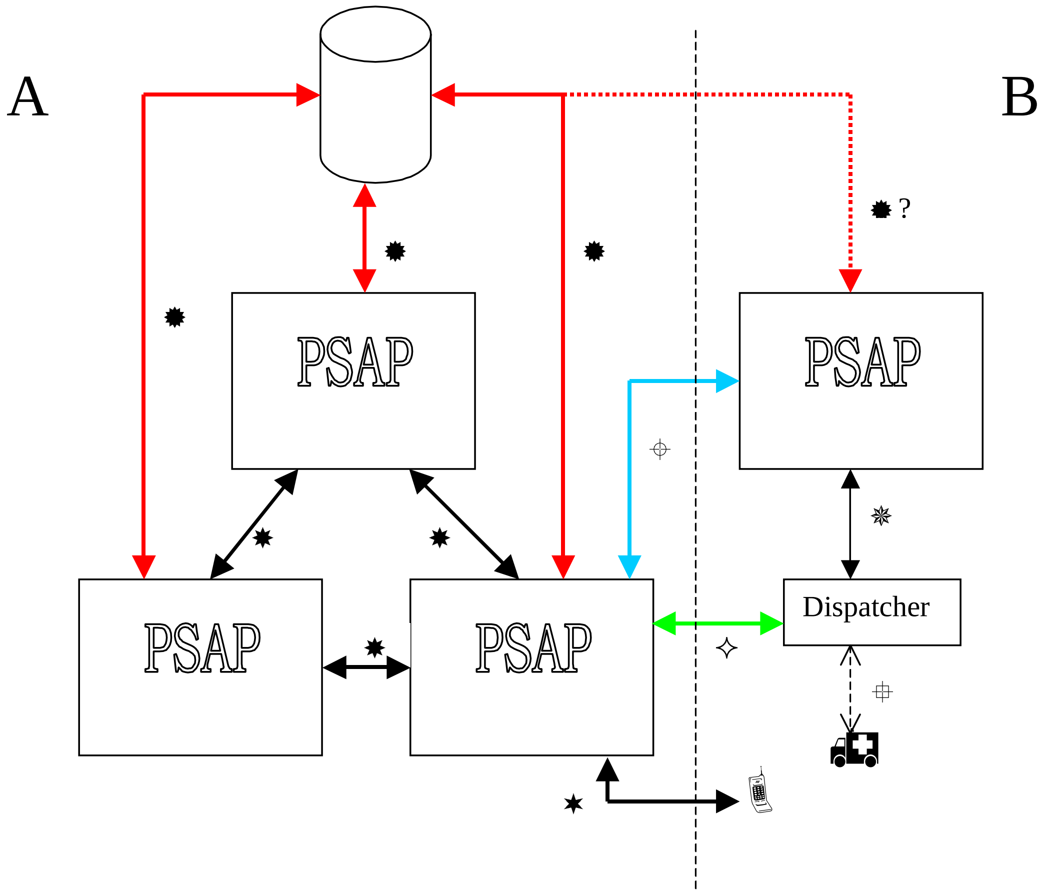

Figure 5: Functional architecture of multiple PSAP and a cross border EMTEL call

Figure 5 shows a possible fully integrated PSAP platform. Not shown here is the possibility of a similar architecture showing multiple databases that are fully integrated to allow for redundancy. This would mean that if a problem occurs in either a PSAP or database there is always a backup to take over the handling of emergency calls.

The interconnection, within a single regulatory environment, of the PSAPs via ② interface can be achieved in a number of ways two examples are:

1) using the existing PSTN/ISDN networks to connect the voice and data;

2) a dedicated VPN type service that could employ any technology e.g. SCN or IP. As long as this interconnection is within a single regulatory environment within A, then this is not a matter for ETSI to get involved with.

ETSI should only get involved if the interconnect of an emergency call crosses a regulatory boundary or a cross border EMTEL call is made. Figure 5 illustrates such a problem:

The scenario is that a 112 call ① from a mobile is made in a border town in country B, but the mobile is still logged onto a cell across the border in country A. The 112 call will then be directed to a PSAP in country A the location information is such that the PSAP recognizes that the call originates from country B. The problem then for the PSAP in country A is to pass the call over to a PSAP or a dispatcher in country B.

This could be achieved by diverting the call to the PSAP in country B by PSTN/ISDN services. The problem with this method is that this call ⑥ would not be recognized as an emergency call but just an ordinary international call. This would mean that for normal circumstances the call would be completed if the PSAP in country B can accept international calls. However if there was a high level of congestion on the international network unless this call has been marked as an emergency call then it may not be able to route into country B. This mark has been accepted in the ITU-T and in ETSI as a new CPC value but the international exchanges will need to be upgraded to implement these new procedures.

Another method for the PSAPs to communicate and at the same time not be impacted by any congestion in the international network would be to extend the VPN type interconnection that exists in country A as shown in interface ② across the international boundary between country A and B. This could be achieved on a bilateral basis. Or if this was to be extended this could be achieved by making this interface ⑥ a new standard.

Another method could be to bypass the PSAP in country B altogether and allow the PSAP in country A to either dispatch the emergency service to the emergency in country B or to pass the information over directly to the dispatcher within country B. This would mean that if this was to be allowed then either an international call would have to be made with the same problems that exist in the previous paragraph or the interface between the PSAP and the dispatcher ④ is extended to cross international boundaries as ⑦, this would then have to be a new ETSI standard.

The last problem for this scenario is the interpretation of the EU data protection act. Is the location information held on the database in country A allowed to be transmitted to either the dispatcher or PSAP in country B?

To allow any of the above would probably need the regulatory environments in countries A and B to have a very close cooperation. This is not however an ETSI problem.

5 Disaster communications

This clause outlines the actions that may be put into place and extrapolates the requirements that may be put into place to deal with a disaster. It should be noted that this clause of the present document has only considered a disaster that occurs within the European sphere and does not consider disasters that occur elsewhere in the world. The disaster is such that the telecommunications infrastructure, this includes PSTN exchanges, GSM cells, IP Routers and line plants, has been damaged beyond repair within the locality. See the fig 06 below.

This clause has been split into three parts where the first part is the requirements for telecommunications in the period that is prior to a known disaster occurring.

The second part is the immediate requirements for the telecommunications network in the period that an unforeseen disaster occurs.

The third part is the long-term requirements for the disaster communications and takes place after the immediate actions have taken place and now a command structure is put in place on the ground and possibly remotely.

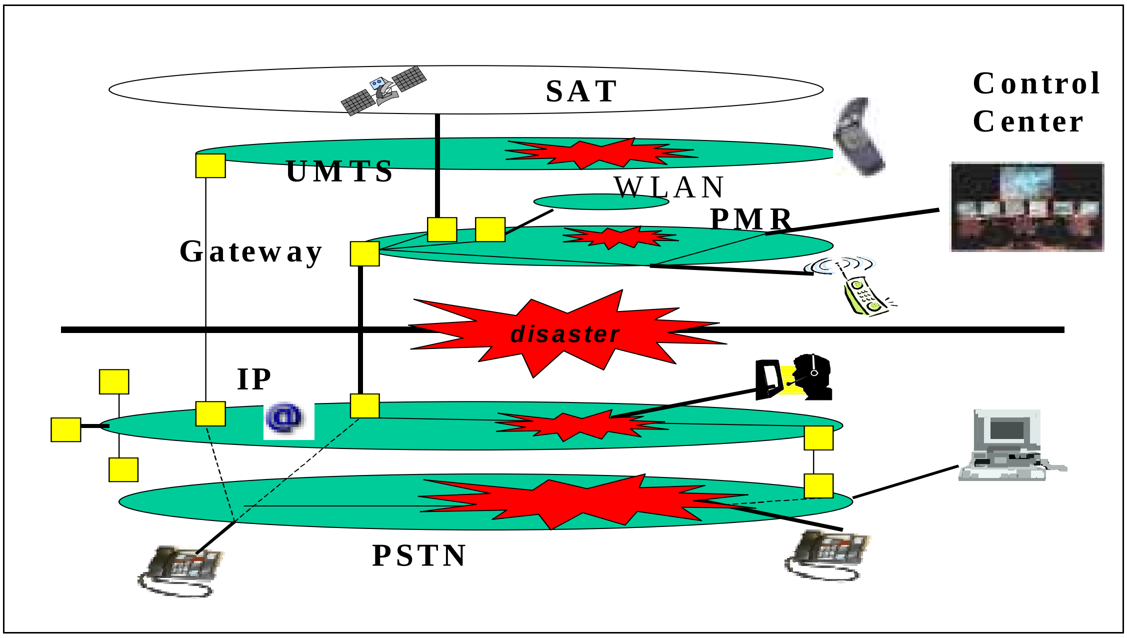

Figure 6: Impact on telecommunications infrastructure in the case of a disaster

5.1 Pre-disaster requirements

5.1.1 Unknown disasters

Most networks cooperate with any disaster plans put in place by the respective governments; they also have disaster recovery programmes in place to deal with telecommunication disasters like exchange failure. As far as signalling is concerned there is no special further requirements needed so there is no work for ETSI in this scenario.

5.1.2 Known disasters

If there is a disaster about to happen e.g. flooding then there may be a need for the emergency authorities to broadcast to a large number of people in the disaster zone.

For the fixed line networks there may be many alternatives to achieve this requirement, e.g. from automatic dialling devices on each exchange to using the IN platform. There is no one standard for this service; this may be an area that ETSI should be involved in.

For mobile users receiving a broadcast is dependent on the technology of the mobile handset e.g. it may be possible for mobiles that have a commercial radio reception to interrupt the radio for an announcement. The one technology that all mobiles have is the ability to receive SMS text messages so it should be possible for all mobiles within a cell area to receive a text message. It also may be possible for any mobile that has roamed into the cell area to be given a text message in the language of the handset, as messages are sent to mobiles today welcoming them onto a roamed network in the language of the handset.

For the data user the broadcasting of announcements is part of the protocol and does not require further work from ETSI. The first problem is that not all data service providers have implemented and therefore do not support the broadcasting of public emergency announcements. Terminals are able to support simultaneously a number of different applications that are capable of receiving a public emergency announcement e.g. email, pop up window from WWW. Consideration is required on the service interaction when simultaneous warnings are received on the same topic.

At present it is unclear to the author what would be the method of achieving this broadcast. It could be a mixture of different methods for the different users. But it is also clear that the media broadcast services would be deployed as well as telecommunications methods such as text messaging every mobile handset within an area.

A further consideration is that the type of disaster such as flooding or poison gas leakage does not respect man made boundaries so it may be worth considering this broadcast across network and country boundaries. This could be technically possible for all the types of users considered above, but would require some regulatory input.

5.2 Immediate requirements

5.2.1 Citizen to authority

When the disaster first strikes then there may be no communication in any form from the effected area, but from the outside of this area there may be a very large number of calls from good Samaritans dialling 112. When the news of this disaster reaches the population a very large number of calls will be generated to the affected area from friends and family of people in the area. This could impact adversely upon the telecommunications networks causing congestion. The current network management controls should be capable of dealing with this.

There could also be a situation where communications from one or more of the technologies within the disaster area may still be functioning e.g. PSTN exchanges may not be functioning but one or more GSM mobile cells in the area, or connections to an ISP may be still functioning. In this case the PSAP needs to obtain location information from any survivors using these technologies so that it can pass over to an emergency service the appropriate information.

This form of communication from the citizen requesting assistance could be in form of text messages either from a GSM mobile phone or from email. The problems of obtaining location information from data networks or SMS messages were outlined in the previous clause so there is no need to restate them here.

The WERT report [4] identified a number of calls made to relatives and loved ones from the towers via mobile networks. This call information could be of use in physically locating survivors. So it may be of use to extend the location information to all calls not just emergency calls in a disaster area.

The use of the devices attempting to page for service connection could also be used to find the location of trapped people. In order for this facility to be effective over a longer period of time the time between page requests is increased from say 10 seconds to 10 minutes. This will preserve the battery life of the mobile device and would ease any congestion on the network caused by mobile devices attempting to log onto a temporary radio link.

5.2.2 Authority to authority

It should also be self evident that for a disaster for which no warning is possible then there would be no immediate emergency command structure in place but this should have been planned for and any disaster plans initiated.

It may be that the PSAP will have to act as the initial command centre and would need to communicate with the various bodies such as the emergency services themselves.

If the PSAP has the information that a particular utility would be required to deal with the disaster e.g. water needs diverting or gas turned off, then the PSAP may contact the utility providers to initiate the relief process. For the PSAP to initiate this it will need to have the ability to make priority calls within the telecommunications networks.

Within the disaster area there is a need for the emergency services to be able to communicate with each other, this could be achieved by filtering call attempts and only allowing a predetermined set of SIMs to be able to use this radio link.

The disaster area could be linked to not affected parts of the network either by line of sight radio communication or by running a trunk into the area.

5.2.3 Authority to citizen

Technically this is not any different from the previous clause (5.1.2) for the broadcasting of warnings etc. prior to an emergency occurring.

In the initial phase of the disaster it could be very difficult to establish the exact nature of the emergency, but there may be a need to issue a standard warning to evacuate or close doors/windows etc. from the areas adjacent to the disaster area.

The use of cell broadcast with SMS to mobile users may be a problem as the network would be congested and SMS messages do not have a high priority so may be delayed.

If no telecommunication is possible then initially loud hailers could be deployed for broadcasting to people within the disaster area but to achieve a consistent message flow the authorities need to be able to inter communicate.

5.3 Long term requirements

The long-term requirements are based upon the assumption that after the disaster has occurred then a disaster HQ has been set-up to coordinate the emergency services. This could be a mobile centre within the area itself or it has been set-up outside the area and communicated to emergency services within the area.

As it has been assumed that all communication infrastructure has been putout of action all communications has to be via radio (TETRA/GSM etc.). Project MESA [5] reports give the requirements for the creation of universal specifications and standards.

5.3.1 Citizen to authority

In the worst-case scenario no communication is possible from the disaster area, but there is a need to for the general population to be able to communicate both with friends and family and the emergency authorities.

This could be achieved by the disaster recover programmes that most network operators have in place which could entail putting in a radio network for line of sight communication to the network and setting up a number of mobile payphone boxes, or using the radio network to establish a mobile cell etc. Then a number of these temporary phones could be directly routed to an emergency authority and others set-up so that a call would only be established for a limited time, these would all be incoming call barred.

The WERT report identified a need to locate possible survivors in the disaster area where survivors have a number of mobile terminals such as GSM phones or pagers which try to log onto a network when a signal is present. This could be used to locate the phone or pager by triangulation. If the phone attempts to answer or initiate a call or send an SMS then a survivor is near by. This highlights the need that location information from text messaging is required. With the developments in the mobile industry (3GPP) to handle emails this requirement will have to be extended into UMTS and IP area.

5.3.2 Authority to authority

It has been highlighted in various presentations to workshops that there is a need for cross emergency service communication, and each emergency service has its own equipment.

Common communication equipment needs to be defined. This could be TETRA as one of the options as outlined in the MESA report [5].

Each emergency service also has its own specialized equipment e.g. telemedicine data back to hospitals, chemical storage data for fire fighters etc which is not required across emergency services. However some data is also common across the emergency services e.g. area maps etc. and there may be a need to have a standardized protocol for communication between emergency services to share relevant data.

5.3.3 Authority to citizen

The same requirements for claue 5.2.3 should also be applied to this clause.

The WERT [4] report indicates a need to communicate with trapped survivors via voice and text including email.

6 Requirements on NGN/IP networks

From the workshops and discussions held in various standards fora there seems to be a common set of requirements emerging for the NGN/IP networks. These can be categorized as follows:

- There is a need to specify EMTEL capability now, not retrofit later.
- Solutions need to be reliable, affordable, backward capable, interoperable to existing systems. It would also be useful to keep the use of the technology simple as it is not seen as helpful to have the emergency service personnel requiring days of training in order to employ the new technology.
- It has been recognized that the protocols such as SIP that uses the IP technology does not recognize country boundaries, so it is important that any service specified does not compromise existing systems.

- There has been a need identified to specify an IP EMTEL marker so communications of emergency service personnel are given priority within the network. At network saturation availability due to congestion is still a problem for IP networks so a priority mechanism is required.

- There is a need to have a very secure authentication of IP EMTEL emergency service personnel priority users so that a country's service is not compromised by attacks to access the priority marker, as this is seen to be under the control of specific governments. Although I have not seen how a priority user registers as an authorized priority user in a congested network, I suppose that he/she will have to potluck along with everyone else.

- It has been identified that voice is a minimum service requirement for the emergency service personnel, but it should be noted that with IP networks pictures, video and data communication services would also be available.

- To support voice a certain level of QoS is required but it may in very catastrophic situations not need to be as good as the commercial voice QoS as degraded communication is better than no communication. This principle should also be applied to the other services, pictures, video and data.

- There is a need to accommodate differing emergency services communications technologies. The interoperability of these differing technologies and tools employed by the emergency services is further complicated by the fact that IP communications may be across national borders. This means that there is a need to standardize the communication and co-ordination between these tools.

- It has been recognized that for most disaster situations mobile technology is usually the key (TCP/IP over satellite links?).

As with normal telecommunications the main problem with the migration from SCN SS7 technology to the packet IP technology is with QoS and security although for emergency service personnel the requirement maybe different, e.g. a higher level of security and a lower level of QoS.

The internet is developed by the IETF which at present is working on a set of documents to support emergency telecommunications but the assumption that has been made in the discussions is that the USA system GETS is the service for emergency telecommunications. A European standard is required. The set of documents being produced by the IETF needs to be carefully looked at to ensure it is fit for purpose for the European Emergency Telecommunications.

It should also be noted, that the location information problem as outlined in clause 4.1.3 also needs to be taken into account.

7 Recommendations

1) From the above clause 4 it can be seen that work may need to be done to extend the service on the PSAP to accept a call for emergency assistance from non real time communications. These are principally SMS and email text messages. The problems outlined in the present document are:

   - These are not real time services, but are widely used. How can these services deliver the message within an agreed timescale?

   - Location information from these services has not been standardized if they are available to the underlying network technologies and this needs to be developed.

   ETSI SPAN could start to undertake this task and previously mentioned tasks by feeding in the requirements to the standards fora that are responsible for the protocols. This would require for the email work that ETSI provides the IETF a draft RFC which would have to be taken up with the ETSI membership and would also require attending the IETF.

   ETSI SPAN could initiate the work for the GSM SMS service by the members of ETSI who are also members of 3GPP.

   For this work to be initiated it would first require that the regulatory bodies including the EU take a lead to ascertain if this is what the users would want and if the network operators can support this extension of the service.

2) From clause 4.1.2 it can be seen that work needs to be initiated to support the E-MERGE project, as it is not clear whether and, how the protocol developed from this project is supported in the public network. Since this information is to be carried in the fixed line network to the PSAP then ETSI SPAN will need to do some work, but clarification is required.

3) From clause 4.1.3 it can be seen that the location of a roaming data terminal is problematic and the interrogation of a LAN/WAN administrator and the interworking of this information to the location database can be worked on by ETSI SPAN taking into account the problems that have been outlined in this clause.

4) In clause 4.1.3.2 SMS message is used to contact the PSAP to ask for assistance from the E112 service. What are the view and requirement of the Commission?

5) From clause 4.2 it can be seen that to support a cross border PSAP interworking then some new protocols will need to be developed. However before the work could begin the regulatory boundaries with regard to data being sent across country borders may need to be investigated. The boundaries of a PSAP in one country contacting an emergency service in another etc. need to be overcome. It may well be that there is no need for ETSI to do any further work as this has already been implemented in non-standard bilateral agreements.

6) From clause 5 the main problem outlined was the authority to citizen scenario and the broadcasting of warnings to the public when a disaster is imminent or has occurred. The problems in this area are the differing types of terminal that are available, so a cell broadcast of SMS could be employed for mobile users but this would only be of limited use in the fixed network. Automatic calling of everyone on an exchange in the disaster area could be deployed, the use of a radio broadcast is another option, this could use the same technology as traffic announcements in cars. The solutions are even more numerous than suggested above so there would not be a single standard method of achieving the broadcast, so this would also require a regulatory input for this service to be implemented across the EU.

7) From clauses 6 and 4.1.3 it can be seen that there is a lot of work for the emergency service to be implemented upon a data network. This would require that work for NGN needs to start to integrate the requirements in when the networks are designed and this work is being done by ETSI SPAN in the architecture work now by the membership.

   How the location information of the emergency call from this NGN based on IP technology is obtained still requires a lot of work and it is unclear where this is being done. ETSI SPAN can work on this activity.

   All the requirements in clause 6 need to be taken into account in the NGN IP based network if they are to provide an emergency service to their users.

History

Document history		
V1.1.1	October 2003	Publication