ETSI TR 102 445 V1.2.1 (2023-04)

TECHNICAL REPORT

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

Reference
RTR/EMTEL-00061

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

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

Modal verbs terminology

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

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

Introduction

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

In emergency situations, efficient and effective communications are critical. The enabling communication technologies need to perform in a robust and reliable manner, providing the requisite functionality to guaranteed service levels. Network and other emergency communication services resilience and preparedness are important factors in that aim.

The objective of the present document is to provide guidelines and recommendations to maximize the level of preparedness and resilience of emergency communication services based on identified risks for involved technologies.

Clause 4 provides an overview of several key technical concepts that can be employed to enhance the preparedness and resilience of emergency communication networks and services. The four main Emergency Communication Service (ECS) areas considered in the present document include communications from individuals with public authorities/organizations, communications between authorities/organizations (including mission critical communications), communications from authorities/organizations to the individuals (including public warning) and communications amongst individuals.

The analysis in clause 7 starts with a study of the potential threats that may affect these ECS, complemented by general guidelines to address these risks. In a second step, the analysis summarizes common physical dependencies for the technologies enabling ECS and provides generic recommendations to prevent failures and malfunctions.

Clause 8 provides a detailed analysis of the enabling technologies that support the different components involved in ECS. This detailed analysis includes for each enabling technology: the list of risks that may directly affect that technology, specific measures that may be taken for that technology, in addition to those already described in clause 4 and in clause 7, and the list of underlying infrastructures that may have an impact on that technology. This analysis is completed by the identification of the main physical dependencies that may directly affect each technology. For clarity reasons only risks with the potential to directly affect technologies are considered; indirect threats can be traced via the physical dependencies and underlying infrastructure chains.

Clauses 9 to 12 provide similar detailed analysis for the different components of each of the four main ECS areas considered in the present document.

Annex A introduces the main entities/roles and typical communication channels involved for fully deployed management of large-scale incidents.

Annex B includes a short presentation of each of the components contributing to the ECS for the four main ECS areas listed above, a short presentation of the enabling technologies analysed in clause 8, and ends with a summary of several external activities addressing preparedness and resilience.

The concepts and analysis in the present document are expected to be useful to emergency services authorities and decision-makers when setting-up or updating their communication networks and services, as well as to other interested stakeholders. Readers are recommended to start with clauses 4 and 7, as the majority of guidelines is provided in these two clauses. They may then select their topics of interest in clauses 8 to 12, as well as in annexes A and B, for a complete information.

1 Scope

The present document presents resilience concepts and considers their application within technical systems enabling emergency communications. Furthermore, it considers preparedness of emergency communication services and proposes guidelines for specialized systems and capabilities.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

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

[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] Centre for the Protection of National Infrastructure (CPNI): "Responding to Terrorist Incidents; Developing Effective Command and Control; Supplementary Guidance - Communication Technology", March 2023.

[i.5] ISO 22301:2019 (October 2019): "Security and resilience -- Business continuity management systems -- Requirements".

[i.6] 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.7] WHO guidance for business continuity planning, WHO/WHE/CPI/2018.60 (2018).

[i.8] Government of Canada, Minister of Public Works and Government Services: "A Guide to Business Continuity Planning", ISBN 0-662-33764-6.

[i.9] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[i.10] ETSI TS 103 479: "Emergency Communications (EMTEL); Core elements for network independent access to emergency services".

[i.11] ETSI TS 122 101: "Universal Mobile Telecommunications System (UMTS); LTE; Service aspects; Service principles (3GPP TS 22.101)".

[i.12] ETSI TS 122 173: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Core Network Subsystem (IMS) Multimedia Telephony Service and supplementary services; Stage 1 (3GPP TS 22.173)".

[i.13] ETSI TS 123 167: "Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) emergency sessions (3GPP TS 23.167)".

[i.14] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[i.15] ETSI TS 103 478: "Emergency Communications (EMTEL); Pan-European Mobile Emergency Application".

[i.16] ETSI TS 103 755: "Emergency Communications (EMTEL); PEMEA ESInet Shared Services".

[i.17] ETSI TS 103 625: "Emergency Communications (EMTEL); Transporting Handset Location to PSAPs for Emergency Communications - Advanced Mobile Location".

[i.18] TS 17184:2018: "Intelligent transport systems - eSafety - eCall High level application Protocols (HLAP) using IMS packet switched networks" (produced by CEN).

[i.19] EN 16062:2015: "Intelligent transport systems - Esafety - eCall high level application requirements (HLAP) using GSM/UMTS circuit switched networks" (produced by CEN).

[i.20] EN 15722:2015: "Intelligent transport systems - Esafety - eCall minimum set of data" (produced by CEN).

[i.21] IETF RFC 8147: "Next-Generation Pan-European eCall".

[i.22] ETSI TS 126 267: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); eCall data transfer; In-band modem solution; General description (3GPP TS 26.267)".

[i.23] ETSI CTI Plugtests Report V 1.0 (2017-04): "2nd NG112 Emergency Services Plugtest".

[i.24] ETSI CTI Plugtests Report V0.0.3: "1st NG112 Emergency Services Plugtest".

[i.25] ETSI CTI Plugtests Report V1.0 (2019-01): "3rd NG112 Emergency Services Plugtest".

[i.26] ETSI CTI Plugtests Report V0.4 (2021-05) "4th NG112 Emergency Services Plugtests", 22nd February to 5th March 2021.

[i.27] C/S G.003 "Introduction to the Cospas-Sarsat System".

[i.28] ETSI TS 101 470: "Emergency Communications (EMTEL); Total Conversation Access to Emergency Services".

[i.29] ETSI TR 103 201: "Emergency Communications (EMTEL); Total Conversation for emergency communications; implementation guidelines".

[i.30] ETSI TS 103 698: "Emergency Communications (EMTEL); Lightweight Messaging Protocol for Emergency Service Accessibility (LMPE)".

[i.31] ETSI TS 103 756: "Emergency Communications (EMTEL); PEMEA Instant Message Extension".

[i.32] ETSI TS 129 002: "Digital cellular telecommunications system (Phase 2+) (GSM) ;Universal Mobile Telecommunications System(UMTS); LTE; 5G; Mobile Application Part (MAP) specification (3GPP TS 29.002)".

[i.33] Recommendation ITU-T Q.700: "Introduction to CCITT Signalling System No. 7".

[i.34] Europe's Digital Decade: digital targets for 2030.

[i.35] ETSI TR 103 708: "Human Factors (HF); Real-Time Text (RTT) in Multiparty Conference Calling".

[i.36] NIST Special Publication 800-39: "Managing Information Security Risk; Organization, Mission, and Information System View", March 2011.

[i.37] ETSI TS 103 871: "Emergency Communications (EMTEL); PEMEA Real-Time Text Extension".

[i.38] ETSI TS 103 872: "Emergency Communications (EMTEL); PEMEA Service Discovery Extension".

[i.39] European Commission COM/2022/551: "Council recommendation on a coordinated approach by the Union to strengthen the resilience of critical infrastructure", 18.10.2022.

[i.40] OASIS Standard 200402: "Common Alerting Protocol, v. 1.0"; document identifier: oasis-200402-cap-core-1.0.

[i.41] ETSI TS 103 337: "Satellite Earth Stations and Systems (SES); Satellite Emergency Communications; Multiple Alert Message Encapsulation over Satellite (MAMES)".

[i.42] ETSI TS 122 268: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Public Warning System (PWS) requirements (3GPP TS 22.268)".

[i.43] ETSI TS 102 900: "Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service".

[i.44] BoR (20) 115: "BEREC guidelines on how to assess the effectiveness of public warning systems transmitted by different means") using the Cell Broadcast Service".

[i.45] ETSI TR 118 546: "oneM2M: Study on Public Warning Service Enabler (oneM2M TR-0046 v4.0.0 Release 4)".

[i.46] ETSI TS 123 041: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041)".

[i.47] European Commission C(2022)9394: "(Draft) Delegated regulation of 16.12.2022 supplementing Directive (EU) 2018/1972 of the European Parliament and of the Council with measures to ensure effective access to emergency services through emergency communications to the single European emergency number '112'", December 2022.

[i.48] ETSI TS 103 260-1: "Satellite Earth Stations and Systems (SES); Reference scenario for the deployment of emergency communications; Part 1: Earthquake".

[i.49] 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.50] ETSI EN 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[i.51] ETSI EN 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

[i.52] TETRAPOL PAS 0001-1-1: "TETRAPOL Specifications; Part 1: General Network Design; Part 1: Reference Model".

[i.53] TIA TSB-102-D: "Project 25 TIA-102 Documentation Suite Overview".

[i.54] ETSI TS 102 658: "Digital Private Mobile Radio (dPMR) using FDMA with a channel spacing of 6,25 kHz".

[i.55] ETSI TS 102 361 (parts 1 - 4): "Electromagnetic compatibility and Radio spectrum Matters (ERM); Digital Mobile Radio (DMR) Systems".

[i.56] ETSI TS 122 179: "LTE; 5G; Mission Critical Push to Talk (MCPTT); Stage 1 (3GPP TS 22.179)".

[i.57] ETSI TS 122 280: "LTE; 5G; Mission Critical Services Common Requirements (MCCoRe); Stage 1 (3GPP TS 22.280)".

[i.58] ETSI TS 123 283: "LTE; Mission Critical Communication Interworking with Land Mobile Radio Systems (3GPP TS 23.283)".

[i.59] ETSI TS 123 180: "LTE; Mission critical services support in the Isolated Operation for Public Safety (IOPS) mode of operation (3GPP TS 23.180)".

[i.60] 3GPP TR 23.700-24: "Study on support of the 5G MSG (Message) Service".

[i.61] ETSI TS 123 289: "5G; Mission Critical services over 5G System; Stage 2 (3GPP TS 23.289)".

[i.62] ETSI TS 129 500: "5G; 5G System; Technical Realization of Service Based Architecture; Stage 3 (3GPP TS 29.500 Release 16)".

[i.63] ETSI GR MEC 031: "Multi-access Edge Computing (MEC) MEC 5G Integration".

[i.64] ETSI TS 123 558: "5G; Architecture for enabling Edge Applications (3GPP TS 23.558)".

[i.65] ETSI TS 123 479: "LTE; Technical Specification Group Services and System Aspects; UE MBMS APIs for Mission Critical Services; (3GPP TS 23.479)".

[i.66] 3GPP TR 23.792: "Study on MBMS APIs for Mission Critical Services".

[i.67] GSMA^{TM} white paper: "Network 2020: Mission Critical Communications", January 2018.

[i.68] ITU Study Group 2 Question 5: "Utilizing telecommunications/information and communication technologies for disaster risk reduction and management", 2021.

[i.69] GSMA^{TM}: Emergency Communication Version 1.0.

[i.70] ETSI TR 103 582: "EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations".

[i.71] ETSI TR 103 166: "Satellite Earth Stations and Systems (SES); Satellite Emergency Communications (SatEC); Emergency Communication Cell over Satellite (ECCS)".

[i.72] IEEE 802.11s^{TM}: "IEEE Standard for Information Technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking".

[i.73] Meshtastic project.

[i.74] ETSI TS 122 125: "5G; Unmanned Aerial System (UAS) support in 3GPP (3GPP TS 22.125)".

[i.75] 3GPP TR 23.755: "Study on application layer support for Unmanned Aerial Systems (UAS)".

[i.76] Public Safety Digital Transformation: "The Internet of Things (IoT) and Emergency Services. EENA Technical Committee Document".

[i.77] Recommendation ITU-T Q.3060 (12/2020): "Signalling architecture of the fast deployment emergency telecommunication network to be used in a natural disaster".

[i.78] Broadband Forum Reports.

[i.79] NEMA member report (01/2021): "Storm Reconstruction Guidebook: Rebuild Smart".

[i.80] ETSI TS 133 401: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401)".

[i.81] ETSI TS 133 501: "5G; Security architecture and procedures for 5G System (3GPP TS 33.501)".

[i.82] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

[i.83] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[i.84] Commission Delegated Regulation (EU) 2019/320 of 12 December 2018 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements set out in Article 3(3)(g) of that Directive in order to ensure caller location in emergency communications from mobile devices.

[i.85] Recommendation ITU-T E.409 (05/2004): "Incident organization and security incident handling: Guidelines for telecommunication organizations".

[i.86] ITU-T FG-DR&NRR: "Overview of Disaster Relief Systems, Network Resilience and Recovery".

[i.87] ITU-T Technical Report on Telecommunications and Disaster Mitigation.

[i.88] ITU-T Gap Analysis of Disaster Relief Systems, Network Resilience and Recovery.

[i.89] ITU-T Requirements on the improvement of network resilience and recovery with movable and deployable ICT resource units.

[i.90] GSMA National Emergency Telecommunications Plans: Enablers and Safeguards. A brief evaluation guide for policy practitioners.

[i.91] ITU Guidelines for national emergency telecommunication plans.

[i.92] FCC Report and Order for Resilient Networks, July 6, 2022.

[i.93] National Coordinating Center for Communications (NCC): "Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment", February 5, 2019.

[i.94] MIL-STD-188-125-1: "Department of Defense Interface Standard. High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-urgent Missions", 17 July 1998.

[i.95] ETSI TS 122 011: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Service accessibility (3GPP TS 22.011)".

[i.96] United Nations Sendai Framework: "The Sendai Framework for Disaster Risk Reduction 2015-2030", March 2015.

[i.97] EC COM(2022) 454: "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020", Brussels, 15.9.2022.

[i.98] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

[i.99] ETSI GS NFV-REL 001: "Network Functions Virtualisation (NFV); Resiliency Requirements".

[i.100] ETSI GS NFV-REL 003: "Network Functions Virtualisation (NFV); Reliability; Report on Models and Features for End-to-End Reliability".

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] and the following apply:

app: any communications application, standalone or in a web browser, running on any kind of device, that a person is able to use to initiate an emergency communication to request help

application enabler: communication functionality offered to emergency communication applications to support their execution

call: any type of emergency communication and associated media (analogue or digital) initiated by an individual towards authorities to request help from them

NOTE: This definition applies to the present document.

common operating picture: single display of information collected from and shared by more than one agency or organization that contributes to a common understanding of a situation and its associated hazards and risks along with the position of resources and other overlays of information that support individual and collective decision making

DCF77: longwave time signal and standard-frequency radio station in Mainflingen, Germany, operated by Physikalisch-Technische Bundesanstalt

NG112: ESInet networking infrastructure and the associated core elements of the NG112 architecture

NOTE: This definition refers to ETSI TS 103 479 [i.10] and is used as a shortened term in the present document.

preparedness: measures to anticipate and prevent failures and outages, i.e. to reduce the risk of a communication service outage

NOTE: Examples are redundant hardware, uninterruptible power supplies, hardening of cables, etc. All these measures increase the availability of a service/system in the context of Emergency Communication Services (ECS). See also: United Nations International Strategy for Disaster Reduction, and more specifically the Sendai framework [i.96].

resilience: measures taken during a system outage alleviating the direct consequences of the outage and allowing the system to return to normal operation

NOTE: Resilience has two aspects:

i) recovery understood as "getting the affected system back to normal operation as fast as possible" (decreasing the mean time to repair); and

ii) measures for alternative services to be taken during a system outage alleviating the direct consequences of the outage.

The latter should be described in a contingency plan, and includes for example having at hand portable nomad TV transmitters to deploy after an earthquake destroyed the legacy infrastructure.

WWVB: time signal radio station near Fort Collins, Colorado, U.S.A., operated by the National Institute of Standards and Technology

3.2 Symbols

Void.

3.3 Abbreviations

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

AAIM	Airborne Autonomous Integrity Monitoring
ABAS	Aircraft-Based Augmentation System
ADS-B	Automatic Dependent Surveillance - Broadcast
AI	Artificial Intelligence
AIS	Automatic Identification System
AM	Amplitude Modulation
AML	Advanced Mobile Location
AoA	Angle of Arrival
AoD	Angle of Departure
AP	Application Provider node
APCO	Association of Public safety Communications Officials
ASP	Aggregating Service Provider node
BCF	Border Control Function
BEREC	Body of European Regulators for Electronic Communications
CAP	Common Alerting Protocol
CBS	Cell Broadcast Service
CCS7	Common Channel Signalling system number 7
CER	Critical Entities Resilience
CI/CD	Continuous Integration and Continuous Deployment
CID	Cell ID
CMAS	Commercial Mobile Alert System
COLT	Cell On Light Trucks
COW	Cell On Wheels
CPNI	Centre for the Protection of National Infrastructure
CPE	Customer Premise Equipment
D2D	Device to Device (communication)
DAB	Digital Audio Broadcasting
DMO	Direct Mode Operation
DMR	Digital Mobile Radio
DNS	Domain Name Service
DoS	Denial of Service
dPMR	digital Private Mobile Radio
DR	Disaster Recovery
DRR	Disaster Risk Reduction
DVB	Digital Video Broadcasting
EC	European Commission
ECC	Emergency Control Centre
ECCS	Emergency Communication Cell over Satellite
ECID	Enhanced CID
ECRF	Emergency Call Routing Function
ECS	Emergency Communication Services
EECC	European Electronic Communications Code
E-LORAN	Enhanced Long Range Navigation (also known as eLORAN)
eMBMS	Evolved MBMS
EMP	Electromagnetic pulse
EMTEL	Emergency Communications
ESA	European Space Agency
ESInet	Emergency Services IP network
ESRP	Emergency Services Routing Proxy
ETSI	European Telecommunications Standards Institute
ETWS	Earthquake and Tsunami Warning System
EU	European Union
FCC	Federal Communications Commission
FDMA	Frequency-division Multiple Access
FECC	Field Emergency Control Centres
FM	Frequency Modulation
FTTH	Fibre To The Home

FTTN	Fibre To The Node
FTTP	Fibre To The Premises
GBAS	Ground-Based Augmentation System
GCSE_LTE	Group Communications System Enablers for LTE
GIC	Geomagnetic Induced Current
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile telephony
GSMA	GSM Association
HFC	Hybrid-Fibre Coaxial cable
HLR	Home Location Register
HPUE	High Power UE
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
ID	Identity
ID/IP	Intrusion Detection and Intrusion Prevention
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IOPS	Isolated Operations of Public Safety
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM	Integrity Support Message
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union Telecommunications standardization sector
LB-SMS	Location Based SMS
LEMA	Local Emergency Management Authority
LIS	Location Information Server
LMPE	Lightweight Messaging Protocol for Emergency service accessibility
LPWAN	Low Power Wide Area Network
LTE	Long-Term Evolution
MAMES	Multiple Alert Message Encapsulation over Satellite
MBMS	Multimedia Broadcast/Multicast Service
MC	Mission Critical
MCData	Mission Critical Data
MCVideo	Mission Critical Video
MCPTT	Mission Critical Push-To-Talk
MEC	Multi-access Edge Computing
MO	Mobile Originated
MS	Mobile Station
MSC	Mobile Switching Centre
MSD	Minimum Set of Data
NAS	Non-Access Stratum
NASA	National Aeronautics and Space Administration
NCC	National Coordinating Center for Communications
NEMA	National Electrical Manufacturers Association
NETP	National Emergency Telecommunication Plan
NFV	Network Function Virtualisation
NGO	Non-Government Organization
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NR	New Radio
NRR	Network Resilience and Recovery
NTP	Network Time Protocol
OTDOA	Observed Time Difference Of Arrival

OTT	Over-The-Top
P&R	Preparedness and Resilience
PBX	Private Branch eXchange
PEMEA	Pan-European Mobile Emergency Application framework
PMN	Public Mobile Network
PMR	Private Mobile Radio
ProSe	Proximity-based Services
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider node
PSTN	Public Switch Telephone Network
PTP	Precision Time Protocol
PWS	Public Warning System
QoS	Quality of Service
RAIM	Receiver Autonomous Integrity Monitoring
RAN	Radio Access Network
RF	Radio Frequency
RRC	Radio Resource Control
RSSI	Received Signal Strength Indication
RTP	Real-Time Protocol
RTT	Real-Time Text
RTT	Round Trip Time
SBAS	Satellite-Based Augmentation Systems
SIP	Session Initiation Protocol
SMS	Short Message Service
SMSC	Short Message Service Controller
SSL/TPS	Secure Sockets Layer/Transactions Per Second
SV	Satellite Vehicle
SWE	Space Weather Europe
SWPC	Space Weather Prediction Center
TC	Technical Committee
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TETRA	Terrestrial Trunk Radio Access
TMO	Trunked Mode Operation
TPS	Transactions Per Second
TPS	Third Party Service
TLS	Transport Layer Security
TV	Television
UAS	Unmanned/Uncrewed Aerial System
UDM	Unified Database Management
UE	User Equipment
UI	User Interface
UMTS	Universal Mobile Telecommunication System
VLR	Visitor Location Register
VoIP	Voice over Internet Protocol
VoLTE	Voice over LTE
VoNR	Voice over New Radio
VMS	Variable Message Sign
VPN	Virtual Private Network
WCDMA	Wideband Code-Division Multiple Access
WebRTC	Web Real-Time Communications
WHO	World Health Organization
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network
xDSL	(all systems) Digital Subscriber Line

4 Network preparedness and resilience (P&R) concepts

4.1 Overview

Objectives: Being able to communicate in emergency situations (e.g. calling an emergency number and asking for help, disseminating information to affected individuals and general public) alleviates the consequences brought by adverse events to individuals, animals, environment, and possessions. The guidelines contained in the present document aim at enabling emergency services to increase the level of resilience and preparedness of their communication solutions in the case unexpected events affect their operation. The concepts and analysis in the present document are expected to be useful to emergency services authorities and decision-makers when setting-up or updating their communication networks and services, as well as to other stakeholders. Readers are recommended to start with clauses 4 and 7, as the majority of guidelines is provided in these two clauses. They may then select their topics of interest in clauses 8 to 12, as well as in annexes A and B, for a complete information.

NOTE 1: The present document analyses the different technologies involved in Emergency Communication Services with the objective to provide guidelines for their preparedness and resilience. These different technologies serve different purposes. The present document does not intend to compare these technologies. The risk evaluation provided in clauses 8 to 12 is done for the identification of these risks and is not an assessment of the technology itself.

The definitions of the terms "preparedness" and "resilience", as considered in the present document, are given in clause 3.1. In the present document, guidelines for emergency communications network preparedness are treated jointly with guidelines for emergency communications network resilience.

Resilience is a concept associated with contingencies and measures to alleviate and ensure a more effective response to the impact of hazards *after* a hazard happened. The objectives are both to minimize mean time to repair and time needed for returning to normal operation. Alleviating the direct consequences of outages - for which typically a contingency plan is needed - is another important aspect. Resilience applies to all levels in the system hierarchy: at component level and at system level, both within communication networks and end devices/applications.

There are a number of differing interpretations of the term "preparedness". Applying the term to emergency service communications, preparedness considers optimizing the availability and quality of service of communications systems and support resources *before* a hazard happens. The objective is to maximize mean time between failure. Requirements for emergency communications network preparedness thus means identifying and implementing specific activities and measures taken in advance to ensure robustness against the impact of hazards, i.e. hardening of emergency communications facilities that need to be prepared for use in the event of a major emergency/disaster.

Figures 1 and 2 aim to clarify the technical coverage of the present document.

The solutions used to enable emergency communications span a very broad range of systems, technologies and interfaces. For the purposes of the present document, the arrangements illustrated below and in annex A are considered.

Figure 1 introduces the four main Emergency Communication Services (ECS) areas:

- communications from individuals with public authorities/organizations [denoted as CALL*];
- communications between authorities/organizations (including mission critical communications) [denoted as MANAGE & REPORT];
- communications from authorities/organizations to the individuals (including public warning) [denoted as INFORM & ALERT];
- communications amongst individuals [denoted as ASSIST & INFORM].

NOTE 2: The (*) beside CALL means that this term should be understood as defined in clause 3.1.

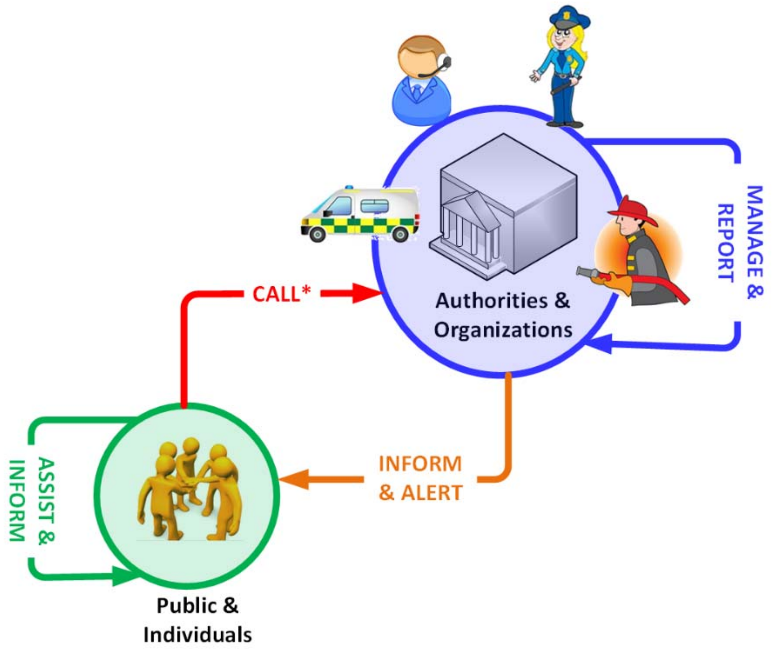

Figure 1: Emergency Communication Services

Figure 2 introduces the main components involved to support Emergency Communication Services:

- Functional components.
- Enablers and interface protocol components.
- Connectivity.

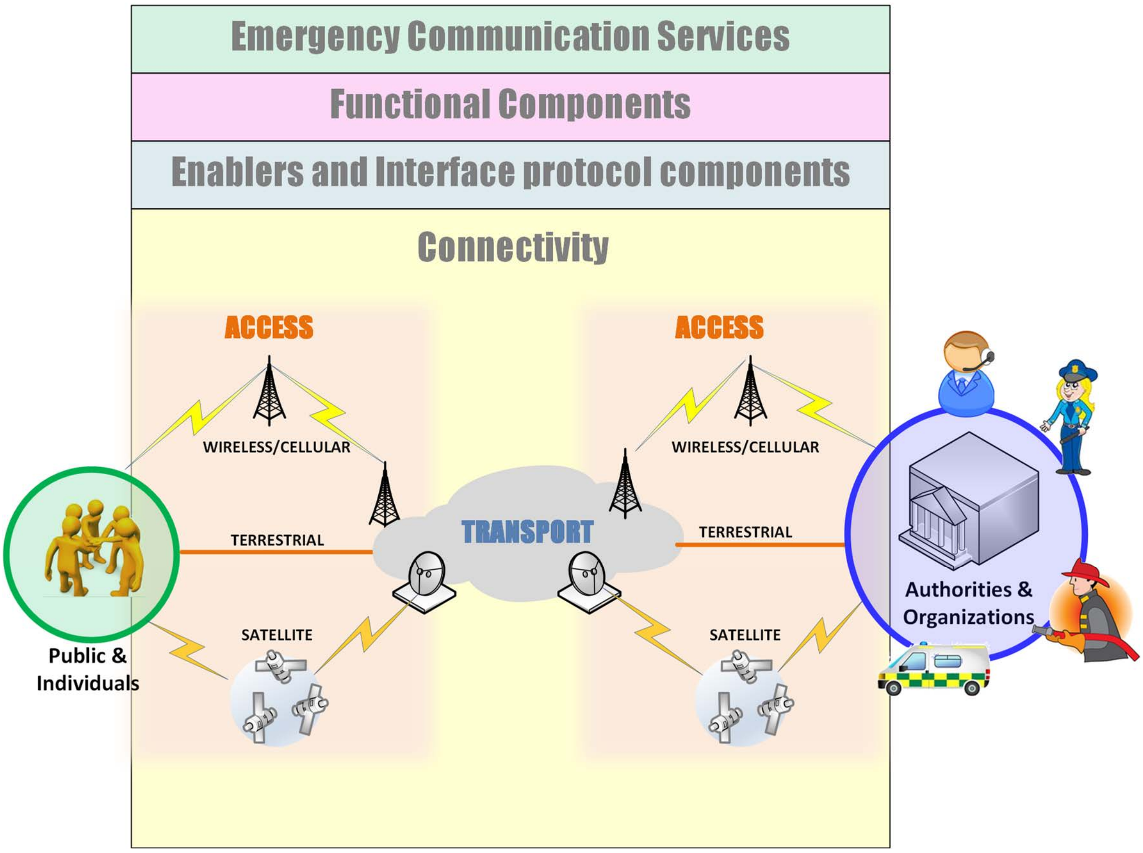

Figure 2: Emergency Communication Services main components

A short overview of key concepts relevant for preparedness and resilience is provided in the subsequent clauses.

4.2 Component level resilience concept

Component-level resilience is the concept of incorporating features into the design of an individual component of a solution 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.
- Local storage of information within the component to enable continued operation in the event of failure of higher-level information sources. This applies especially to client-server architectures.
- (Geographically) distributed storage of information and solutions to reduce the risk of data loss and enable continued operation in the event of network outages by providing a back-up solution.
- Employing persistent volume storage to maintain data and/or process state so processing can resume where it left off following a restart.

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 ranged from manual intervention to fully automatic. This is also referred to as an Active-Standby approach.
- Active Parallel Mode: In the event of failure, operation continues but with reduced capacity.
- Active Active Mode: In this mode, process state for a single operation is shared across at least two and sometimes more components. A single node failure is invisible to the overall processing of component and system as a whole.

The Active Active Mode is somewhat different to the Active Parallel Mode in two ways:

1) All process state is shared, so all nodes are doing exactly the same processing on the same operation.

2) A failure has no impact on the capacity of the system.

This approach is commonly deployed in cloud-based solutions. There is horizontal scaling, which is kind of like the Active Parallel Mode, where specific requests may be processed in a round-robin approach across the functions. There is also mirroring within and across clusters. This means that the state is common across two or more instances. The upshot is that a failure is generally invisible outside of the virtual environment in which the processes are running.

The different modes have differing advantages and disadvantages. In Redundant Mode solutions, 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. In Active Parallel Mode solutions, overall, 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. Active-Active Mode solutions provide the highest level of resilience without loss of performance and are increasingly popular in software-only solutions where applications and infrastructure are provided as code and the configuration patterns to support node state sharing are well defined.

4.4 Path/route diversity and separation concepts

Diversity is the concept of ensuring that specified communications are not routed over the same transmission paths. Route diversity is a method which allows to assure continuity of service by using multiple transmission routes to deliver a particular service between two points on a network. However, there may be some common physical network sites and/or equipment within the communications routings.

Diverse routing concepts relate to the ability to use, select or switch between different links to avoid congestion or network failure. A link is the direct connection between two processing nodes in a network. It may be physical, such as a wire, or it may be logical in packet switched networks.

Path separation is a more reliable means of ensuring that specified communications are not routed over the same media (cables, radio), equipment or transmission systems. It also ensures that there are no common physical sites within the communications paths. Normally, separated routes enter a building through separated ports using different service facilities (power, etc.). They only physically combine at the terminal equipment.

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

In theory a single incident affecting one particular route should not affect transmission capacity of the paths that are diverse or separate. However, the avoidance of a single point of failure can only be guaranteed in fully separated routes. This can lead to route/path congestion though without proper planning, because alternative path/route is unlikely to be used exclusively as a fall-back for the first link. This means that it is possible that bandwidth may become an issue if traffic that normally uses that link is particularly high. Proper network planning can usually take care of this issue.

The presence of a diverse set of operators is a necessity that should also be taken into consideration. In order for data and communications to be routed across all of the locations that are networked without having to share common cable lines, equipment, or entry points, the operator diversity should include a number of distinct service providers. Each of these providers utilize their own independent connections. The network of a specific provider should be completely separated end to end in a geographical area, including buildings and towers, in particular avoiding that one provider hosts the second provider in the same building/tower as its own devices.

Diverse routing capability is built upon the provision of transmission diversity and path separation. Routing and transmission devices are capable of detecting a reduction in performance on a particular link and reroute traffic based on specific recovery rules to balance the network load. Rules may apply to things like traffic type as well as identified final destinations. For example, real-time traffic such as RTP may be given access to a faster link than HTTP browser traffic. Signalling can follow a route different from the communication content.

The routing rules between the different parts of the network need to be carefully protected, especially regarding network maintenance and cyber security.

Load-balancing can also be performed using various techniques, such as:

- Volume partitioning where a higher percentage of traffic may take one route but a lower percentage of traffic is forced to take an alternative route.
- Round-robin where traffic is evenly distributed across each possible route.
- Data source routing where the address of the data source is used to determine the selected path.

4.5 Void

4.6 Fault-tolerant concepts

Fault tolerant systems are solutions 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 ICT systems designed to lose little or even no performance due to issues they may face, either in the hardware or associated software components.

4.7 Disaster Recovery (DR) concepts

Disaster Recovery (DR) is a coordinated activity to enable the recovery of ICT/business systems due to a disruption. DR can be achieved by restoring ICT/business operations at an alternative location, recovering telecom/IT/business operations using alternative 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 alternative communications service. Examples include:

- If a public TV service fails, public radio systems, cellular networks or other means described in clause B.2 could still broadcast emergency messages.
- If a Public Mobile Network (PMN) fails, satellite phone systems or over-the-top Internet-based applications could still be used for initiating emergency communications with the authorities. The communication may also be handled by an alternative PMN operator.
- If terrestrial systems fail, there is the ability to use targeted satellite systems.
- Apps can provide an alternative communication to operator core network solutions when contacting emergency services.

4.9 Network segmentation

Dividing a larger network into smaller subnetworks and controlling the traffic exchanged between them is called network segmentation. For private networks the main objective is to prevent cyber threats from causing widespread damage.

Applying network segmentation to public networks means being able to separate faulty or overloaded portions in case of incidents. This allows uninterrupted service provision in not affected network segments.

Prerequisites are a multiple component operation concept for network modules and defined network breaking points.

In PMR systems network segmentation is an implicit service attribute. There are typically several talk groups for voice group calls available which are used by different user groups in order to avoid congestion.

4.10 Isolated operation (network, grid, satellite)

In case of external risk on the network or communication system, it may sometimes be safer to isolate part of the network/ system from the external network and make it operate in isolated mode until the threat has disappeared or the isolated component has recovered from the damage and resumed its normal operational mode. Examples include:

- Cyber-attack on a web site (see clause 7.2.3.1) where the whole system is isolated from the Internet.
- Geomagnetic storm or electromagnetic pulse to protect electronic equipment (see clauses 7.2.1.5 and 7.2.3.3).

4.11 Planning/enhancing preparedness and resilience

Preparedness and resilience typically require additional expenditure. 100 % guaranteed P&R is not usually affordable. Emergency response organizations should balance the risks to their ECS from 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. See for example NIST Special Publication 800-39 [i.36] for managing information security risk.

A number of documents relevant to ICT systems resilience and preparedness are publicly available. They are listed in clause 2.2 (see also clause B.6):

- United Nations Sendai Framework [i.96];
- CPNI guide [i.4];
- ISO 22301:2019 [i.5];
- WHO guide [i.7]; and
- Government of Canada's guide [i.8].

Their main recommendation is to prepare and document a continuity management plan which identifies the critical internal and external dependencies of services and products involved in the ECS. This plan should include a risk assessment for each of these dependencies as well as the formulation of specific mitigation measures and procedures to prepare for the identified risks and minimize disruption (disaster recovery plan). It should help taking faster critical decisions and actions. It should be regularly reviewed and periodically practiced in real-life conditions to train the operational staff. The CNPI guide recommends that a recovery plan is established even before making the decision in a procurement process.

ISO 22301 [i.5] is complemented by a self-assessment questionnaire to help build such a continuity management plan.

5 Void

6 Void

7 Technologies analysis for Preparedness and Resilience (P&R)

7.1 Introduction

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 and mission critical communications).
- 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 communications facilities and systems that need to be prepared for use in the event of a major emergency/disaster are compiled and summarized 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. Once a communication is established, it needs to be maintained until it is no longer needed.

Clause 7.2 introduces the potential risks that may affect ECS in general and provides guidelines for preparedness and resilience relevant to each of these identified risks. In a second step, clause 7.3 evaluates which are the main physical dependencies common to a large number of the technologies involved in ECS and listed in annex B, and how they can be addressed for P&R.

Clauses 8 to 12 provide the detailed analysis of which risks may directly impact a specific listed ECS technologies. To simplify the analysis, a risk has been identified as such in these clauses only when it directly impacts the analysed technology. If a risk indirectly impacts a technology (for example a risk impacting the public cellular network also indirectly impacts IMS), it is identified only for the underlying technology that is directly impacted.

7.2 Potential risks and guidelines for preparedness and resilience against these risks

7.2.1 Natural events

7.2.1.1 Earthquake

Earthquakes may destroy part of the network, e.g. broken poles and lines:

- The damage caused by earthquakes is unpredictable. It may break physical cable plant, like poles and cables. Such plant destruction may result for both terrestrial lines, such as fibre, copper and coax, and mobile antennas and poles, in an almost total communications outage for the general public and emergency service teams. Handheld radio devices and satellite phones may continue to work.

- Earthquakes can also result in loss of power to buildings. Leading to exchanges and equipment buildings either being forced to rely on backup power such as batteries or generators until power can be restored.

- Earthquakes may also destroy building and equipment resulting in a total outage. If it is a cable plant termination building and transmission equipment is destroyed, then this may result in wide spread communications loss to the general public and emergency service teams.

- Meteorites may cause similar damages.

- Possible measures for preparedness and resilience of ECS:

  - Distribute cellular base station deployments across building and poles/towers where possible rather than opting for single deployment methods.

  - Implement secondary backhaul capabilities for cellular sites and key data hubs. This backhaul could be in the form or microwave or fixed wireless services.

  - Plan a backup solution to terrestrial communications using emergency satellite communications (see clause 7.3.3) through temporary base stations. In that case, the mobile network operator may need to set up a roaming agreement with the satellite operator.

  - Employ suitable earthquake resilient equipment and building practices as per building standards.

  - Use batteries, backup generators, thermocouples and/or solar panels to provide an alternative power source in the event that power is lost.

7.2.1.2 Volcanic eruptions

Volcanic eruptions can result in large amounts of airborne debris, such as dense charged dust clouds. These can impact terrestrial equipment coolers causing systems to overheat and shutdown or become damaged.

Airborne dust and debris also significantly impact wireless communications. This may result in loss of microwave transmission links, cellular services, and satellite communications. This is of particular concern for islands or mountainous regions where cable backhaul may be impractical.

Lava flows may result in loss of tower and pole infrastructure or make access to service pits unavailable resulting in service outages. Centralized exchanges and communications hubs are less likely to be impacted by volcanic eruptions as they tend to be placed well away from likely eruption areas.

- Possible measures for preparedness and resilience of ECS:
  - Distribute cellular base station deployments across building and poles/towers where possible rather than opting for single deployment methods.
  - Implement secondary backhaul capabilities for cellular sites and key data hubs. This backhaul could be in the form or microwave or fixed wireless services. Where possible point these away from the source of the volcanic activity to minimize interference.
  - Use batteries, backup generators, thermos-couples and/or solar to provide an alternative power source in the event that power is lost.

7.2.1.3 Wildfires

Wildfires generate many issues that may hamper, inhibit or interrupt communications:

- Wildfires are unpredictable and may be remote or relatively urban.
- Communication infrastructure in remote areas tends to be sparser and often does not have redundancy. In these cases, a loss of a cellular or other transmission tower could result in significant loss of communications capabilities in regional areas. This may result in a near total loss of public to authority communications. It will also make authority to public communications difficult owing to terrain, area access and loss of wireless communications.
- Wildfires can also produce significant amounts of smoke and fine dust particles attenuating or stopping some radio signals. Microwave links and satellite services can be significantly impacted by these types of obstructions.
- Equipment in the vicinity of wildfires may overheat and shutdown as a direct result of the fires, or systems may be impacted by the dust and fine smoke particles resulting in system failures.
- Firefighting methods for wildfires in remote areas include things such as water bombing, which deposit large amounts of water over large areas. Since it is hard to predict precisely where this water will fall, it may also have collateral impacts to transmission equipment.
- Wildfires in or close to urban areas pose very significant risks to larger populations of people and hence homes and property. However, more urban areas often have more communication options, meaning that a single failure is less likely to result in a complete communications failure. However, mass calling may place significant strain on backup communications channels resulting in further reduced service.
- Possible measures for preparedness and resilience of ECS:
  - Use underground power cables instead of overhead cables. The latter are less robust to wildfires and are known to increase the risk of wildfires.
  - Clear vegetation and debris to a reasonable distance around buildings and communications towers so as minimize the ability of the fire to reach them.
  - Place equipment in sealed cases, and where possible underground to protect it from exposure to fire.
  - Install a reliable fire suppression system that is non-toxic and does no damage to electronics and buildings.
  - Provide clear line of sight radio links for emergency redundant backhaul.

7.2.1.4 Severe weather conditions

Thunderstorms, hurricanes, cyclones, tornadoes, flooding, tsunamis, mudslides and avalanches, and heavy snow fall, all generate issues that may hamper, inhibit or interrupt communications:

- Despite of multi-level protection systems, lightning strikes can damage adjacent/nearby telecommunication infrastructure. Resulting service outages are mostly local.
- In some regions, operators share the same communications towers, so a loss of a tower may result in supposed alternative communications mechanisms becoming unavailable.
- Flooding can impact cable plant and terrestrial transmission and repeater equipment. In modern networks, this may result in domestic wired services becoming unavailable.
- Flooding can impact cellular power sources, as well as transmission equipment resulting in a loss of service.
- Heavy snowfall can damage telecommunication cables between poles and can impair wireless communications.
- The high-winds associated with storms, hurricanes, cyclones and tornadoes, can result in loss of above ground infrastructure such as towers and buildings. Loss of towers and antennas can cause mass outages for wireless services and make it difficult to return to service until after the storm has passed.
- Destruction of buildings that house transmission and cable-plant terminations can result in extended outages for both terrestrial and wireless services.
- Heavy rain can impact wireless communications.
- Possible measures for preparedness and resilience of ECS:
    - Installation of underground (subterranean) cable and packet switching plant can mitigate the impact of strong winds and other weather condition by limiting exposure to the elements.
    - Ensure strong grounding the installation of breakers, arrestors and lightning rods to mitigate impact of lightning strikes damaging equipment (electromagnetic compatibility).
    - Place equipment in upper floor of building or on poles to mitigate the risk of damage due to flood waters.
    - Distribute cellular base station deployments across building and poles/towers where possible rather than opting for single deployment methods. This provides redundancy in terms of localized damage or installation better able to withstand certain weather conditions.
    - Use of indoor as well as outdoor antenna systems for cellular sites so that service can continue to some degree even in heavy rain or snow falls.
    - Deployment of auxiliary power sources co-located with the equipment will allow continuation of operation for some time in the event of the loss the regular power source.

7.2.1.5 Geomagnetic storms

A geomagnetic storm is a major disturbance of Earth's magnetosphere that occurs when there is a very efficient exchange of energy from the solar wind into the space environment surrounding Earth. The solar wind produces major changes in the currents, plasmas, and fields in Earth's magnetosphere. The duration of a magnetic storm ranges from hours to several consecutive days:

- These storms can disrupt satellite communications and Global Navigation Satellite Systems (GNSS), damage satellite hardware, even dragging down the satellite, especially those in Low Earth orbit.
- They can also create harmful Geomagnetic Induced Currents (GICs) in the power electricity grid and pipelines, resulting in pipeline corrosion, massive scale electrical blackouts, causing large-area Internet connections outage, affecting long-haul telephone lines, including undersea cables unless they are fibre optic.

- Possible measures for preparedness and resilience of ECS:
    - Geomagnetic storms mainly affect underlying infrastructure. ECS operators need to ensure that the infrastructure they depend on has been prepared to overcome such storms. Examples of protections are given below.
    - The primary measure for preparedness is the monitoring of space weather. ESA is developing a common service to inform the operators of potentially impacted infrastructure about the upcoming arrival of a storm (SWE, see https://swe.ssa.esa.int/ssa-space-weather-activities). Sensors are placed in Lagrange points to send early warnings to the Earth. In USA, the NOAA has also setup such a monitoring web site: the Space Weather Prediction Center (SWPC, see https://www.swpc.noaa.gov/).
    - Satellites can be protected when they are designed by hardening the electronics on-board through metal shielding. Satellites may also potentially be secured by a shutdown of sensitive electronics or a temporary reorientation of the satellite both resulting in service interruption. In general, satellites in low Earth orbits are less sensitive to geomagnetic storms in terms of surface and internal charging than satellites in medium or geostationary Earth orbit. Nevertheless, satellites in extremely low Earth orbits may suffer from increased drag which can lead to an early demise. Thus, these storms should be considered especially during the launch and early orbit phase, when satellites may be temporarily in such extremely low orbits.
    - High voltage and power systems operators, on which all ECS rely, should harden their system and plan for alternate means to supply electrical power (e.g. generators or any other emergency power supply) until the storm calms down. For example, the interconnected system can be separated in smaller islands which are less sensitive to the storm, load can be re-routed, etc.
    - Houses terminating cable communications should be disconnected from the wires, except if they are made of fibre, as a major solar storm has the capability to set fire to the terminating points.

7.2.2 Technical triggered events (unintended)

7.2.2.1 Software related risks

Software/firmware updates, misconfigurations, certificate issues, data format changes, but also human errors may cause side-effects:

- Insufficiently tested software/firmware updates for user terminals and network elements can lead to unwanted side effects. This includes untrustworthy update procedures. Single to many user terminals might lose connectivity, or in case of affected network elements, complete network failures are possible too. Examples are operating system, network driver, router/switch firmware, or VPN endpoint firmware updates.
- Software components developed by different suppliers can lead to dependencies from different libraries or different versions of the same library. This bears the risk of unwanted behaviour.
- Insufficiently tested configurations have a similar potential. Examples are network settings in user terminals, filter rules, name resolution misconfigurations and routing tables.
- Digital certificates can be actively withdrawn (e.g. after an IT security incident) or can expire. This might lead to authentication errors in network elements and user terminals causing service interruption.
- Changes of digital data formats without backward compatibility, without sufficient notice, or based on ambiguous specifications leading to different implementations by different vendors can affect or interrupt information exchange.
- Terminals or other network equipment, which are overloaded with other high-priority concurrent intensive computing tasks (for example automatic translation) or with poor multitasking capabilities, might have insufficient remaining resources to process emergency communications (e.g. warning messages).
- Preparedness and resilience measures for software and configuration related risks are typically:
    - State-of-the-art software engineering according to adequate software quality standards (e.g. aerospace, automotive, military). This applies to all software suppliers contributing to a system.

    - Applying the key concepts of information security to all software and configuration items (see clause 7.2.3.1).
    - Thorough tests in small portions of live-systems before full deployment.
    - On-site and off-site mechanisms based on independent or redundant communication means for quick and uncomplicated software or configuration reversing, so that in case of problems returning to the previously used version is possible.
    - Independent watchdog systems monitoring critical software for abnormal behaviour.
    - Fail-safe modes with limited but highly stable functionality.
    - Adequate multi-tasking operating systems prioritizing ECS together with ECS-related applications allowing fall-back modes to reduce processing load.

7.2.2.2 Technical Network failure or damage

Technical network failures affect the transmission and /or routing of the communication:

- Technical network failures are caused by software issues (see clause 7.2.2.1), the failure of a piece of equipment, for example if it is outdated or suffers from overheating, or the break of a physical link between two peripherals in the network, for example if a cable is severed during road works by an excavator or by rodents entering networking trenches. Network failure may also happen in case of severe load congestion.
- Work-related emergencies such as explosions, machinery malfunction, chemical spills, or dangerous gas releases are work accidents which have the potential to erode network cables and create downtime or even loss of connectivity. Explosions can lead to breakage of the equipment such that it cannot generate signal and therefore is not useful in the emergency.
- Accidents (aircraft, ground-based or maritime vehicles): these unintended accidents may result in the physical collision to telecom equipment, thereby damaging the hardware equipment such that it can no longer connect. An example is if a submarine accidentally cuts through an underwater communication cable, then all the telecom network connected to this cable including emergency communications, are affected by the loss of connectivity. Another example is if an aircraft accidentally crashes in a field which is hosting telecom systems, then this may damage the equipment such that it can no longer transmit.
- Preparedness and resilience measures include:
    - Planning of redundancy in the network and critical network elements, off-site when relevant, to prevent loss of operational capabilities.
    - Planning of network evolution and scalability.
    - The adoption of physical security related standards for the infrastructure and the premises in case of accidents.
    - Place equipment in sealed cases, and where possible underground to protect it from exposure to chemical spills or any other type of damaging event.
    - Installation of subterranean cable and packet switching plant can mitigate the impact of physical accidents on the network.
    - Ensure strong grounding the installation of breakers, arrestors and lightning rods to mitigate impact of damaging equipment.
    - Deployment of auxiliary power sources co-located with the equipment will allow continuation of operation for some time in the event or the loss of the regular power source (see clause 7.3.4).
    - Planning of regular maintenance to assess the status of the network.
    - Installation of monitoring systems to raise alerts to technical personnel sufficiently early.

  - Careful planning and procedures for all network updates (devices, peripherals, servers, software, cable plant, etc.) and coordination between the different technical staff teams who are performing internal actions and interventions and those who manage the network, whether they belong to the same company or to different companies. Ideally, network updates should be tested on pre-production elements on the entire environment before being approved for full deployment.
  - Solutions may be deployed in virtualized environments with clusters spread across multiple data centres. This approach minimizes the impact of network and infrastructure failures as traffic is moved from failed nodes to active nodes operating normally. Multiple communications paths between environments ensure that network infrastructure have minimal impacts.

7.2.2.3 Outage of underlying or related infrastructure

Practically all network elements require infrastructure:

- Electrical power for network electronics, but also for active cooling.
- Time references especially for cellular system base stations, which are very often based on Global Navigation Satellite Systems (GNSS).
- Command and control systems for remote monitoring and maintenance.
- Secondary (remote) infrastructure for required services like name resolution, reference time provision, or authentication might be subject to connectivity interruptions or service outages.
- Additionally, underlying infrastructure can be the network transporting the messages to fulfil a specific function, for example public mobile network is an underlying infrastructure for eCall, wireless access network is an underlying infrastructure for the ESInet, etc.
- Possible measures for preparedness and resilience of ECS:
  - Electrical power see clause 7.3.4.
  - Time references see clause 7.3.3.
  - Other infrastructure: see P&R concepts described in clause 4 and enabling technologies in clause 8.

Network incompatibilities in roaming:

- Core infrastructure:
  - While all core networks enable voice communications, most still do not enable video and Real-Time Text (RTT) services. This means that a person that called in their home area where certain services were enabled may have call failure in time of need when roaming to another region.
  - Since the service is enabled in the core, when a person is on a call and roams to a different region, even though the advanced communications are established, they may drop if the new operator network does not support the services.
- Over-The-Top (OTT) services:
  - OTT services will have issues establishing communications if the area in which the caller is does not support the App capabilities. Discovery mechanisms can allow users to establish ahead of time which capabilities will be available in time of need, so alternative means for contacting help can be established ahead of making the call.
  - OTT solutions, for example PEMEA or NG112, may use web technologies and peer-to-peer rather than core network communications. Web technologies can mitigate issues with inter-jurisdictional incompatibility through the use of browsers and the like.
- Possible measures for preparedness and resilience of ECS:
  - Core network service availability and access method can be mitigated through education and advertising to the general public to avoid issues at call time.

- Using newer technologies that employ service indicators rather than numbers can avoid the issue of numbers being different from region to region but will not aid in determining service availability ahead of time.
- OTT services, for example PEMEA or NG112, can provide a fallback to the home region PSAP in the event that no suitable service is available in the roamed to region.
- Critical components should be accessed through multiple operators, ensuring that a single operator is not responsible to all network access and control in a certain area. See also clause 4.4.

7.2.3 Human triggered events (intended)

7.2.3.1 Cyber-security attack on critical infrastructure

Society-critical infrastructure, such as emergency management, is becoming increasingly complex and dependent on networks of interconnected devices. Only a few decades ago, emergency networks and other vital infrastructure were independently managed. Both geographically and in terms of the industries they work in, they are now significantly more interconnected. Critical infrastructure systems, such as those responsible for emergency communication, public warning, power generation, water treatment, and electricity production, are interconnected to form these networks. Even if it serves the public interest, these networks are also vulnerable to attacks.

A cyber security attack on critical infrastructures may render the infrastructure inoperable by targeting the operation lifecycle. Denial-of-service attacks and malicious reconfiguration/destruction of software-based systems are examples. Another significant threat is software vulnerabilities that are continuously discovered not only on the emergency system, but also third-party tools, libraries, and components. The risk and applicability of these detected vulnerabilities can then be assessed, allowing decisions to be made regarding actions such as patching and upgrading. Consequently, systems with Internet access are inherently susceptible to cyberattacks. The PSAP and other critical communication infrastructure should be considered as critical infrastructure, and emergency services should adhere to cybersecurity best practises.

There are several aspects of information security which have to be considered in preparedness and resilience concepts. These are:

- Confidentiality: communications between individuals and authorities, but also among authorities are normally confidential.

EXAMPLE 1: Health data.

- Integrity: information and software to be exchanged/installed need to be correct and all changes have to be traceable. Software and required libraries for network elements have to be digitally signed or at least distributed together with checksums (hashes) which have to be checked before installation.

EXAMPLE 2: A PSAP hands over emergency call data to an ECC. A workstation in a PSAP gets a software update.

- Authenticity/non repudiation/accountability: a receiver has to be able to check the trustworthiness of the received information or software.

EXAMPLE 3: Does a warning message really come from an authority? Or from someone else pretending to be the authority?

- Configuration management: maintain consistency among involved hardware and documentation and software versions including all libraries.
- Access control: only authorized personnel should have access to infrastructure, end devices and be able to participate in the ECS.
- Technical risk assessment: the implementation of technology that has been validated according to predetermined criteria.
- Human risk assessment: an examination of the human weaknesses that exist throughout the workforce.

The implementation of security-related standards for the physical space and the underlying infrastructure are thus important measures to be taken.

Modern Continuous Integration and Continuous Deployment (CI/CD) build environments can support automated vulnerability scans across the code, libraries and execution environment. CI/CD pipelines also improve the quality of the software, as they apply large numbers of automated tests that are executed during the build phase and after the deployment phase is complete. Employing a CI/CD pipeline approach further mitigates the risks associated with software faults and security vulnerabilities:

- Perform dynamic code analysis and component penetration testing.
- Use E-vulnerability databases to scan for the existence of such in the software.
- Use firewalls and apply best practice filtering.
- Install components for Intrusion Detection and Intrusion Prevention (ID/IP).
- Perform antivirus scans on any uploaded or downloaded files.

A detailed description of all possible P&R activities in this domain would go beyond the scope of the present document. Depending on the sensitivity of the envisaged infrastructure, a dedicated IT-security certification is recommended.

7.2.3.2 Radio jamming

Wireless devices and infrastructure used in communication services, and also GNSS receivers that are essential for network synchronization and services like navigation and safety of live (e.g. locating a 112 caller), are subject to radio jamming, whether intentional or unintentional. While these systems operate under local and international regulations and laws, it is possible for bad actors to introduce RF interference by transmitting unlawfully in the frequencies used by the targeted terminals or network equipment. Most products used in these services are designed to recognize, reject, and recover from such attacks, but the source of the unlawful transmissions will need to be identified and authorities or service providers will need to take correction action in terminating the unlawful transmissions in non-transient offenses.

- Preparedness and resilience measures include:
  - Beamforming antennas allowing to mask the direction of the jamming signal source, dynamically if possible.
  - Signal processing with band-stop filtering.
  - Frequency hopping and band-spreading technologies.
  - Jamming source localization equipment allowing to determine the jammer's position.

7.2.3.3 Electromagnetic pulse

An ElectroMagnetic Pulse (EMP) is an electromagnetic wave similar to radio waves that occurs from secondary reactions (e.g. nuclear reactions) that happen when radioactive gamma radiation is absorbed by the air or ground. It varies from standard radio waves. Initially, it generates significantly stronger electric field forces. The EMP pulse creates a single pulse of energy that totally dissipates in a fraction of a second. In this regard, it resembles the electrical signal produced by lightning, although the increase in voltage is often one hundred times quicker. This implies that the majority of lightning protection technology is ineffective against EMP:

- Preparedness and resilience measures include:
  - The Emergency services needs to consider the possibility of using equipment that will be able to handle EMP strikes.
  - The use of military EMP standards like ML-STD-188-125-1 [i.94].
  - The use of EMP shielding in rooms and racks.
  - The EMP protect guidelines needs to be considered (see NCC guidelines [i.93]).

7.2.3.4 Intentional destruction of terrestrial infrastructure

In case of sabotage, conflicts, wars, terrorist attacks, mass protests or similar situations, the telecom infrastructure may be physically damaged such that any form of communication becomes impossible:

- If this was intentional damage, mitigation for preparedness and resilience of ECS may include possible suggestions as below:
    - Backup system, that can use alternative channel of communication e.g. if it was terrestrial damage then satellite system can be set up in an emergency.
    - Implement secondary backhaul capabilities for cellular sites and key data hubs. This backhaul could be in the form or microwave or fixed wireless services.
    - Use batteries, backup generators, thermocouples and/or solar panels to provide an alternative power source in the event that power is lost.

7.3 Preparedness and resilience guidelines for physical dependencies

7.3.1 Wired Networks

Generic P&R guidelines for wired networks are provided in clause 4. The assumption in the present document is that wired networks cover any medium of communications that uses cables (copper or fibre).

Resilience in the transmission network:

- The transmission network is usually composed of a number of technologies including:
    - Copper based landlines, including coaxial cables.
    - Optical fibre networks.
    - Radio links.

At the link level, redundancy may be implemented by duplication of the equipment that supports a single link, such as multiple Ethernet switches or modular fibre distribution systems, as well as through duplication of the links themselves. When connections are duplicated, it is best practise to physically separate the pathways geographically in order to guard against the possibility of a single physical incident disrupting both the primary and backup links (e.g. severing of cables by digging machinery).

At the network level, redundancy may be provided by designing the network with several connections from node to node, connections in a mesh arrangement and designing pathways between pairs of nodes that can transmit communication between other, more distant nodes. When a connection or node on a network is lost, the network will automatically redirect traffic through the remaining nodes and links in a new order (diverse routing). This approach is used more often by systems that employ packet switching methods, such as Internet Protocol (IP).

Resilience in the packet switching network:

- Packet switching networks are typically constructed using redundant or highly resilient components. The following techniques can be used within a packet switching network:
    - Duplication and backup of system databases, both within a single site and between sites, to ensure resilience of user and system configuration.
    - Duplication and backup of packet switching intelligence to ensure mobility and communication control functions are maintained in event of failures.
    - Duplication of packet switching components, or adoption of more resilient distributed approaches, typically based on IP, with redundant routing components.
    - Redundant Local Area Networks connecting packet switching components.

- Redundant network interfaces connecting each packet switching site with other packet switching sites and with cellular networks.

In addition, duplicate packet switching sites can be used, such that a single packet switching site may be configured and switched into place of any failed packet switching site (see clause 7.3.5), or multiple packet switching sites employed up to the case that each primary packet switching site is duplicated. Duplication of packet switching sites should take place across multiple geographic locations to increase resilience in event of loss through disaster.

7.3.2 Wireless Networks

The assumption in the present document is that wireless networks cover any medium of communications that uses radio (excluding satellite communications).

Mobile radio systems are usually dedicated or prioritized for usage by one or more emergency response organizations. They typically include 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 packet switching systems.
- Packet switching network - for communication control and routing.
- ECC transmission - transmission systems from the packet switching systems to ECCs.
- Network management - support systems to configure and operate the network.

P&R 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 wireless networks and to avoid single points of failure, including at the inter-connection between the above components, when feasible.

P&R measures for Radio Access Networks (RAN) include:

- Service provider diversity: often there are multiple cellular network providers operating in the same region. Alternatives therefore exist in terms of the selected network operator.
- Technology diversity: different generations of cellular technology may cover the same areas, for example 3G, 4G and 5G and these may provide fallback access in times of need. Also, almost all cellular wireless devices will have access to WLAN, which can provide Internet access and act as a radio access network to the cellular providers' IMS emergency services, or to OTT service offerings.
- Satellite services may be utilized for backup connections (for example the backhaul of cellular networks).
- Overlapping base station coverage: cellular networks are normally subject to sophisticated frequency and coverage planning so that there are practically no coverage areas overlaps. With dynamically adjustable transmit power and antenna beamforming at neighbouring base stations, it is possible to partly mitigate outages of transceiver sites.
- Overlapping coverage from multiple cell sites in the same area.
- Configuration of network such that adjacent base station sites are connected to different packet 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.
- Redundancy of components on base station sites (e.g. transceivers, site controllers, antennas, etc.).
- Use of multiple core network and transmission links to sites using various topologies including redundant stars and rings. 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 components.
- Use of redundant home/visitor location registers (HLR/VLR for 2G-3G, HSS for LTE, UDM for 5G).
- Redundancy of power supply capability, including battery and generator powered supplies.

- Fall-back strategies to allow standalone operation of sites disconnected from packet switching sites. In this case communications are possible between terminals connected to the same site ("island mode").

With the evolution to digital communications, 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.

In addition to the mechanisms employed to provide protection against failures in the RAN, mechanisms are also employed to provide resilience against interference, both deliberate and accidental (see also clause 7.2.3.2). The strongest protection against deliberate interference to transmissions 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 standalone operation of a cell site.

7.3.3 Satellite Services

The assumption in the present document is that satellite services include satellites as means for communications and GNSS. GNSS is used by a large number of technologies for localization, but also for timing and synchronization.

Satellite Communication Systems:

Alternatives to satellite communication systems can be other satellite communication systems (i.e. different provider) or terrestrial wireless networks. In both cases additional dedicated hardware is required, which may be available in cold standby or actively (hot standby). The latter includes failover and traffic load balancing scenarios.

Depending on the actual use case, it might be advantageous to consider backup satellite communication systems with different orbit altitudes. Geostationary Earth orbit satellites require directive antennas on the ground and are more sensitive to geomagnetic storms (in terms of charging) and jamming, but require only an unobstructed line of sight between ground terminal and one satellite. Low Earth orbit satellite communication systems typically require open sky conditions, i.e. ideally a completely unobstructed hemisphere.

Global Navigation Satellite Systems (GNSS):

GNSS resilience is the capability to quickly recover from space-based positioning, navigation or timing service outages. Threats are interference by other signal sources, jamming, and spoofing. Live re-broadcast of GNSS signals is sometimes called meaconing ("masking beacon") and is e.g. required for indoor tests of aircraft GNSS receivers. In case of insufficiently electromagnetically confined buildings, these signals can disturb other receivers outside.

In GNSS context, integrity is defined as both the measure of the trust that can be placed in the correctness of the information supplied by a GNSS and the ability of the system to provide timely warnings to users when the system should not be used for navigation. There are different integrity architectures possible, which augment GNSS and are mainly designed for aviation:

- Satellite-Based Augmentation System (SBAS):
  - Task: Broadcast augmentation information (corrections & integrity) and ranging capabilities.
  - Area: Limited to a regional level (broadcast via geostationary satellite).
- Ground-Based Augmentation Systems (GBAS):
  - Task: Broadcast augmentation information (corrections & integrity) and ranging capabilities.
  - Area: Limited to a local level (broadcast via ground station).
- Aircraft-Based Augmentation System (ABAS):
  - Task: Focus is on integrity only, i.e. without improved solution accuracy.
  - Area: Single user (e.g. single aircraft).

  - ABAS Types:
    - Receiver Autonomous Integrity Monitoring (RAIM):
      - Algorithm that determines the integrity of the GNSS solution.
      - Compares the smoothed pseudo-range measurements.
    - Airborne Autonomous Integrity Monitoring (AAIM):
      - GNSS information only completed by on-board sensor data.
- Advanced Receiver Autonomous Integrity Monitoring (RAIM):
  - Frequency diversity (e.g. dual frequency measurements).
  - Geometry diversity (e.g. use data from as many GNSS constellations as possible).
  - Using Integrity Support Messages (ISM) for specific airspaces.

Enhanced Long Range Navigation (Enhanced LORAN), also known as eLoran or E-LORAN, has been designed specifically as a terrestrial fall-back solution for GNSSs. eLoran is capable of providing wireless time accuracy similar to GNSS-time, but is typically available in some coastal regions of the Northern hemisphere only.

In case of jamming scenarios there are different mitigation approaches. Horizontally blocking antennas or antennas with active beamforming are able to suppress jamming signals. Low-power and narrow-band jammers can be suppressed with different RF techniques, including blanking, targeted filtering, or high linearity, too.

Spoofing or meaconing attacks require more elaborate countermeasures. With controlled beamforming antennas it is possible to track GNSS satellites as signal sources only. In the signal processing domain, there are methods to detect and overcome these attacks, too (e.g. check for Doppler plausibility, range plausibility checks, signal strength behaviour over time, etc.). Last but not least cryptographic techniques applied to the spreading codes (e.g. Galileo^{TM} public regulated service, GPS military code) can help to overcome these threats.

In general, most GNSS receivers increase the trust in GNSS data (both on measurement level and data level) by receiving GNSS signals from different independent satellite constellations (e.g. GPS, Galileo^{TM}, Beidou, Glonass, etc.) on different (protected) frequency bands. Additionally, GNSS receivers can use multiple sources of data (e.g. secure servers for product-specific GNSS receivers providing orbit/clock information and cross-checked demodulated data) in order to assess the health, integrity, and trustworthiness of individual satellites up to an entire constellation through Satellite Vehicle (SV) probation and constellation disablement. Furthermore, GNSS receivers can include measurement and positioning/timing data provided by other sensors (e.g. inertial/attitude) in order to evaluate the trustworthiness of the GNSS signals.

Alternative/complementary position determination approaches include celestial/inertial navigation supported by radar system and/or hydrographic charts and sonar correlation in maritime environments. Coarse user terminal localization is possible in cellular networks (WWAN) or when connected to WLAN access points with known position:

- WLAN standard-based positioning using RSSI and/or Round-Trip Time (RTT) determination.
- Proprietary signal-strength-based approaches providing high accuracy especially in areas densely populated with WLAN access points.
- Cellular networks/WWAN standard-based positioning using:
  - 3G/4G: Cell ID (CID), Enhanced CID (ECID), Observed Time Difference of Arrival (OTDOA).
  - 5G New Radio (NR): CID, RTT, Angle of Arrival (AoA)/Angle of Departure (AoD), OTDOA.

Other technologies are e.g. Bluetooth® beacons or similar.

If GNSS receivers are used as source for precise time only, then protocol-based mitigation strategies are possible, Precision Time Protocol (PTP) is more accurate than the Network Time Protocol (NTP) and is capable of distributing reference time to e.g. network/power grid nodes or base stations of cellular networks. Prerequisite is the availability of at least one sufficiently stable reference clock and a wired computer/data network interconnecting all nodes.

For relaxed time accuracy requirements, time signal radio stations (e.g. DCF77 in Germany or WWVB in the U.S.A.) may be an alternative to GNSS-time, too.

7.3.4 Electrical Power

Electrical power is the most critical underlying infrastructure to all, as it holds alive all the necessary equipment. In general, underground power cables are less sensitive to natural hazards (fire, dust, storms, icing, etc.) in comparison to overhead cables.

Outages of electrical power can be mitigated by continual power systems (uninterruptible power supplies, emergency power systems) or standby generators. Gridding the electrical power distribution allows to implement alternative paths and resilience in case a power distribution path has been destroyed by a storm or another natural hazard. However, the grid should be broken into pieces to cope with a strong geomagnetic storm.

Generators driven by combustion engines require constant fuel supply which might be problematic in scenarios with widely destroyed infrastructure. Photovoltaic systems with batteries do not depend on external supplies, but can have limited or stopped power output in bad weather conditions or at night. The same type of restrictions applies to windmills.

Operational staff should be equipped with batteries and chargers to be able to communicate even in the case of a power outage.

Energy distribution is entering the digital age. This means that the infrastructure is monitored and controlled by sensors and other command systems. The distribution thus becomes sensitive, through its control centres, to cyber-security risks, technical failures, software related risks such as software updates, technical network failure as well as to destruction of the control centres themselves. Furthermore, there is a reciprocal dependency between the electrical power supply and the telecom network used by technical staff when restoring the power supply during an event. All measures explained in clause 7.2, as well as redundancy measures, can support preparedness and resilience. The utilities communication network should be isolated from the public telecom network as well as from jamming, as the latter may compromise the AC frequency and break the devices of the communication network.

The Storm Reconstruction Guidebook from NEMA [i.79] provides exhaustive guidelines in this field.

7.3.5 Buildings

Buildings are mainly subject to physical risks, such as earthquakes, storms or intentional destruction. Accordingly, buildings hosting sensitive equipment should be hardened to reduce the impact of these risks, e.g. by applying anti-seismic standards, burying the floors hosting the equipment or securing the access. Hardening practices also include upgrading the material used to build them and secure poles and towers with guy wires and similar structural supports.

Alternative sites may be set up to be activated in case the main site is lost. Their level of furnishing, equipment, depends on the resources available. The guide in [i.8] introduces the notions of cold, warm and hot sites. Their activation time depends on this level. Some alternative sites may also be hardened with alternate power supplies or increased protection from intrusion.

7.3.6 Equipment

The assumption in the present document is that equipment supports functionalities and includes at least one piece of hardware (e.g. user terminal, network peripherals, etc.).

Equipment hosting ECS functionalities is subject to physical risks similar to the buildings hosting them, as described in clause 7.3.5. As they contain hardware parts, equipment strongly depends on the availability of electrical power. Measures as described in clause 7.3.4 should apply.

Moreover, the first measure for the security of sensitive equipment, such as servers or network peripherals, is to install them in separate locked rooms with access restricted to authorized persons only. Sufficient information such as technical documentation, system diagram, licenses, should be maintained in a safe location to be able to reproduce the destroyed equipment in the event of a disaster.

Terrestrial electronic equipment may burn when submitted to EMP (see clause 7.2.3) or as a result of a geomagnetic storm (see clause 7.2.1.5) and should be protected against them.

In a specific system deployment, the devices and peripherals that compose the system should demonstrate cross-equipment interoperability, including regarding the tools and software they contain.

Scalability is also an important factor. The system may show degraded performances or even stop working when new equipment is added because the initial solution design had not been prepared properly. This should be considered as early as feasible in the design and deployment of ECS and select performance-capable equipment that will enable the expansion of services when it becomes necessary to do so.

8 Preparedness and resilience for Enabling Technologies

8.1 Overview

The objective of this clause is to provide a detailed analysis of the enabling technologies that support the different components involved in ECS listed in clause B.5. As relevant, this detailed analysis includes for each enabling technology: the list of risks that may directly affect that technology, specific measures that may be taken for that technology, in addition to those referenced in the present clause, and the list of underlying infrastructures that may have an impact on that technology. This analysis is completed by the identification of the main physical dependencies that may directly affect each technology. For clarity reasons only risks with the potential to directly affect technologies are considered; indirect threats can be traced via the physical dependencies and underlying infrastructure chains.

NOTE: The present document analyses the different technologies involved in Emergency Communication Services with the objective to provide guidelines for their preparedness and resilience. These different technologies serve different purposes. The present document does not intend to compare these technologies. The risk evaluation provided in clauses 8 to 12 is done for the identification of these risks and is not an assessment of the technology itself.

The main guidelines for ECS preparedness and resilience relevant for each of the technologies analysed in this clause are given in clause 4, clause 7.2 and clause 7.3.

In each of the clauses below, physical dependencies are mentioned only when they directly affect the respective technology. To avoid repetitions, when a technology is indirectly affected through an underlying infrastructure, this is not indicated in this clause, but rather through the analysis of the underlying infrastructure. The list of underlying infrastructures is given for each technology in this clause.

8.2 Cellular access/WWAN (2G to future 6G), WLAN

This clause excludes satellite communications, which are addressed in clause 8.5. The type of risks that will affect these networks are listed here:

- Natural Hazards.
- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Radio jamming.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

Cellular networks, especially in 4G and 5G have very robust security frameworks (see ETSI TS 133 401 [i.80] and ETSI TS 133 501 [i.81] respectively). Prior to accessing the IMS core, the following layers of security are provided:

- Non-Access Stratum (NAS) signalling confidentiality.
- NAS signalling integrity.
- User plane confidentiality.
- User plane integrity.
- Radio Resource Control (RRC) signalling confidentiality.
- RRC signalling integrity.
- Authentication.

Further P&R guidelines for wireless networks are given in clause 7.3.2.

Identification of underlying infrastructure: Cellular access cannot work without the underlying cellular infrastructure and the connectivity to the core infrastructure. They are thus vulnerable to all of the risks that have been highlighted in this clause, in addition to those posed by virtualization and cloud computing (clause 8.9).

Identification of direct physical dependencies:

- Wired Networks: Cellular access/WWAN/WLAN interconnections necessitate a wired network for user traffic and terrestrial broadcast.
- Wireless Networks: Backhaul links connect to the core through microwave, fibre, or laser links.
- Satellite Services: Satellite services are utilized for synchronization service.
- Electrical Power: Stations require electrical power.
- Buildings: Equipment is installed in top buildings, poles/towers.
- Equipment: Cellular access/WWAN/WLAN devices are by definition hardware used to transmit.

8.3 Wired connectivity for IMS

IMS provides core IP switching services for public telephony networks and may be accessed either through cellular wireless or fixed cable, wired, access. When accessed through wired services, IMS is sensitive to the following risks:

- Natural Hazards.
- Software related risks.
- Technical Network failure or damage.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

Specific guidelines for preparedness and resilience have already been provided for wired connectivity in clause 7.3.1.

Wired connectivity is an underlying infrastructure for IMS. Clause 4.4 provides guidelines for operator diversity.

8.4 Internet of Things (IoT) devices and platforms

IoT devices include advanced sensors that allow devices, buildings, and even clothing to become smart and connected. This has important benefits for emergency responders - the more information they have, the easier and safer their jobs become. The type of risks that will affect these devices and connected platforms are as follows:

- Natural Hazards.
- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Radio jamming.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

Clause 7 of ETSI TR 103 582 [i.70] contains a series of recommendations, some of which could be relevant to preparedness and resilience.

Identification of underlying infrastructure: In some cases, IoT devices and platforms rely on cellular infrastructure for their operation. They are thus subject to all risks affecting this network (see clause 8.2). Most of the time, they use other means of communications such as proprietary RF, WLAN, Bluetooth®, LPWAN, wired connectivity, etc., with dedicated communications networks.

Identification of direct physical dependencies:

- Wired Network: sensors and actuators maybe connected through a wired network.
- Wireless Networks: sensors and actuators maybe connected through a wireless network.
- Satellite Services: location services are often derived from GNSS.
- Electrical Power: electricity is needed to power most of the IoT devices and platforms in order to operate. Other devices are usually powered by batteries.
- Buildings: IoT devices and platforms are housed in buildings.
- Equipment: IoT devices and platforms are by nature made of physical sensors and actuators.

8.5 Satellite Communication and Navigation Services

This clause excludes terrestrial assets apart from user terminals.

Satellite communication and navigation systems provide ubiquitous connectivity/positioning and require very limited user equipment only, but national legislation has to be considered in terms of frequency regulation. A suitable antenna location is needed (line-of-sight to geostationary satellites, clear sky for constellations). There are several risks to be considered:

- Geomagnetic storm that may affect or permanently damage satellites and their payloads.
- Software related risks that may cause malfunctions of uplink stations, user/network equipment, payload operation, or satellite command & control.
- Technical network failure or damage may cause user or command & control link interruption.
- Cyber-security attack on critical infrastructure.

- Radio jamming affecting user links.

Generic guidelines for preparedness and resilience are indicated in clause 8.1. Specific P&R measures related to satellite services are covered in detail in clause 7.3.3.

Identification of direct physical dependencies:

- Wired Network: ground stations for satellite operations require wired networks for user traffic and for terrestrial transmission of tele-commands and telemetry.
- Satellite Services: satellite communication and navigation are by nature satellite services.
- Electrical Power: both satellite user terminals and ground stations require electrical power. The former may operate on battery power, too.
- Equipment: satellite communication and navigation require user terminals with suitable antennas/modems and ground stations.

8.6 Wireless mesh networks

Wireless mesh networks (or ad hoc networks) do not rely on pre-existing infrastructure. They are self-organizing and fully scalable which makes them very robust against loss of network nodes.

Risks associated with this network technology include:

- Software related risks causing e.g. incompatibilities between network nodes so that traffic routing/forwarding may be affected.
- Cyber-security attack on critical infrastructure which may include download sources for mesh network software or firmware.
- Electromagnetic pulse which may cause temporary or permanent outages/damages.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

Identification of underlying infrastructure: electrical power is needed especially for long-time operation and suitable antenna locations are required.

Identification of direct physical dependencies:

- Wireless Networks: wireless mesh networks are dependent on radio and potentially can use other wireless networks.
- Equipment: Wireless mesh networks are made up of devices that establish radio links amongst themselves.

8.7 Drones/UAS to support Emergency Communications

Natural disasters, like wildfires and hurricanes, can lead to many lives lost and billions of dollars in costs according to NASA. To help reduce that impact, drones have great potential to assist emergency responders by making their interventions faster, more targeted and better able to adapt to changing circumstances (see Recommendation ITU-T Q.3060 [i.77]). Also known as unmanned aircraft systems, or UAS, these vehicles and the systems that support them could multitask in unique ways, for instance by using software to track firefighters on the ground before dropping forest fire retardant a safe distance away (see for example NASA STEReO project at https://www.nasa.gov/feature/ames/drones-for-disaster-response-nasa-stereo-project-kicks-off).

The type of risks that drones are subject to are as follows:

- Natural Hazards that may cause failure to operation of the drones.
- Software related risks that may cause failure to operation of the drones.
- Technical Network failure or damage may cause the drones to not operate as intended.

- Outage of underlying infrastructure may cause break with controller.
- Cyber-security attack on critical infrastructure: similar to radio jamming, this may cause the drone to become counter effective or to send wrong data.
- Radio jamming may cause drones to react in a way that will affect their operation e.g. fly to wrong location.
- Intentional destruction of terrestrial infrastructure could break signal with controller.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

Clause 7.2 covers the P&R recommendations identified as responses to the risks listed above and this can be applied here.

Identification of direct physical dependencies:

- Wireless Networks: services are initiated through the public mobile network. Drones use wireless communications.
- Satellite Services: drones provide and receive location data obtained from GNSS or alternative means.
- Equipment: drones are unmanned aircraft systems.

8.8 Security

Cyber-security is sensitive to the following risks:

- Software related risks.
- Cyber-security attack on critical infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

More specifically, the type of security risks that services are subject to are as follows:

- Development not complying with best practices.
- Libraries that are "called" and expose vulnerabilities.
- Outdated software.

Additionally, the security subsystems need to consider software related risks (clause 7.2.2.1), as well as the risk of technical network failure or damage (clause 7.2.2.2). The risk of human triggered events also applies (clause 7.2.3).

Identification of underlying infrastructure: All network equipment interconnected to the public Internet (see also clause 7.3.6).

8.9 Virtualization and Cloud

Virtualization and cloud are sensitive to the following risks:

- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

In the majority of scenarios nowadays, virtualization and cloud technologies are utilized in order to achieve Network preparedness and resilience in the field of emergency communications. In the scenario of virtualisation, the hosting of emergency infrastructure on a third-party cloud creates a systemic risk, and it will be necessary to utilize technologies like hybrid cloud to provide cloud-based solutions. In accordance with an active-active strategy, the virtualization software used to deploy the solution should also leverage separate technology diversity for the backup structure.

The software that is used in virtualized environments is designed to be portable so that it may be easily moved from damaged nodes to operating nodes in the event that the network is disrupted or broken. This makes virtualized environments extremely resilient to such events. This also applies to the various components of the network. The best industry practise for deployments into these settings suggests clustered deployments across multiple geographically dispersed data centres with software components that share state. This allows workloads to be moved throughout the cluster without any interruptions in the event that a breakdown occurs. It is crucial, especially from a security standpoint, to be able to recover a failed virtual image with an identical picture. Utilization of virtualization technologies for Network Function Virtualization (NFV) in order to provide robustness should adhere to ETSI NFV standards (see for example [i.99], [i.100]).

Additionally, software-related risks (see clause 7.2.2.1) are the most important risks to consider in terms of virtualization and cloud computing since they have the potential to disrupt operations.

Identification of underlying infrastructure: the data centre and network infrastructure utilized for the establishment of virtualised network should conform to data centres standards.

Identification of direct physical dependencies:

- Electrical Power: Virtualized computing platforms and cloud solutions are all dependent on computer servers that need electricity to operate.
- Buildings: Computer systems need to be housed in data centres.
- Equipment: Virtualized computing platforms and cloud solutions are dependent on the computers servers on which they run.

8.10 Public Internet connection

The public Internet connection is sensitive to the following risks:

- Natural Hazards.
- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

The public Internet is accessed through both wired and wireless networks making it generally resilient to single path failures due to network failure or damage. Disruptions to access networks as a result of natural events (clause 7.2.1) or deliberate acts of sabotage (clause 7.2.3.4) can result on impacts to the general public and agencies alike gaining access to a local Internet Service Provider (ISP).

The public Internet is made up of thousands of nodes each run by different organizations, so a unified and coordinated approach to node upgrades and software changes across the entire network is not possible. This leaves the network somewhat susceptible to issues relating to software upgrades (clause 7.2.2.1) that contain problems or errors. Such problems may result in incorrect traffic routing or more widespread corruption in the routing tables of other nodes which may take some time to resolve.

Traffic conveyed through the public Internet is public. This makes some nodes, such as DNS, susceptible to corruption either through deliberate cyber-attacks (clause 7.2.3.1) or erroneous software updates (clause 7.2.2.1). Further, nodes may become saturated with high volumes of traffic trigger a Denial-of-Service attacks (DoS) in order to disrupt normal service flows.

At the time of writing, the most widespread kind of "fixed" service access to communications is the public Internet via a variety of access modes. These services may be delivered via a range of cable-plant technologies, including xDSL, FTTP/FTTH, FTTN and HFC, as well as wireless technologies. Broadband Forum provides significant materials about industry best practises and broadband network installations (see www.broadband-forum.org).

Access technologies are utilized to offer bearer and link connectivity to an Internet Service Provider (ISP), which assigns an IP address and completes connectivity to the public Internet. Once Internet connectivity is established, users have access to generic data services that enable them to begin various types of communication.

In general, individual dwelling cables are not installed with redundant connections. However, many current residential Internet modems feature cellular wireless backup (4G/5G at the time of writing) that may be utilized to provide critical services in the case of cable plant failure. Backhaul transition from wireline to wireless may be automated or may need human device connection to a new in-premises network. The available mechanism depends on the complexity of the Customer Premise Equipment (CPE).

Underlying infrastructure for public Internet includes:

- Cable plant, fixed-wireless and cellular wireless towers.
- Power; residential, commercial and enterprise.
- Switching and routing nodes.
- Domain name services.

Identification of direct physical dependencies:

- Wired networks: the public Internet consists of a mesh of interconnected servers, routers and switches and this interconnection often occurs through wired networks. End user equipment, such as a home router, is often connected to the public Internet using wired.
- Wireless networks: the public Internet consists of a mesh of interconnected servers, routers and switches and this interconnection often occurs through wireless networks. End user equipment is increasingly using wireless networks to connect to the public Internet.
- Satellite services: in remote areas where terrestrial mobile or wired networks cannot reach, public Internet may be accessed via satellite services.
- Electrical power: the public Internet uses servers, switches and routers all of which require electrical power to operate.
- Buildings: the servers, switches and routers that make up the public Internet need to reside in a building.
- Equipment: the public Internet uses servers, switches and routers which are all equipment.

8.11 Artificial Intelligence (AI)

Artificial Intelligence (AI), in particular Machine Learning (ML), plays an important role in Disaster Risk Reduction (DRR) - from the forecasting of extreme events and the development of hazard maps to the detection of events in real time, the provision of situational awareness and decision support, and beyond (see https://public.wmo.int/en/resources/bulletin/artificial-intelligence-disaster-risk-reduction-opportunities-challenges). Although AI is useful in preventing some of the emergencies, the risk to AI systems can be identified as follows:

- Software related risks.
- Cyber-security attack on critical infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

Identification of underlying infrastructure: AI relies on the performance of the underlying infrastructure in terms of its speed, storage capacity, processing power, security and connection. As such they are subject to the risks identified affecting the underlying network (clause 7.2.2.3) and cloud systems (clause 8.9) and responses to these risks as per clauses 7.2 and 8.9 apply.

8.12 Over the top apps for voice and data communication, video distribution, video conferencing

Over the top apps are sensitive to the following risks:

- Software related risks.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

Many of these solutions are built to run in modern virtualized environments such as those used in the creation of public and private cloud systems. Such solutions are easy and fast to upgrade and rollback in the event of issues being discovered. Clause 7.2.3.1 and clause 8.8 highlight several approaches that can be taken to bolster security in these environments.

Many of these services operate through the public Internet and so can be subject to cyber-attacks and denial of service attacks. Since the services are most commonly operating in virtualized cloud environments impacts are the same as those discussed in clause 8.9.

Identification of direct underlying infrastructure:

- Public Internet.
- Data centre and virtualized environment.

8.13 Smart grid, power and utility distribution

The smart grid, power and utility distribution are sensitive to the following risks:

- Natural Hazards.
- Geomagnetic storm.
- Software related risks.
- Technical Network failure or damage.
- Cyber-security attack on critical infrastructure.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 8.1.

Specific guidelines for preparedness and resilience of electrical power supply have already been provided in clause 7.3.4.

Furthermore, the smart grid may have a higher dependency on communications and networks than the legacy electricity supply because of the interactions taking place between intelligent switches.

9 Preparedness and resilience for ECS between individuals/devices and PSAPs

9.1 Overview

The objective of this clause is to provide a detailed analysis of the enabling technologies that support the different components involved in ECS listed in clause B.1. As relevant, this detailed analysis includes for each enabling technology: the list of risks that may directly affect that technology, specific measures that may be taken for that technology, in addition to those referenced in the present clause, and the list of underlying infrastructures that may have an impact on that technology. This analysis is completed by the identification of the main physical dependencies that may directly affect each technology. For clarity reasons only risks with the potential to directly affect technologies are considered; indirect threats can be traced via the physical dependencies and underlying infrastructure chains.

NOTE: The present document analyses the different technologies involved in Emergency Communication Services with the objective to provide guidelines for their preparedness and resilience. These different technologies serve different purposes. The present document does not intend to compare these technologies. The risk evaluation provided in clauses 8 to 12 is done for the identification of these risks and is not an assessment of the technology itself.

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

ETSI TR 102 180 [i.1] sets out requirements for communication of individuals with authorities/organizations in case of distress, including in the event of a major disaster. ETSI TS 103 479 [i.10] specifies facilities in the core elements for network independent access to emergency services with the objective to support centralized mapping and routing functions for current and future emergency communications and operational requirements. The continuity of the communication should be maintained from start to finish. Interoperability of software and systems (not just at the level of individual devices) should be ensured. This is of utmost significance in situations where the communication process involves two or more networks and/or two or more systems. In case ECS between individuals/devices and PSAPs are unreachable, the general public should be informed using the public warning methods described in clause 10.

Software architectures can be developed as micro services running as containers in a virtualized or cloud environment. This means that a failure in one component due a software error allows the previous container image to reload allowing for an almost instantaneous recovery to the previous stable version of the software. Components are software that execute as a collection of orchestrated micro-services as containers in a virtualized environment. There are multiple design patterns to provide high-availability and resilience to these networks including multiple clusters across multi data centres. Deploying nodes in this manner will mitigate infrastructure issues that may impact a node's operation. Where the environment is integrating with legacy environments, some physical equipment may be required outside that addressed through virtualized systems.

The main guidelines for ECS preparedness and resilience relevant for each of the technologies analysed in this clause are given in clauses 4, 7.2 and 7.3.

In each of the clauses below, physical dependencies are mentioned only when they directly affect the respective technology. To avoid repetitions, when a technology is indirectly affected through an underlying infrastructure, this is not indicated in this clause, but rather through the analysis of the underlying infrastructure. The list of underlying infrastructures is given for each technology in this clause.

9.2 Core elements of the NG112 architecture

In the present document, NG112 is used as a shortened term for the ESInet networking infrastructure and the associated core elements of the NG112 architecture. The present clause covers only the core elements (and core services) part of the NG112 architecture (see ETSI TS 103 479 [i.10]).

NG112 core elements are sensitive to the following risks:

- Software related risks.
- Technical Network failure or damage.

- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

Identification of underlying infrastructure:

- All dependencies associated with the ESInet (see clause 9.3).
- Equipment: any physical servers, terminals, or communications equipment that are not virtualized or part of the ESInet.

Identification of direct physical dependencies:

- All dependencies associated with virtual cloud environments (see clause 8.9).
- All physical dependencies associated with the public Internet (see clause 8.10).
- Electrical Power: in case containerized components are deployed, they depend on power.
- Buildings: they host containerized components in case some are deployed.

9.3 NG112 Emergency Services IP network (ESInet)

In the present document, NG112 is used as a shortened term for the ESInet networking infrastructure and the associated core elements of the NG112 architecture. The present clause covers only the ESInet part of NG112.

ESInet comprises the components that form the IP transport network and associated services used by NG112 Core elements to interoperate and provide the ECS. The ESInet is an IP-Based emergency response network that may provide all of its own servers, switches and routers, depend on public Internet resources, or use a combination of both.

ESInets are sensitive to the following risks:

- Natural Hazards.
- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

ESInets require preparedness from all parts of network, as the only part over which an authority has full control is the Authority side. These parts include:

- Transport.
- Network.
- Access.
- Securing the critical infrastructure.

Critical infrastructure of NG112 ESInet is normally protected against the various risks. However, the public commercial access networks which interconnect with it are potentially not considered as critical infrastructure, although they are involved in ECS. The routing rules between the operators and the ESInet need to be carefully protected, especially regarding network maintenance and cyber security, especially if the ESInet is deployed as a private network.

Identification of underlying infrastructure:

- All physical dependencies associated with the public Internet (see clause 8.10).
- All physical dependencies associated with virtualized cloud environments (see clause 8.9).
- Ingress and egress cable plant and termination points.

Identification of direct physical dependencies (in case of a private network deployment):

- Wired networks: may be used to provide connectivity between private ESInets or different functional elements within an ESInet.
- Wireless networks: may be used to provide connectivity between private ESInets or different functional elements within an ESInet.
- Electrical Power: all servers, switches and routers that comprise the components of the private ESInet are dependent on power.
- Buildings: all private ESInet equipment is housed in buildings.
- Equipment: Terminal points, physical routers, switches and servers not considered part of any virtualized environment that are necessary for a private ESInet to provide the required services.

9.4 IMS Emergency Services

In the present document, IMS Emergency Services considerations apply to core components only.

IMS Core is sensitive to the following risks:

- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

Risk of cyber-security attack on critical infrastructure: the majority of IMS emergency services are based on cellular networks (see clause 8.2). IMS uses industry standards to provide more protections, including techniques such as Secure Sockets Layer/ Transactions per Second (SSL/TPS), the Internet Protocol Security (IPSec) for securing IP sessions, the use of SIP over TLS 1.2, Secure RTP, etc. Best practices are defined in NIST SP 800-39 [i.36] and are used to address various attacks. Figure 1 in the NIST report illustrates a risk management process to manage information security risks.

IMS Services Providers commonly coordinate during system outages, of any nature, by enabling roaming (e.g. sharing of IMSI and authentication information between service domains), sharing of deployable infrastructure, etc., IMS Service Providers user structural separation for emergency services infrastructure, a practice called Isolated Operations of Public Safety (IOPS).

Identification of direct physical dependencies:

- All dependencies associated with virtual cloud environments if the IMS core is virtualized (see clause 8.9).
- Wired networks.
- Wireless networks.

- If not virtualized:
  - Electrical Power: all aspects of IMS are dependent on power.
  - Buildings: all IMS core equipment is housed in buildings.
  - Equipment: IMS software runs on servers or in virtual environments that are dependent on servers.

9.5 Pan-European Mobile Emergency Application (PEMEA)

The PEMEA is sensitive to the following risks:

- Software related risks.
- Technical Network failure of damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

PEMEA is a framework where the intelligence is at the end-points, as described in [i.15], [i.31], [i.37]. Functionality is therefore only implemented if both ends support the capability and the capabilities do not impact one another, so a change to one capability does not impact another capability or anything in between.

Identification of underlying infrastructure relevant to the PEMEA framework:

- Power sources for exchanges and inground-plant such as line concentrators.
- Access and backhaul cable plant as well as fixed-wireless.
- Exchanges and cable termination points.
- If mobile access is used then cellular towers, base-stations and associated power infrastructure.
- Public Internet.

Identification of direct physical dependencies:

- All physical dependencies associated with the public Internet (clause 8.10).
- Satellite Services: PEMEA uses device-determined location which is dependent on GNSS.
- All physical dependencies associated with virtualized cloud environments (clause 8.9).
- Equipment: The user-device on which the PEMEA application runs.

9.6 Advanced Mobile Location (AML)

The AML is sensitive to the following risks:

- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

AML has no unique aspects to it per se. It is a short-term mechanism until true IMS signalling takes place. It is one function of any cellular legacy (see clause 8.2) or IMS Emergency Services (see clause 9.4) deployment.

If a user can make an emergency call or sends a text to an emergency number, the AML should also work. AML is just the device under the hood sending an MO (mobile originated) SMS, unbeknownst to the user, to the carriers SMSC, with a destination address of the PSAP. AML relies on the cellular infrastructure, i.e. GSM, WCDMA, LTE and NR as well as on WLAN networks and Public Internet in case of AML over HTTPS. SMS is a very mature technology; its success rate is very high. It is based on one logical SMSC, but deployment would include multiple physical SMSCs for redundancy, as for any other cellular node in the core network. AML thus inherits the robustness of SMS services. AML over HTTPS has security risks similar to any other public Internet application (see clause 8.12).

The SMSC is one of many 3GPP network elements that while appears to be one logical node, is actually many dual active/geographically dispersed, load balancing, etc., collection of nodes. For example, if a city burns down, the one SMSC lost will not impact SMS service for those that still have cellular access in other parts of the country.

Identification of underlying infrastructure: AML allows to pass location data from the handset using SMS and/or HTTPS transmission of the location information over the cellular mobile network. It also relies on the public Internet.

Identification of direct physical dependencies:

- Wireless Networks: AML information is carried on wireless networks.
- Satellite Services: location information is derived from GNSS or similar services.
- Equipment: AML depends on the end-user equipment.

9.7 eCall

The eCall system is sensitive to the following risks:

- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

The main difference between eCall and a regular call for help is the provision of the Minimum Set of Data (MSD) collected by the vehicle with additional information and sent to the PSAP in-band through the 3G network. An upgrade to subsequent generations of cellular networks is ongoing, but would need to be retro-fitted to existing vehicles already equipped with this capability.

Identification of underlying infrastructure: eCall relies on the cellular network to transfer its messages and is thus subject to all risks affecting this network (see clause 8.2).

Identification of direct physical dependencies:

- Wireless Networks: the call is initiated through the public mobile network.
- Satellite Services: eCall provides location data obtained from GNSS or alternative means.
- Equipment: eCall depends on specific on-board equipment located in the vehicle.

9.8 Cospas-Sarsat

Cospas-Sarsat is sensitive to the following risks:

- Geomagnetic storm that may affect or permanently damage satellites and their payloads.
- Software related risks that may cause malfunctions of uplink stations, user/network equipment, payload operation, or satellite command & control.
- Cyber-security attack on critical infrastructure including ground control stations or search & rescue coordination sites.
- Radio jamming affecting satellite links.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

Cospas-Sarsat as a satellite-based beacon alert system is sensitive to strong geomagnetic storms causing satellite hardware damages. Nevertheless, considering the high number of satellites there is a good chance that beacon alerts will be received - with some additional delay - by undamaged satellites which are still capable of forwarding. If the space segment fails completely, then internationally agreed distress signals (pyrotechnics, flags, etc.) or terrestrial/maritime radio systems will have to be used as fall-back options with their known limitations. Depending on actual coverage and availability, position determination can be based on Loran or use classical methods like celestial or inertial navigation. The Automatic Identification System (AIS) for ships or the Automatic Dependent Surveillance - Broadcast (ADS-B) for aircraft may support search-and-rescue operations by providing the last known position.

Beacon location determination is possible with two independent approaches (transmission of beacon position derived from local navigation source and Doppler-based signal analysis) involving two different frequency ranges.

If GNSS frequencies are subject to jamming, then the beacon will not be able to determine its position, but a Doppler-based signal analysis on-board the receiving satellite or in the ground segment is still possible.

If the distress beacon transmitter frequency itself is subject to jamming, then the effect is similar to a complete failure of the space segment. Related mitigation activities are described in clause 7.2.1.5.

Identification of direct physical dependencies:

- Satellite Services: Cospas-Sarsat is designed as a satellite service.
- Electrical Power: satellite ground stations require electricity, beacons require (rechargeable) batteries.
- Buildings: operations buildings are required for ground control.
- Equipment: Cospas-Sarsat relies on distress beacons and ground network peripherals.

9.9 Multimedia communication services

This is indeed a set of applications running on top of infrastructure and enablers. This set of applications includes total conversation and protocols such as Lightweight Messaging Protocol for Emergency Service Accessibility (LMPE), or the PEMEA Instant Message and Real-Time Text extensions.

The risks are covered in clause 8.12 or in underlying technologies (see below).

The guidelines are similar to guidelines in clause 8.12.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

Identification of underlying infrastructure:

- Multimedia conversations need technologies such as NG112, IMS or PEMEA to run.

9.10 Legacy 112 (wireless)

Legacy 112 wireless networks are sensitive to the following risks:

- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

Underlying infrastructure for legacy 112 wireless networks includes:

- Cellular towers and base stations.
- Power sources for base stations and exchanges.
- Backhaul cable plant or point-to-point wireless.
- Exchanges and cable termination points.

Identification of direct physical dependencies:

- Wireless network: legacy wireless networks are dependent on cellular radios for communications.
- Satellite services: legacy wireless networks are dependent on accurate timing mechanisms that are often obtained through satellite signals. Satellite navigation signals are also used by the device and wireless network nodes to determine the location of a caller for use in first responder dispatch.
- Electrical power: the base stations, and all equipment used to provide the ECS capabilities, all require electricity in order to operate.
- Buildings: all equipment is housed in telephone exchanges and data centres.
- Equipment: radio towers, physical switching equipment and user devices.

9.11 Legacy 112 (landlines)

Legacy 112 landline services are sensitive to the following risks:

- Geomagnetic storm.
- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

Underlying infrastructure for legacy 112 landline services includes:

- Power sources for exchanges and inground-plant such as line concentrators.
- Backhaul cable plant or point-to-point wireless.

- Exchanges and cable termination points.

Identification of direct physical dependencies:

- Wired network: legacy wired networks are dependent on physical cable plant for operation.
- Electrical power: all switching equipment used to provide the ECS capabilities require electricity in order to operate.
- Buildings: all equipment is housed in telephone exchanges and data centres.
- Equipment: physical switching equipment and telephones.

9.12 Legacy 112 (campus & private venues)

Legacy 112 campus and private venue services are sensitive to the following risks:

- Geomagnetic storm.
- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure .
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 9.1.

Underlying infrastructure for legacy 112 campus and private venue services includes:

- Power sources for PBX and computer equipment.
- Backhaul cable plant or point-to-point wireless.
- Physical telephone handsets and devices.

Identification of direct physical dependencies:

- Wired network: campus and private venues are dependent on wired networks for connectivity to the PSTN.
- Wireless network: campus and private venues may use wireless networks for connectivity to the PSTN.
- Electrical power: all PBX switching equipment requires electricity in order to operate.
- Buildings: all equipment is housed in buildings.
- Equipment: PBX equipment and telephones.

10 Preparedness and resilience for Public Warning ECS

10.1 Overview

The objective of this clause is to provide a detailed analysis of the enabling technologies that support the different components involved in ECS listed in clause B.2. As relevant, this detailed analysis includes for each enabling technology: the list of risks that may directly affect that technology, specific measures that may be taken for that technology, in addition to those referenced in the present clause, and the list of underlying infrastructures that may have an impact on that technology. This analysis is completed by the identification of the main physical dependencies that may directly affect each technology. For clarity reasons only risks with the potential to directly affect technologies are considered; indirect threats can be traced via the physical dependencies and underlying infrastructure chains.

NOTE: The present document analyses the different technologies involved in Emergency Communication Services with the objective to provide guidelines for their preparedness and resilience. These different technologies serve different purposes. The present document does not intend to compare these technologies. The risk evaluation provided in clauses 8 to 12 is done for the identification of these risks and is not an assessment of the technology itself.

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

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

The main guidelines for ECS preparedness and resilience relevant for each of the technologies analysed in this clause are given in clauses 4, 7.2 and 7.3.

In each of the clauses below, physical dependencies are mentioned only when they directly affect the respective technology. To avoid repetitions, when a technology is indirectly affected through an underlying infrastructure, this is not indicated in this clause, but rather through the analysis of the underlying infrastructure. The list of underlying infrastructures is given for each technology in this clause.

10.2 Common Alerting Protocol (CAP) and alert message encapsulation

The alert message encapsulation is sensitive to the following risks:

- Software related risks.
- Cyber-security attack on critical infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 10.1.

As part of software related risks, almost every alert originator utilizes its own custom-tailored profile for CAP. In case that the authorized alert originator system, which has the knowledge of this profile, fails at the time an alert is needed, and no duplication was planned, the authorities are blocked and cannot send the warning. Harmonising the profiles across nearby regions could improve such scenario. Pre-filled templates, suited to the different events envisioned, can be prepared to reduce the time to send an alert.

10.3 Cellular Public Warning System (PWS)

As a dedicated function potentially deployed in the cellular networks, the cellular Public Warning System is sensitive to the following risks:

- Software related risks.
- Technical Network failure or damage.

- Outage of underlying infrastructure.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 10.1.

Cellular Public Warning System depends on the availability and coverage of the public mobile network in the target geographical area (see clause 8.2). In the case when the public mobile network is unable to carry out warnings, e.g. after a major earthquake, navigation satellite broadcast may serve as a resilient backup (see clause 10.7). The cellular PWS should be considered only as one of the methods to reach the general public, in addition to the other media described in clauses 10.4 to 10.8.

Identification of underlying infrastructure: the cellular PWS is a function included in the cellular network and relies on this infrastructure to transfer its messages. It is thus subject to all risks affecting this network (see clause 8.2).

Identification of direct physical dependencies:

- Wireless Networks: the cellular PWS depends on the cellular PMN.
- Equipment: the warning is transmitted to the end-user terminals.

10.4 IoT Public Warning Service

IoT Public Warning Service is provided by IoT devices which receive warnings triggered by external systems with sufficient and machine interpretable emergency information. IoT devices can be used:

- to distribute and present locally the warning received to individuals, e.g. by speaking out the message, thus maximizing the reachability of the warning;
- to directly react to the warning, by e.g. opening automatic doors' locks in public transportation, stopping/deactivating an elevator or turning off a gas tap.

IoT devices which are part of the IoT Public Warning Service should benefit from their connectivity at all times and be considered as critical equipment.

The IoT Public Warning Service is sensitive to the following risks:

- Software related risks.
- Technical Network failure or damage.
- Cyber-security attack on critical infrastructure.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 10.1.

The IoT Public Warning Service should be considered only as one of the methods to reach the general public, in addition to the other media described in clauses 10.3 to 10.8.

Identification of underlying infrastructure: IoT Public Warning Service may use the cellular network to receive the warning or execute an action. In that case, it relies on this infrastructure. It is thus subject to all risks affecting this network (see clause 8.2). Most of the time, they use other means of communications such as proprietary RF, WLAN, Bluetooth®, LPWAN, wired connectivity, etc., with dedicated communications networks.

Identification of direct physical dependencies:

- Wired Network: an IoT device receiving the alert and the actuators reacting to the warning maybe connected through a wired network.
- Wireless Networks: an IoT device receiving the alert and the actuators reacting to the warning maybe connected through a wired network.

- Satellite Services: location services are obtained from GNSS.
- Electrical Power: electricity is needed to power some of the IoT devices and platforms involved in this service
- Buildings: IoT devices are building dependent.
- Equipment: IoT devices are by nature made of physical equipment.

10.5 Public Terrestrial Broadcast

The public terrestrial broadcast is sensitive to the following risks:

- Natural Hazards.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

The main P&R guidelines to be applied are described in clauses referenced in clause 10.1.

Identification of underlying infrastructure: public terrestrial broadcast is distributed through its own network of transmitters and relay stations. Its main dependency is thus on the electrical power availability in each of the equipment involved.

Identification of direct physical dependencies:

- Wireless Networks: public terrestrial broadcast is by nature a wireless service.
- Electrical Power: both transmitter stations and user terminals require electricity.
- Buildings: content production facilities and transmitter stations require operations buildings.
- Equipment: public terrestrial broadcast relies on user hardware (receivers) and ground network peripherals.

10.6 Public Satellite Broadcast

Public Satellite Broadcast is sensitive to the following risks:

- Geomagnetic storm that may affect or permanently damage satellites and their payloads.
- Software related risks that may cause malfunctions of uplink stations, user/network equipment, payload operation, or satellite command & control.
- Cyber-security attack on critical infrastructure including ground control stations.
- Radio jamming.

Generic guidelines for preparedness and resilience are indicated in clause 10.1.

Modern broadcast satellites sometimes support beamforming which means that antenna directivity can be adjusted to actual needs. With this technology the satellite's receiving antenna pattern can be moved away from a ground-based jammer so that there is a chance to suppress the jamming signal. Another simple (but not necessarily feasible) mitigation measure for uplink jamming is determining the jammer's position and stopping its transmission. Depending on the actual satellite hardware changing uplink transmission frequencies to unaffected bands might be possible, too.

Identification of direct physical dependencies:

- Satellite Services: public satellite broadcast is by nature a satellite service.
- Electrical Power: both satellite ground stations and user terminals require electricity.

- Equipment: public satellite broadcast relies on user hardware and ground network peripherals.

10.7 Navigation satellite broadcast

The navigation satellite broadcast is sensitive to the following risks:

- Geomagnetic storm.
- Software related risks.
- Cyber-security attack on critical infrastructure.
- Radio jamming.

Generic guidelines for preparedness and resilience are indicated in clause 10.1. No specific guidelines other than those referenced in clause 10.1 apply here.

Identification of direct physical dependencies:

- Satellite Services: navigation satellite broadcast is by nature a satellite service.
- Electrical Power: both satellite ground stations and user terminals require electricity.
- Equipment: Navigation satellite broadcast relies on user hardware and ground network peripherals.

10.8 Sirens, VMS

Equipment such as sirens or VMS used to alert citizens are sensitive to the following risks:

- Natural Hazards.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Electromagnetic pulse.
- Intentional destruction of terrestrial infrastructure.

Specific guidelines in addition to those referenced in clause 10.1:

- Restrict access to the triggering equipment and system to authorized staff only.
- Educate the citizens to understand the meaning of audio signals.

Identification of underlying infrastructure: warning messages distributed through sirens or VMS use their own network for transmission. The main dependency is thus on the power availability of each of the equipment involved.

Identification of direct physical dependencies:

- Wired Networks: the alert distribution network is typically a terrestrial wired network.
- Electrical Power: the warning equipment requires electrical power to be able to operate.
- Buildings: the warning equipment is usually mounted on local poles or buildings owned by public or transmitting organization (e.g. a road operator).
- Equipment: the transmission of the alert requires specific equipment by nature.

11 Preparedness and resilience for communications between emergency service teams

11.1 Overview

The objective of this clause is to provide a detailed analysis of the enabling technologies that support the different components involved in ECS listed in clause B.3. As relevant, this detailed analysis includes for each enabling technology: the list of risks that may directly affect that technology, specific measures that may be taken for that technology, in addition to those referenced in the present clause, and the list of underlying infrastructures that may have an impact on that technology. This analysis is completed by the identification of the main physical dependencies that may directly affect each technology. For clarity reasons only risks with the potential to directly affect technologies are considered; indirect threats can be traced via the physical dependencies and underlying infrastructure chains.

NOTE: The present document analyses the different technologies involved in Emergency Communication Services with the objective to provide guidelines for their preparedness and resilience. These different technologies serve different purposes. The present document does not intend to compare these technologies. The risk evaluation provided in clauses 8 to 12 is done for the identification of these risks and is not an assessment of the technology itself.

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

An ECC may decide to contact certain emergency services personnel using PMR or a commercial cellular network.

Communications between emergency service teams are achieved in several ways, including:

- Using legacy private mobile radio systems direct to vehicle mounted and mobile devices.
- Using private networks based on data links to fixed devices in operational locations such as fire stations, police stations and ambulance stations.
- Using commercial cellular networks and digital mobile broadband; for example, using the MCPTT functionality.

However, 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 other cases, the commercial cellular network may become congested with traffic, affecting the ability for emergency services personnel to make and receive communications. In such situations, the communications should be prioritized for authorized emergency services personnel.

ETSI TS 102 181 [i.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 in the paragraphs below and next clauses.

The main guidelines for ECS preparedness and resilience relevant for each of the technologies analysed in this clause are given in clauses 4, 7.2 and 7.3.

In each of the clauses below, physical dependencies are mentioned only when they directly affect the respective technology. To avoid repetitions, when a technology is indirectly affected through an underlying infrastructure, this is not indicated in this clause, but rather through the analysis of the underlying infrastructure. The list of underlying infrastructures is given for each technology in this clause.

11.2 Private Mobile Radio (PMR)

PMR is sensitive to the following risks:

- Natural hazards affecting base stations, network hardware, and cabling.
- Software related risks that may cause malfunctions of base stations, network switches, location registers, or encryption functionalities.

- Technical network failure or damage may cause user link or network management interruption.
- Outage of underlying infrastructure, mainly electrical power and GNSS.
- Electromagnetic pulse which may cause local or regional temporary or permanent outages/damages.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.
- Radio jamming.

Generic guidelines for preparedness and resilience are indicated in clause 11.1.

In case of (un-)intentional destruction of a base station, a neighbouring base station can provide overlapping coverage. This requires suitable coverage planning and antenna systems supporting coverage adjustment on demand.

Data exchanged via PMR are normally highly sensitive. E.g. an ECC needs to know from the on-site medical emergency team the patients' preliminary diagnoses and police teams do not want to disclose their strategies. PMR systems like TETRA support basic air interface encryption. On top of that, end-to-end encryption based on key cards is the preferred approach to ensure authenticity of the radio device and integrity of data.

Terminals should support remote localization and deactivation in case of loss, especially mobile and handheld radio terminals.

In case of jamming, it is possible to assign different frequencies, when interference occurs on a frequency in use, by monitoring the quality of the signal link between cell site and mobile device.

PMR usually provide additional means of communication outside the main communications network. This is known as Direct Mode Operation (DMO, see also Device to Device communications (D2D) in cellular networks), as terminals communicate directly rather than via base stations. 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.

Identification of direct physical dependencies:

- Wireless Networks: PMR is by nature a wireless network.
- Satellite Services: GNSS are used for synchronization of base stations. Radio terminals determine their position with GNSS (e.g. for logistics or geo-fencing).
- Electrical Power: PMR systems rely on electrical power (base stations, network switches, home/visitor location registers, network control centres, etc.).
- Equipment: PMR communications depend on specialized equipment.

11.3 Mission critical communications and services through Public Mobile Networks

Mission critical communications are used by public safety services to support mobility of responders in an emergency. The risk associated to these communication systems are subject to the underlying networks and include the following:

- Software related risks.
- Technical Network failure or damage.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.

- Intentional destruction of terrestrial infrastructure.

Generic guidelines for preparedness and resilience are indicated in clause 11.1.

These services depend on the availability and coverage of the public mobile network in the target geographical area (see clause 8.2).

Satellite communication services may also be used in case the terrestrial infrastructure has been destroyed.

Identification of underlying infrastructure: Mission critical communication is a function included in the cellular network and relies on this infrastructure to transfer its messages. It is thus subject to all risks affecting this network (see clause 8.2).

Identification of direct physical dependencies:

- Wireless Networks: this functionality operates over PMN.
- Satellite Services: communications are synchronized and terminals localized using satellite services.
- Electrical Power: terminals and equipment used need the availability of electricity to operate.
- Equipment: MC communications depend on specialized equipment.

12 Preparedness and resilience for ECS amongst individuals

12.1 Overview

The objective of this clause is to provide a detailed analysis of the enabling technologies that support the different components involved in ECS listed in clause B.4. As relevant, this detailed analysis includes for each enabling technology: the list of risks that may directly affect that technology, specific measures that may be taken for that technology, in addition to those referenced in the present clause, and the list of underlying infrastructures that may have an impact on that technology. This analysis is completed by the identification of the main physical dependencies that may directly affect each technology. For clarity reasons only risks with the potential to directly affect technologies are considered; indirect threats can be traced via the physical dependencies and underlying infrastructure chains.

NOTE: The present document analyses the different technologies involved in Emergency Communication Services with the objective to provide guidelines for their preparedness and resilience. These different technologies serve different purposes. The present document does not intend to compare these technologies. The risk evaluation provided in clauses 8 to 12 is done for the identification of these risks and is not an assessment of the technology itself.

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

- Coordinate actions of mutual interest.
- Ascertain/learn the state of relatives, property, etc.

ETSI TR 102 410 [i.6] establishes a minimum set of recommendations 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. It gives recommendations on basic facilities that should be catered for and hints at possible realization.

The main guidelines for ECS preparedness and resilience relevant for each of the technologies analysed in this clause are given in clauses 4, 7.2 and 7.3.

In each of the clauses below, physical dependencies are mentioned only when they directly affect the respective technology. To avoid repetitions, when a technology is indirectly affected through an underlying infrastructure, this is not indicated in this clause, but rather through the analysis of the underlying infrastructure. The list of underlying infrastructures is given for each technology in this clause.

12.2 Open data

Open data are sensitive to the following risks:

- Software related risks.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.

In addition to the guidelines referenced in clause 12.1, guidelines in clause 8.12 apply. The main point for open data is to maintain their integrity and reliability. They should be kept updated on a regular basis, depending on the content. Another important point is that any change to their format or content that is not backwards compatible should be advertised sufficiently early enough to enable the algorithms in data analytics and data consumers to adapt.

Identification of underlying infrastructure: Open data are generally hosted in cloud servers. Guidelines for the servers are provided in clause 7.3.6. They are accessible through the Public Internet (see clause 8.10).

12.3 Social networks

Social networks and social media platforms are sensitive to the following risks:

- Software related risks.
- Outage of underlying infrastructure.
- Cyber-security attack on critical infrastructure.
- Intentional destruction of terrestrial infrastructure.

Social networks are applications running on top of infrastructure and enablers such as public Internet and the cloud. In addition to the guidelines referenced in clause 12.1, guidelines in clause 8.12 apply.

Annex A: Basic architecture

A.1 Graphical representation

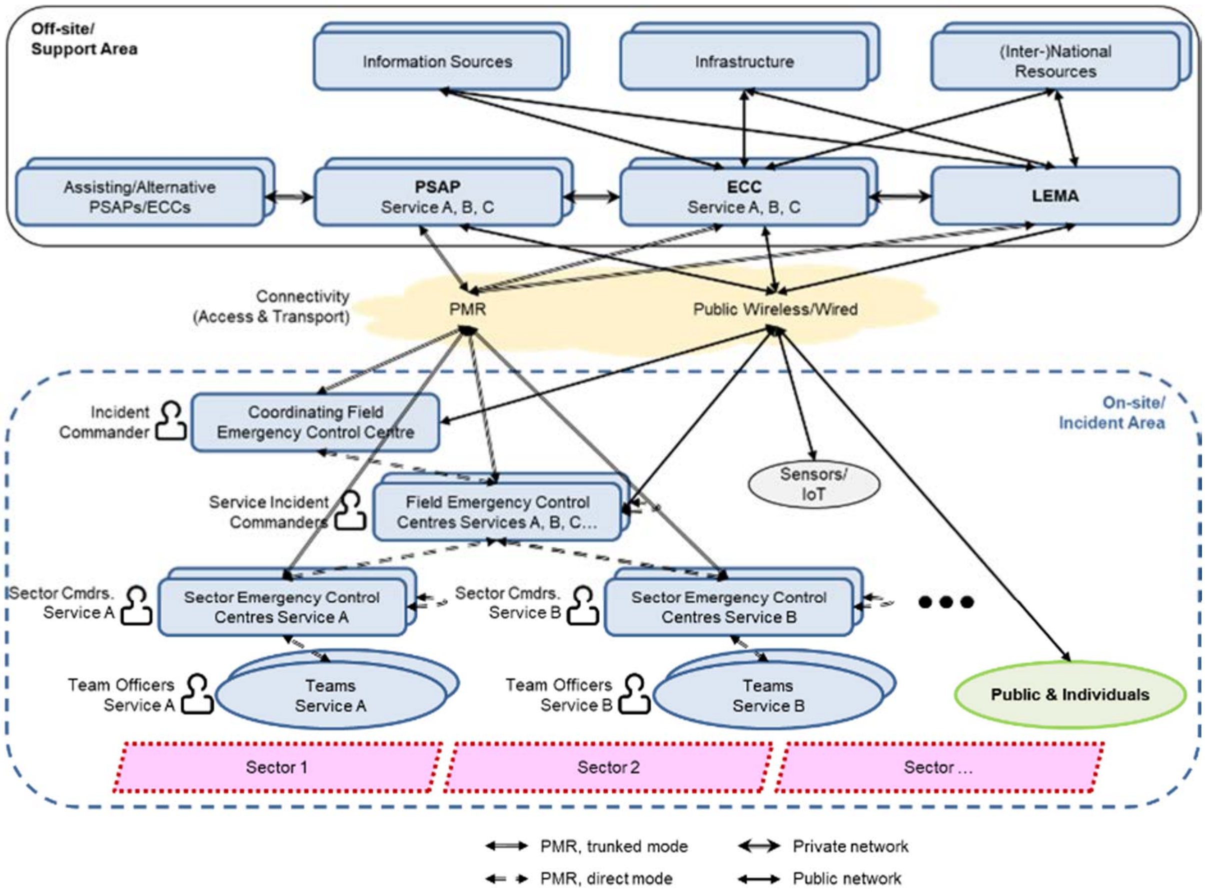

Figure A.1: Functional basic architecture

Figure A.1 depicts the main involved entities/roles and typical communication channels for fully deployed management of large-scale incidents. These set-ups are largely common for emergency and disaster management approaches in many countries, but there are various regional differences. In fact, the authority(s) to decide on incident related issues depend(s) on the actual legislation, on the sort and extent of the incident, and on the involved emergency/public safety services.

Emergency services (e.g. technical/medical rescue, social care, firefighting, police, etc.) are shown as "Services A, B, C…". Depending on the incident there might be none, one or many Field Emergency Control Centres (FECCs) for each emergency service operating in a hierarchical structure.

Each deployed emergency service may have its own hierarchy structure in the incident area consisting of teams, sector commands, and a service incident command. A sector is understood in this context as an area of responsibility.

Emergency services may combine two or more disciplines (e.g. technical rescue and emergency medical service) within the same command hierarchy. This applies to Public Safety Answering Points (PSAPs) and Emergency Control Centres (ECCs) in the background support area, too. The coordinating on-site incident command can be subject to individuals or task forces.

The off-site "infrastructure" block covers e.g. hospitals, shelters, technical equipment, materials, and catering. "Information sources" provide information related to emergency management. Examples include:

- preparedness activities;

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

A.2 Local packet exchange/mobile switch to PSAP

The set-up of the communication to a Public Safety Answering Point (PSAP) or local authorities 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 communication should be given a higher priority than other traffic. The initial establishment (customer to PSAP) achieves this based upon analysis of the communication destination.

Various resilience techniques are applicable to emergency calls.

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

In times of overload, Restrictive Network Management controls can be applied. Non-emergency and low priority traffic may be granted less bandwidth than usual. However, emergency and high-priority traffic are exempt from such restrictions, protecting their availability in times of overload.

Access into emergency networks is no longer constrained to services provided by traditional telecommunications operators, as communication may be delivered via the Apps operating over the public Internet.

Communications that are initiated or delivered to the PSAP network from a traditional telecommunications provider have mechanisms such as priority access and route diversity employed by the operator to increase the likelihood of successful emergency communications establishment. Similarly, high-priority may be provided to first-responders requiring urgent communications. These requirements are laid out in ETSI TS 122 011 [i.95]. When technically feasible, the priority should be maintained end-to-end.

Apps delivering emergency communications over the public Internet generally do not have access to bearer-level bandwidth reservations and may be more prone to interruptions owing to heavy network usage. However, Internet access is often provided through high-bandwidth infrastructure that is inter-connected to infrastructure providing multiple network paths. Consequently, the ability of Apps to easily move between network connectivity types, as well as inherent diversity provided in routing to reach a destination, will often overcome the need to reserve specific bearer resources.

Software and system interoperability should be guaranteed end to end, especially if the communication involves two or more networks and/or two or more systems. For example, an emergency call may be generated from an operator not hosting any PSAP and routed through an operator hosting the PSAP.

A.3 PSAP functional components and inter-/intra-PSAP communication

PSAPs typically house "contact centre" technology to enable the efficient and effective handling of emergency calls. In this environment, fault tolerant systems and intra-PSAP communication networks 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 by means of inter-PSAP communication networks.

Alternatively, or in addition, Disaster Recovery concepts introduced in clause 4 are appropriate to minimize the impact of any major system failure. These could take the form of a replicated secondary/back-up PSAP.

Increasingly, virtualized hardware platforms are used, whether in private data centres or in cloud environments. The solutions allow software components in multiple physical and virtual locations at the same time-sharing state, leading to far more resilient and fault tolerant systems. Migration from dedicated UI applications to browser-based interfaces using multi-media services reduces costs and increases resilience further. Cloud-based solutions are often targeted to provide high-performance and reliability for Web services ensuring that high-security and best practice design patterns are readily available speeding up time to deploy and minimizing any loss in the event of a failure.

A.4 ECC functional components

Emergency Control Centres house a number of operational systems. In this environment, fault tolerant systems are appropriate to maximize the availability of "mission critical" applications. This includes intra-ECC communication networks and inter-ECC-networks connecting different emergency services (e.g. technical/medical rescue, police, etc.).

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:

- Link diversity and route separation.
- Alternate means of communicating with the remote operational location (service diversity).

Furthermore, Disaster Recovery (DR) concepts such as those described in clause 4 are appropriate to minimize the impact of any major system failure.

A.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.

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.

Separated PSAP and ECC:

- In cases where the functions are in separate locations, communications between PSAPs and ECCs are typically achieved using a dedicated 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 provider.
    - Link diversity and separation applied to the connections from ECC to packet switches.
    - Separation and diverse routing capability across the PSAP to ECC links, and PSAP to data stores.
    - Ability to re-route calls to another ECC, should the initial target ECC be unavailable/unreachable.

Annex B: Technologies involved in emergency communication services

B.0 Introduction

This annex provides tables presenting the technologies that are considered in the present document, grouped by the four ECS main areas, as described in clause 4.1. Each table is organized as follows:

- Column 1: Scope/Scenario/Service/Application described.
- Column 2: Short description of the technology, with 2 sub-bullets: first one with a short description of the technology and sensitive components if relevant, second one with a couple of sentences for existing preparedness and resilience, if any.

Clause B.5 lists common enabling technologies. An additional clause B.6 contains other related topics, such as regulations.

NOTE: All 3GPP specifications are referenced using their ETSI publication number.

B.1 Emergency communications between individuals/devices and PSAPs

Scope/Scenario/ Service/Application	Notes
Communication requirements [i.1]	• ETSI TR 102 180 [i.1] gives an overview of the requirements for communication from individuals to authorities and organizations in all types of emergencies. It collects operational and organizational requirements as a basis for a common 112 service, including location information (E112). It is one of the EMTEL four main areas documents. • The technical report in [i.1] addresses resilience by stating that network operators "should make every reasonable effort to ensure the call set-up, inter-network forwarding and termination of emergency calls, including in exceptional circumstances such as insolvency, crises, catastrophes, etc.". In case of network outages or overload situations it recommends routing of calls to other secondary (or tertiary) PSAPs.
NG112 [i.10]	• In the present document, NG112 is used as a shortened term for the ESInet networking infrastructure and the associated core elements of the NG112 architecture. ETSI TS 103 479 [i.10] introduces new technologies and describes a new architecture, its core elements and corresponding technical interfaces for network independent access to emergency services. Elements are: Border Control Function (BCF), Emergency Service Routing Proxy (ESRP), Emergency Call Routing Function (ECRF), Public Safety Answering Point (PSAP), the Location Information Server (LIS), and the Call Transfer Bridge (BRIDGE). These elements enable citizens/individuals to contact emergency services in different ways, using the same types of technology as those they use to communicate every day. It also enables PSAPs to receive information about emergencies of different magnitudes. • There are two mentions for resilience in clauses 5.2.5 "Policy Routing" and 6.6.1 "RTP Transport" of ETSI TS 103 479 [i.10].

Scope/Scenario/ Service/Application	Notes
IMS Emergency Services [i.11], [i.12], [i.13], [i.14]	• Stages 1, 2 and 3, requirements, call flows, protocols and procedures for IMS Emergency Services. ETSI TS 123 167 [i.13] defines the stage 2 service description for emergency services in the IP Multimedia Core Network Subsystem (IMS). This includes multi-media services, such as voice and text access to emergency services (e.g. text over LTE/NR, VoIP, VoLTE/VoNR, video over LTE/NR). • These elements enable cellular based citizens/individuals to contact emergency services as one common example of existing means of access to 112 and NG112. It allows cellular users to call PSAPs and enabled PSAPs to retrieve location information associated with the caller. 3GPP provides specifications for both 2G, 3G and 4G circuit-switched based cellular mobile networks as well as deployment patterns for resilience and redundancy. • Apparently, there are not really any standards on resiliency and redundancy of IMS, but carriers build out networks to "Five 9s". Most network elements are logical but in actual networks, there are many deployed with geographical separation. For example, the "HLR", the main database that is used to store subscription data and allow access to the network, will reside in many places and there is massive load balancing - so a natural disaster does not shut down the network. Base Stations have local power sources so can go days without line power. But if one falls to the ground then a temporary has to be installed. Resiliency and preparedness are technically out of scope of 3GPP standardization work, even though 3GPP does specify coding technologies to overcome radio issues like duplication of bits over the air, so the other side can handle lost bits. They also provide levels of "quality of service" so voice uses RTP as noted as an example in NG112 standard. This is mostly left to implementation and oversight of the network.
Pan-European Mobile Emergency Application (PEMEA) [i.15], [i.16], [i.31]	• ETSI TS 103 478 [i.15] provides the requirements, protocol and procedures for the core PEMEA system. This includes descriptions of the Application Provider (AP), PSAP Service Provider (PSP), Aggregating Service Provider (ASP) and PSAP nodes. These elements enable any application to roam and provide communications from individuals to the most appropriate PSAP, whether providing primary communications through text or WebRTC-enabled audio/video services, or ancillary user-related data supporting traditional mobile calls. • PEMEA capabilities, with the exception of the concrete implementations provided in ETSI TS 103 478 [i.15] are provided in additional specifications, such as PEMEA Instant Messenger extension ETSI TS 103 756 [i.31], PEMEA Real-Time Text extension ETSI TS 103 871 [i.37], and PEMEA Service Discovery ETSI TS 103 872 [i.38]. PEMEA operational documents are provided by the PEMEA consortium, as well as specifications for PEMEA capabilities not yet forwarded for standardization. • PEMEA extensions documents explicitly define basic mechanisms for connection and session reliability and failure recovery. The Web services architecture of PEMEA lends itself to the micro-service design methodologies used by cloud and virtual service environments. Design patterns and functions within these environments specifically cater for load and failure scenarios enabling fast detection, mitigation through scaling, and switchover capabilities to be invoked.

Scope/Scenario/ Service/Application	Notes
Advanced Mobile Location (AML) [i.17]	• AML enables citizens using cellular service to send their location to the PSAPs during an emergency call. The location can be sent via either a mobile originated SMS, encoded to be not visible as a normal text message, or via HTTPS to a known PSAP endpoint. The standard allows for the data sent within the message to include further attributes than supported in current deployments. It also considers the future evolution of transport methods as PSAPs, networks and terminals become increasingly IP based. • Both SMS and HTTPS are based on 3GPP and IETF standards that allow for resilient and robust deployments.
ETSI NG112 Plugtests [i.23], [i.24], [i.25], [i.26]	• The event's goal was to improve preparedness and resilience by validating independently all 112 communication components by different vendors using an ETSI established Next Generation 112 network. Main components validated were: – location-based emergency call routing; – policy-based emergency call routing; and – Next Generation media types.
eCall [i.18], [i.19], [i.20], [i.21], [i.22], [i.13]	• The Pan-European eCall system is a standardized and mandated mechanism for emergency calls by vehicles, providing a voice channel and transmission of data. Under EU rules, it is allowed to use a Third-Party Service (TPS) eCall system in addition to the standard 112-based one. These additional services could for example include roadside assistance. eCall establishes procedures for such calls to be placed by in-vehicle systems, recognized and processed by the mobile network, and routed to a specialized PSAP where the vehicle data is available to assist the call taker in assessing and responding to the situation. eCall provides a standard set of vehicle, sensor (e.g. crash-related), and location data. eCall has the same priority as a 112 call. • eCall standards were initially applied to in-band UMTS/GSM communications. It was later updated to transfer the MSD through more recent mobile systems such as LTE using IMS, but current deployment still widely uses the UMTS/GSM features. • Three components are involved in the eCall system: the in-vehicle device, the mobile network and the PSAP. Legislative measures have been taken at European level to ensure the proper deployment of the system. A first regulation was published on 19 May 2015 ((EU) 2015/758), complemented by an implementing regulation ((EU) 2017/78) and a delegated regulation ((EU) 2017/79) on 17 January 2017. • All three components need to be deployed for resilience and preparedness.
Cospas-Sarsat [i.27]	• Cospas-Sarsat is a satellite-based beacon alert communication system for the support of search and rescue operations around the world and more specifically in maritime and remote areas. It is based on distress beacons to be located by the Cospas-Sarsat system which in turn forwards the distress alert position information to a suitable PSAP. • Both Cospas-Sarsat ground and space segment are highly redundant. The latter consists of more than 60 satellites in low/medium-altitude and geostationary Earth orbit with search-and-rescue payloads. Additionally, beacon location determination is possible with two independent approaches: transmission of beacon position derived from local navigation source and Doppler-based signal analysis.
Multimedia communication services (including total conversation and LMPE) [i.28], [i.29], [i.30], [i.35], [i.15], [i.31], [i.37]	• Total Conversation Access to Emergency Services defines a multi-party real time communication supported using text, audio, video and relay services. The user interface guidelines for Real-Time Text (RTT) conference establish call interfaces and identify technical support needed to implement the guidelines. • Total conversation is E2E protocol agnostic. It addresses the human factors on the device, for example UI guidelines. The protocols used E2E rely on IMS Emergency Services [i.13], [i.14], and can include voice, text, and video (including RTT). This technology is not yet deployed. • Total conversation capabilities can also be provided through over-the-top solutions such as PEMEA [i.15], with text services being defined in [i.31] and [i.37]. • The Lightweight Messaging Protocol for Emergency (LMPE) [i.30] Service Accessibility is presented for the enhancement of the capability of the underlying message protocol. The extensions' primary objective is to offer a streamlined chat session mode along with tools to divert or transfer a chat session. In addition, the standard permits the creation of a lightweight messaging programme for emergency chat or bot services. The fact that, other from a signalling plane, no additional media sessions are required enables a direct interaction with firewalls or network security mechanisms. • The LMPE protocol defines all components needed for a resilience service while also explaining in details the interaction among the various components of NG112 Architecture.

Scope/Scenario/ Service/Application	Notes
Legacy 112 (wireless) [i.32]	• These systems use a range of radio technologies to provide connectivity to a Mobile Switching Centre (MSC). The MSC connects into a CCS7 TDM network which has full support for route diversity and redundancy. The MSC, most commonly, use tables that map area and cell identifiers to telephone long-numbers representing the PSAP Customer Premises Equipment (CPE) that subsequently distribute calls to PSAP call-takers. • 3GPP provides specifications for both 2G, 3G and 4G circuit-switched based cellular mobile networks as well as deployment patterns for resilience and redundancy.
Legacy 112 (landlines) [i.33]	• These systems are built around CCS7 TDM networks which have full support for route diversity and redundancy. Emergency destination is selected based on calling party number with the selection of the PSAP generally based on area code or using mechanisms such as global title translation and number analysis to determine the destination. • 3GPP provides detailed specification for CCS7 and TDM network deployments.
Legacy 112 (campus & private venues) [i.9]	• Campus environments use PBX solutions to provide access to and from the PSTN for staff communication services through phones and softphones. Emergency calling often does not identify the specific extension making the call but rather an aggregated number servicing an area in which a number of extensions are in close proximity to, or a single number for the enterprise. Civic locations for these numbers are provisioned into the PSAP calling-line databases, and the local exchanges configured to support the correct routing of calls. • There is currently no binding legislative requirement for providing access to 112 from private networks in the EECC, Article 109, paragraph 1: "*Member States shall promote the access to emergency services through the single European emergency number '112' from non-publicly available electronic communication networks enabling calls to public networks, in particular when the operator responsible for that network does not provide an alternative and easy access to an emergency service*".
Emergency communication guide by GSMA [i.69]	• An important element of communication is the emergency communication for roamers in different technologies. This includes emergency calls for different technologies (2/3/4/5G networks); improvement in terms of location accuracy using Advanced Mobile Location (AML); eCall for different technologies (2/3/4/5G networks), a guide [i.69] to the operational element amongst these different networks has been considered by GSMA. • Although the information presented in the guide does not cover resilience and preparedness, it can be implied that roaming among different networks should maintain resilience.

Examples of data flows for emergency communications between individuals/devices and PSAPs

Figures B.1 and B.2 aim to help visualize the different technologies involved in Emergency Communication Services: emergency communications between individuals/devices and PSAPs.

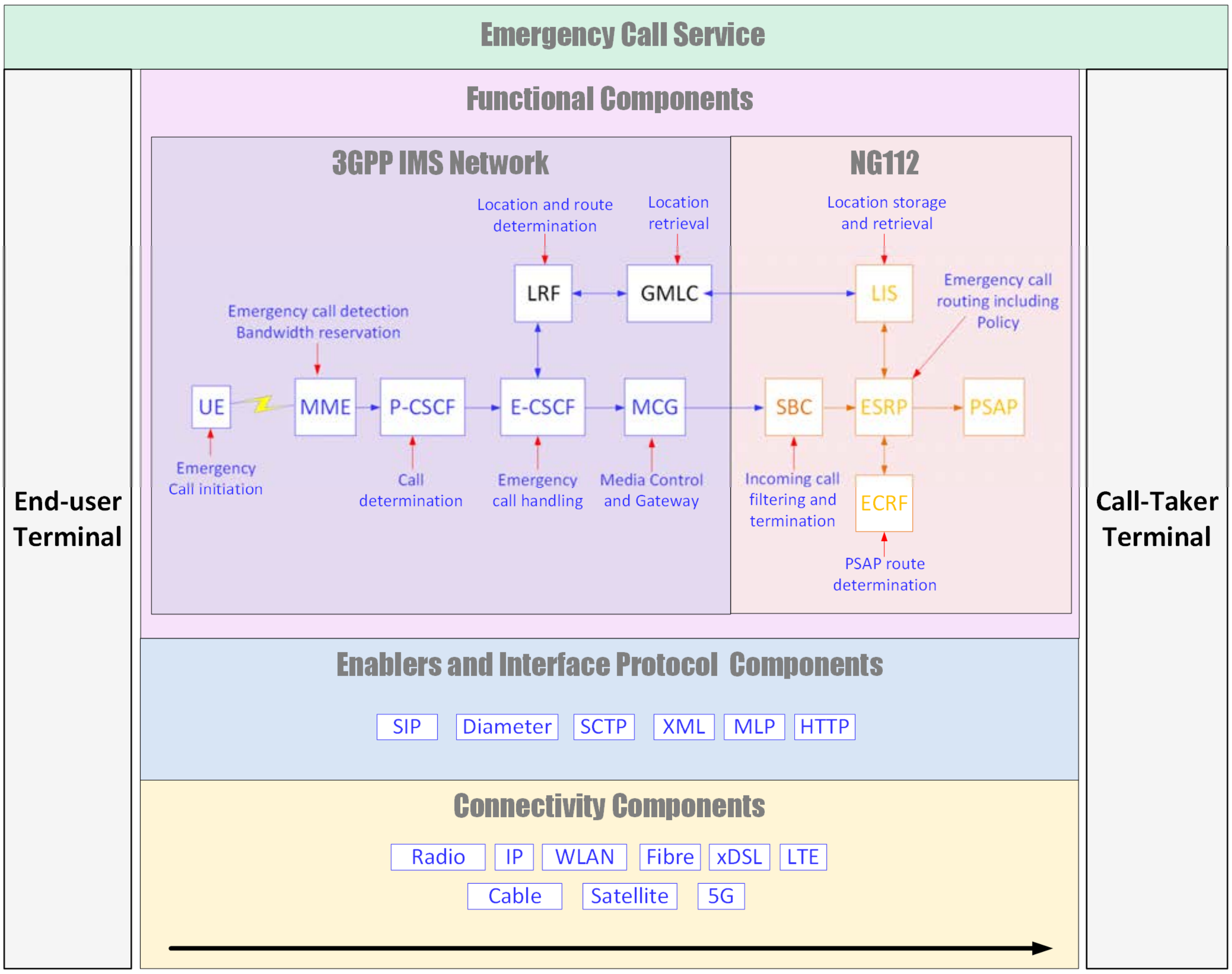

Figure B.1: IMS Emergency Services

In the present document, NG112 is a shortened term for the ESInet networking infrastructure and the associated core elements of the NG112 architecture (see ETSI TS 103 479 [i.10]).

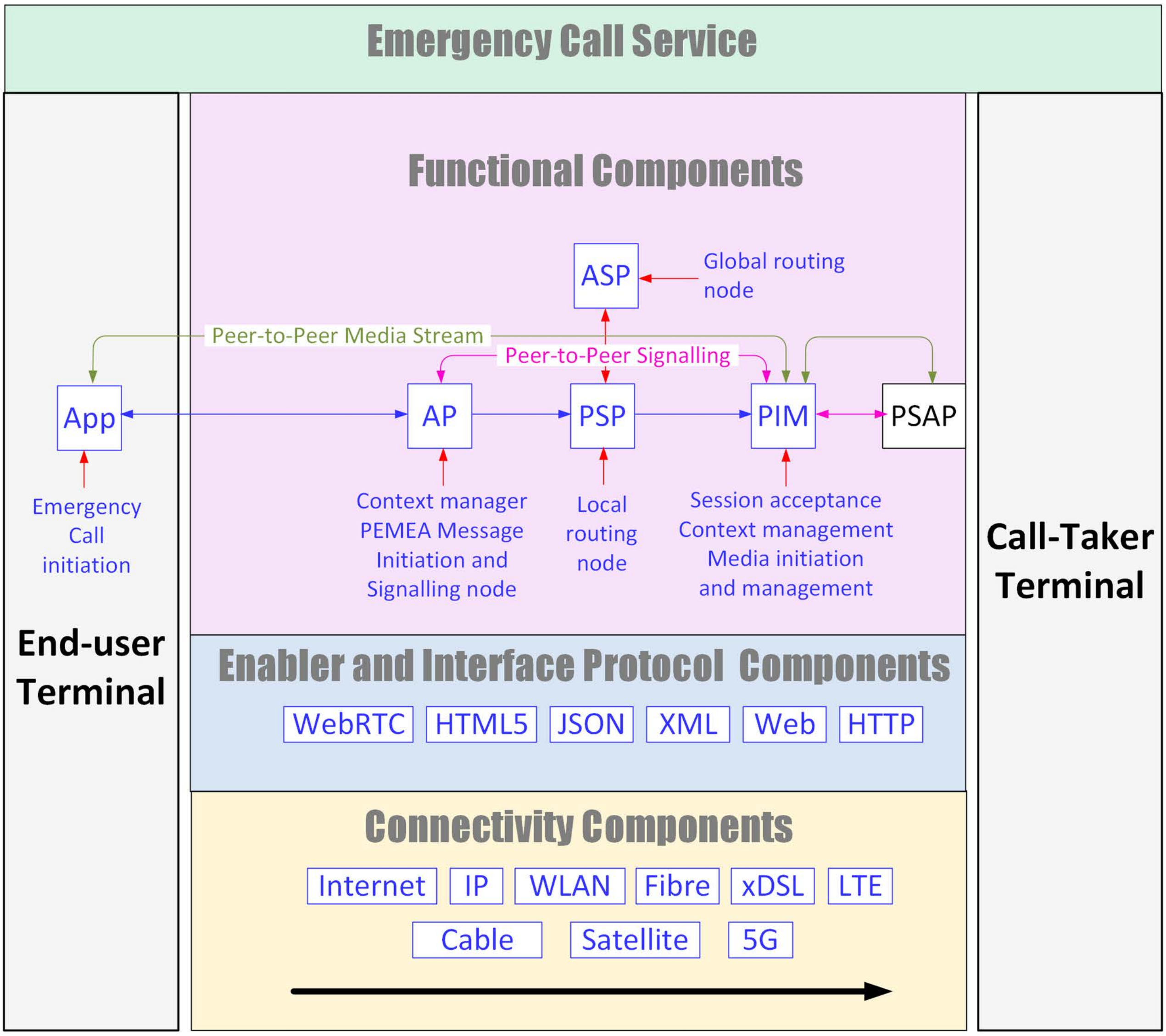

Figure B.2: PEMEA

B.2 Communications from authorities/organizations to individuals, groups, or the general public (public warning)

Scope/Scenario/ Service/Application	Notes
Communication requirements [i.3]	• ETSI TS 102 182 [i.3] provides an overview of the requirements for communication from authorities/organizations to citizens in all types of emergencies. It is one of the EMTEL four main areas documents. Operational and organizational requirements are provided as a basis for a common notification service, including targeting of the area to be notified. • The specification in [i.3] contains a few guidelines about preparedness and resilience. Apart from high availability one of the recommendations is geographic redundancy for emergency notification systems.

Scope/Scenario/ Service/Application	Notes
Common Alerting Protocol (CAP) [i.40]	• The Common Alerting Protocol (CAP) is a general format for exchanging public warnings and emergency alerts over all kinds of networks. CAP allows a warning message to be disseminated simultaneously over many different warning systems. Key features include geographic targeting, multilingual and multi-audience messaging, specification of effective times and expirations, and authenticity/accountability using digital signatures. CAP supports transport of other binary objects such as images, audio and video files. See note. • Not relevant for resilience and preparedness.
Alert message encapsulation [i.41]	• MAMES (Multiple Alert Message Encapsulation over Satellite) is an encapsulation protocol for single or concatenated alert protocol messages (e.g. CAP) transport over satellite links, as well as over other terrestrial communication networks, like LTE. Furthermore, it defines additional (optional) functions for service extension. • Not relevant for resilience and preparedness.
Cellular Public Warning System [i.42], [i.43], [i.44], [i.46]	• PWS provides an additional mechanism to distribute public warning notifications over cellular systems in complement to other media such as TV, radio, etc. This system also includes subsystems such as the Earthquake and Tsunami Warning System (ETWS) and the Commercial Mobile Alert System (CMAS). The technical realization and EU-Alert aspects for support of EU-Alerts over cellular networks are specified in ETSI TS 123 041 [i.46]. • The BEREC guidelines [i.44] address CBS, LB-SMS (Location based SMS) and Mobile Application Based PWS. The BEREC document gives indications on resilience in its clause 4.2.9, "Reliability", with very relevant questions to answer when the system is setup.
IoT Public Warning Service [i.45], [i.70]	• The unified information model of a public warning system over oneM2M is applicable not only for an emergency alert that authorities send the public but also for warnings that are distributed to IoT devices in commercial services. • The information presented by oneM2M for IoT Public Warning Service does not directly address resilience and preparedness.
Public Terrestrial Broadcast	• Broadcasting means in general one-to-many transmissions which are intended for reception by the general public. This includes analogue (e.g. AM or FM) or digital (e.g. DAB) radio programs, and terrestrial wireless or cable television • The terrestrial distribution network incurs the same vulnerabilities as the commercial mobile network, for example it may be destroyed in case of earthquake. The same applies at the reception side.
Public Satellite Broadcast	• With few exceptions public satellite broadcast is mainly based on geostationary Earth orbit satellites as relay stations. For power and bandwidth efficiency reasons, digital transmission schemes are normally applied (e.g. DVB-S2 for radio and television). In comparison to very high frequency terrestrial wireless broadcasting systems, satellites offer much larger coverage areas. • Like all other broadcasting systems, satellite radio and television are very suitable for providing information to the public including remote regions. Georeferencing of warning messages suffers from large coverage areas. On receiver side electrical power and a directive antenna plus modem are required.
Navigation satellite broadcast	• Additional features are subject to be added to satellite GNSS. For example, in Europe, the Galileo GNSS system is being enhanced with an early warning messaging service independent from the mobile networks. The messages are inserted in one of the emitting signals of data broadcasted by the satellite. The message contains information about the alert, complemented by specific fields such as the ID of the country, national agency raising the alert and target area (2D ellipse). The plan is to make it available when the regular mechanisms such as CBS are not available (loss of cell transmission). • Requirements for resilience and preparedness of this feature are similar to other satellite systems.
Sirens, VMS	• Fixed mounted or portable sirens are used to warn of fires, natural disasters, or attacks. Designed as loud speakers they are capable of transmitting announcements. They can be located inside or outside a building. If implemented as noise-making device only, the audience needs pre-existing knowledge of the meaning. Typical triggering possibilities are manual activation, sensor thresholds (e.g. smoke) or PMR-based (e.g. from an ECC or a local authority). • The alert distribution network is terrestrial and so incurs the same vulnerabilities as the commercial mobile network, for example it may be destroyed in case of earthquake. The same applies at the reception side. An additional consideration is that it is triggered at local level and requires adequate coordination between the decision authority and the triggering authority, which are often different.
NOTE: CAP is mentioned in ETSI TS 102 182 [i.3], too.	

Examples of data flows for communications from Authorities/Organizations to Individuals, Groups, or the General Public (Public Warning)

Figures B.3 and B.4 aim to help visualize the different technologies involved in Emergency Communication Services: communications from Authorities/Organizations to Individuals, Groups, or the General Public (Public Warning).

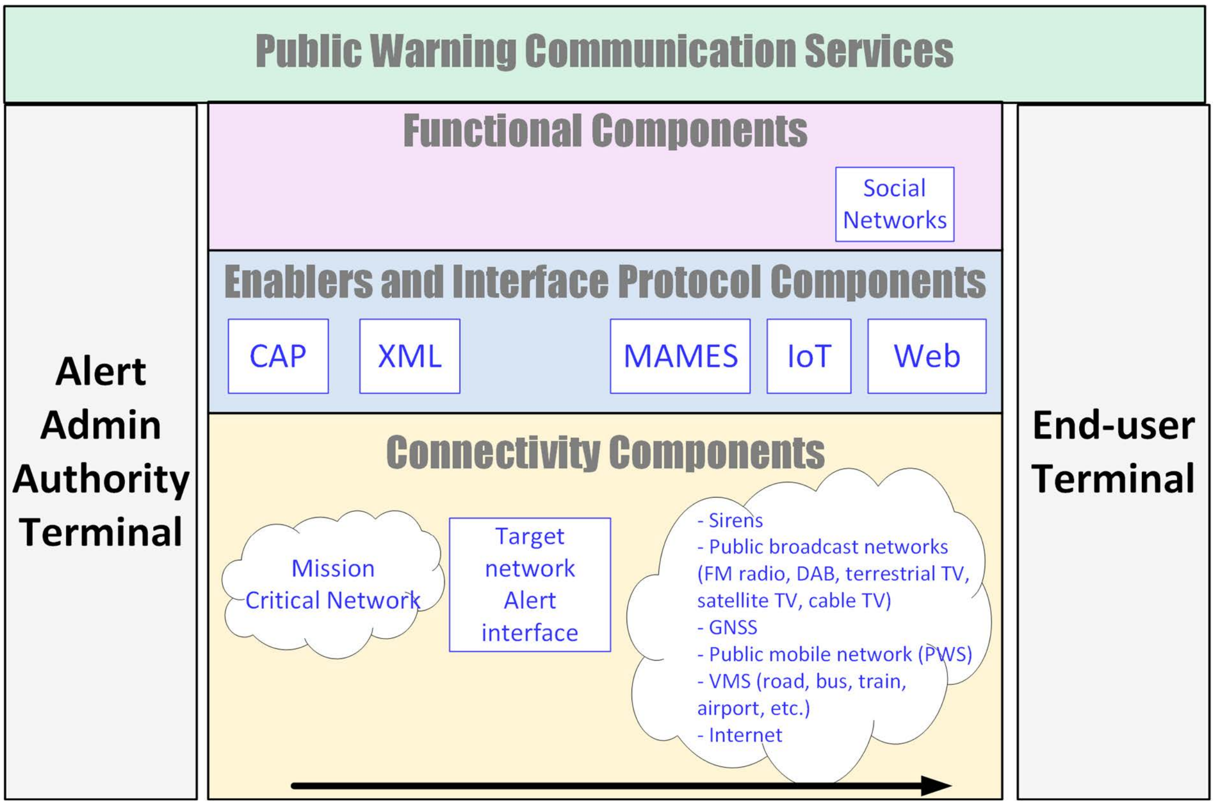
Public Warning Communication Services
Alert Admin Authority Terminal
Functional Components
Social Networks
Enablers and Interface Protocol Components
CAP
XML
MAMES
IoT
Web
Connectivity Components
Mission Critical Network
Target network Alert interface
- Sirens
- Public broadcast networks (FM radio, DAB, terrestrial TV, satellite TV, cable TV)
- GNSS
- Public mobile network (PWS)
- VMS (road, bus, train, airport, etc.)
- Internet
End-user Terminal

Figure B.3: Public Warning

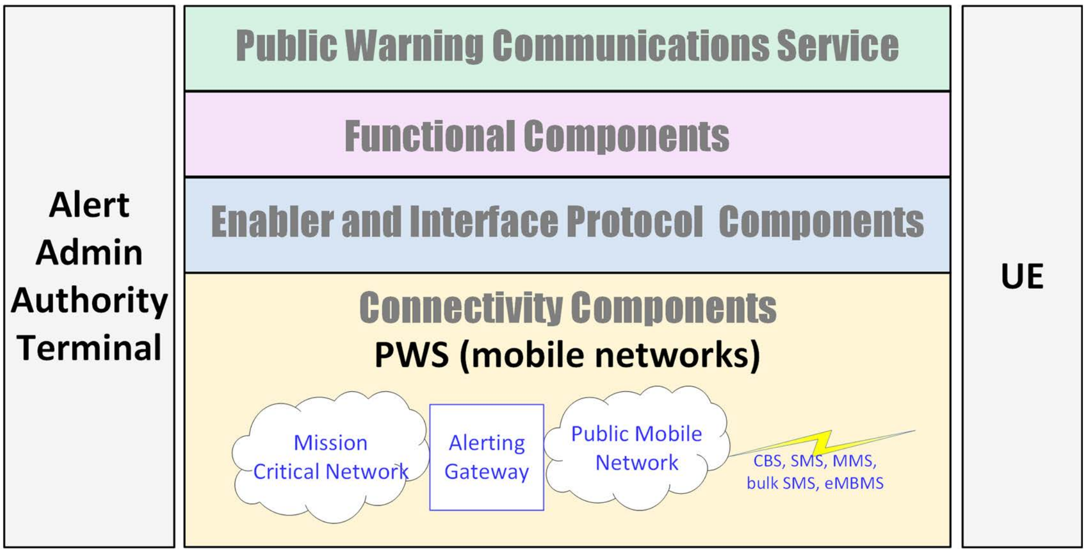
Alert Admin Authority Terminal
Public Warning Communications Service
Functional Components
Enabler and Interface Protocol Components
Connectivity Components
PWS (mobile networks)
Mission Critical Network
Alerting Gateway
Public Mobile Network
CBS, SMS, MMS, bulk SMS, eMBMS
UE

Figure B.4: PWS (public mobile networks)

B.3 Communications between emergency services (authorities/organizations)

Scope/Scenario/ Service/Application	Notes
Communication requirements [i.2]	• ETSI TS 102 181 [i.2] addresses the requirements for communications between the authorized representatives who can be involved in the responses and actions when handling an emergency. It is one of the EMTEL four main areas documents. • Clause B.4 of ETSI TS 102 181 [i.2] lists possible contingency planning contents at organizational level. One of the recommendations is to have procedures at hand allowing the activation of network operators priorities including QoS and priority access.
Scenarios and dimensioning [i.48], [i.49]	• Both technical specifications [i.48] and [i.49] describe generic reference scenarios, what actions need to be taken by which actors (who will have communication need), and what their tasks are. These definitions constitute a basis for the nature of information exchanges needed among emergency services/organizations and authorities. Furthermore, the specifications define the detailed parameters relating to positions and movements of scenario actors, which are intended to form a basis for modelling of the scenario response topology. • Reference scenarios and model parameters allow assessing actors' communication exchanges and associated capacity needs. The results of the modelling process may serve as input for suitable preparedness/contingency planning and risk mitigation strategies.
Private Mobile Radio (PMR) - TETRA [i.50], [i.51]	• Terrestrial Trunked Radio (TETRA) is a PMR system for Voice plus Data (V+D). The standards specify the air interface (physical layer), base transceiver stations, the interworking between TETRA systems and other systems via gateways, the terminal equipment interface on the Mobile Station (MS), the security aspects in TETRA networks, the management services offered to the operator, and other supplementary services. • A key TETRA preparedness and resilience feature is that radio terminals support both Direct Mode Operation (DMO, direct communication between radio terminals with optional repeaters but without base stations) and Trunked Mode Operation (TMO). Furthermore, TETRA supports emergency calls and pre-emptive priority calls. • Many other resilience characteristics are possible but subject to actual network implementation.
Private Mobile Radio (PMR) - TETRAPOL [i.52]	• TETRAPOL is a digital Private Mobile Radio (PMR) technology designed for armed forces and public safety users. It is based on FDMA technology and supports both voice and data services. • TETRAPOL radio terminals support both direct mode and trunked mode, so that operation without infrastructure is still possible.
Private Mobile Radio (PMR) - Project 25 [i.53]	• Project 25 (P25 or APCO-25) is a suite of standards for public safety users. P25 has been developed by the Association of Public safety Communications Officials (APCO) and other agencies and departments specifically for North American public safety authorities and organizations. • If needed, P25 is backwards compatible to old/existing analogue radio systems. • Similar to TETRA and TETRAPOL, P25 radio terminals support "talk around" (direct) mode and trunked mode operation.
Private Mobile Radio (PMR) - Digital PMR [i.54]	• Digital Private Mobile Radio (dPMR) is a narrowband FDMA technology with a channel spacing of 6,25 kHz supporting voice and data applications capable of operating in the existing licensed land mobile service frequency bands below 1 000 MHz. It is the basis for dPMR446 radios which are licence-free products within Europe. • Does not directly address resilience and preparedness.
Private Mobile Radio (PMR) - DMR [i.55]	• ETSI TS 102 361 [i.55] describes a Digital Mobile Radio (DMR) system for Tier I (license-free usage in the European PMR446 band; without repeaters or other infrastructure), Tier II (for small radio networks with base transceiver stations; requires licensed frequency bands) and Tier III (large radio networks with base transceiver stations supporting several frequency bands; requires licensed frequency bands) products which employs a Time Division Multiple Access (TDMA) technology with a 2-slot TDMA solution and RF carrier bandwidth of 12,5 kHz. • Does not directly address resilience and preparedness.

Scope/Scenario/ Service/Application	Notes
3GPP mission critical communications and services [i.56], [i.57], [i.58], [i.59], [i.60], [i.61]	• The mission critical services make use of capabilities included in Group Communications System Enablers for LTE (GCSE_LTE) and Proximity-based Services (ProSe), with additional requirements specific to the MCPTT Service such as in 3GPP MCVideo Service and MCData Service. The mission critical services can be used for public safety applications and also for general commercial applications (e.g. utility companies and railway operators). • This service indirectly deals with resilience and preparedness for ECS.
MC networks deployment [i.67]	• The capabilities of LTE networks and especially the eMBMS broadcasting functionality can be leveraged not only to provide mission critical communications at system parity with existing solutions, but to enrich them by allowing users to exchange multimedia content in addition to voice and enjoy access to mobile broadband. • GSMA describes different deployment scenarios for Mission Critical communication hence it covers resilience aspect and indirectly covers preparedness. More specifically, section 5.4 of the GSMA white paper [i.67] provides measures for hardening commercial 3G and 4G networks.

Examples of data flows for communications between Emergency Services (Authorities/Organizations)

Figures B.5 and B.6 aim to help visualize the different technologies involved in Emergency Communication Services: communications between Emergency Services (Authorities/Organizations).

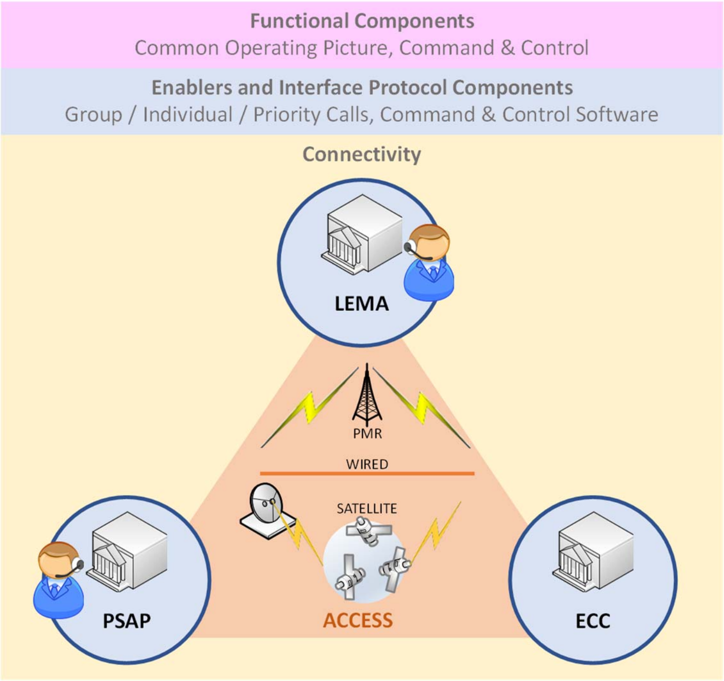
Functional Components
Common Operating Picture, Command & Control
Enablers and Interface Protocol Components
Group / Individual / Priority Calls, Command & Control Software
Connectivity
LEMA
PMR
WIRED
SATELLITE
PSAP
ACCESS
ECC

Figure B.5: Communication between Authorities/Organizations

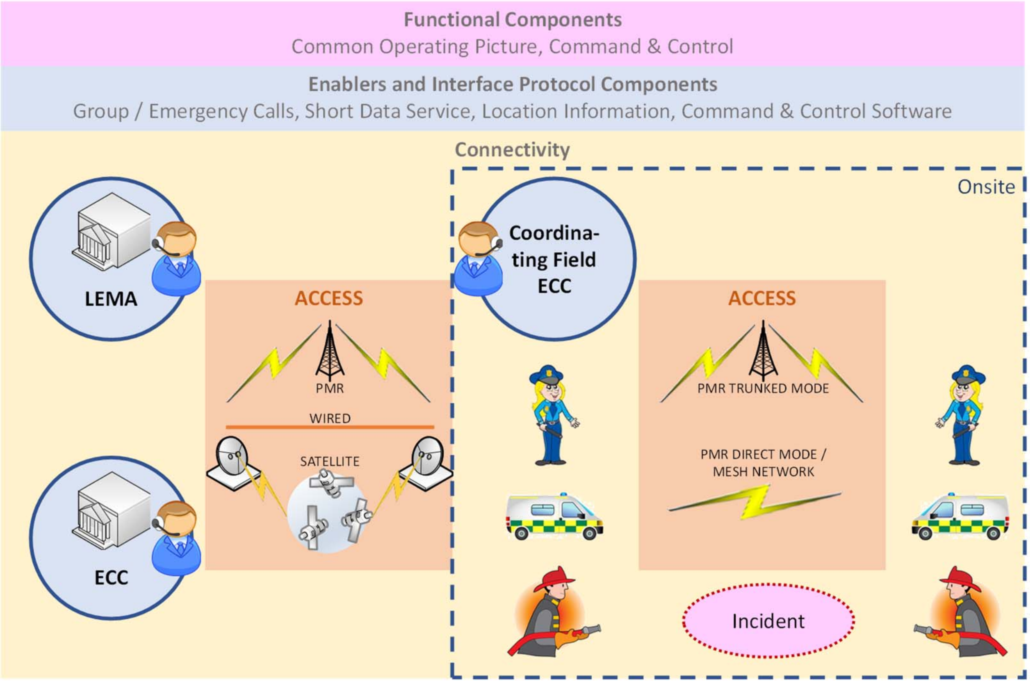
Functional Components
Common Operating Picture, Command & Control
Enablers and Interface Protocol Components
Group / Emergency Calls, Short Data Service, Location Information, Command & Control Software
Connectivity
Onsite
LEMA
ECC
ACCESS
PMR
WIRED
SATELLITE
Coordinating Field ECC
ACCESS
PMR TRUNKED MODE
PMR DIRECT MODE / MESH NETWORK
Incident

Figure B.6: Communication between Authorities/Organizations and on-site service teams

B.4 Communications amongst individuals

Scope/Scenario/ Service/Application	Notes
Communication requirements [i.6]	• ETSI TR 102 410 [i.6] addresses the requirements for communication facilities among individuals and to authorities/organizations, Non-Governmental Organizations (NGO) and media while emergencies are in progress, not including alerting communication. ETSI TR 102 410 [i.6] concentrates on means of communication between affected individuals in an emergency situation and establishes a basis of requirements for the corresponding communication functions. It is one of the EMTEL four main areas documents. • ETSI TR 102 410 [i.6] lists several potential resilience/availability requirements, ranging from sufficient network capacity via island mode operation of network segments to back-up power supply solutions for network equipment.
Open data	• Open data published by authorities can be used by web sites or the press to inform the public (e.g. Covid). • There may be issues when format of the data changes. This is also linked to the cloud storage where they are made available. No specific information on resilience & preparedness has been identified, other than the protection of the cloud servers that host the data.
Social networks and social media platforms	• They should be added to the list as a means to distribute and share information between individuals. Private groups allow to communicate within an organization to exchange information or distribute specific measures. They are closely linked to over-the-top apps for voice and data communication, video distribution and video conferencing. • No specific information on resilience & preparedness identified.

B.5 Enabling technologies

Scope/Scenario/ Service/Application	Notes
Cellular access/WWAN (2G to future 6G) 5G Cellular (3GPP) and MEC [i.62], [i.63], [i.64] MBMS and eMBMS [i.65], [i.66]	• Cellular access is mainly standardized by 3GPP. It can be public or private. The points below introduce some of its features of interest for ECS. Other features are also listed in the different tables of annex B. The referenced documents [i.62], [i.63] and [i.64] provide the solution proposal and recommendation for the integration of Multi-access Edge Computing into the 5G System Technical realization. MBMS ([i.65], [i.66]) allows to distribute data through the cellular network using unidirectional multicast or broadcast, i.e. to a large audience. It can be used to distribute large files (e.g. text, audio, picture, video, etc.). It also allows to select the geographical area where the message will be transmitted through the selection of the relevant cells. MBMS and eMBMS can also be used for mission critical communications. • The detailed realization of MEC in 5G can be used for preparedness and resilience in emergency management. • Preparedness and resilience for MBMS are identical to the cellular network.
Internet of Things devices and platforms [i.70], [i.76]	• The "Internet of Things" has the potential to enable the digital transformation in Public Safety and Emergency Communication Services through various aspects. It addresses all four TC EMTEL main areas. ETSI TR 103 582 [i.70] describes use cases of communications involving IoT devices in all types of emergency situations, such as automatic direct emergency call from IoT device, mission critical logistics support, emergency services teams accessing pre-deployed IoT devices, warning sent via IoT device or IoT-based action following public warning message reception (e.g. stopping/deactivating an elevator, switching on/off of electrical switches, turning off a gas tap, etc.). It prepares the potential standardization requirements enabling a safe operation of these communications. • Clause 7 of ETSI TR 103 582 [i.70] contains a series of recommendations, some of which could be relevant to preparedness and resilience.
Satellite communications [i.71]	• Emergency Communication Cells over Satellite (ECCS) are intended as instant means to provide quasi-autonomous communication infrastructure in the field (i.e. incident area) supporting one or more terrestrial wireless standards. • Satellite communications may be considered as part of preparedness and resilience strategies in case of terrestrial network failure or overload.
Wireless mesh networks [i.72], [i.73], [i.77]	• Wireless mesh networks interconnect devices (user terminals, but also routers and repeaters) directly without dedicated infrastructure. Design objectives are typically self-configuration (including late entry scenarios and transmission path redundancy) and support of multi-hop topologies. IEEE 802.11s [i.72] is mainly used for local area networks, whereas LPWAN in combination with Meshtastic is designed for long-range-low-bandwidth applications. • Mesh networks may be part of preparedness and resilience strategies if temporary ad hoc communication network topologies are required.
Drone/UAS to support Emergency Communication [i.74], [i.75], [i.77]	• Drone (UAS) communication maintains connections between drones and a ground station with an adequate data rate for fortifying real-time transmissions. The referenced documents show how drones communication are supported by 3GPP network or WLAN mesh networks. • The referenced documents do not cover resilience and preparedness however there is use for drones for resilience in emergency communication (see Recommendation ITU-T Q.3060 [i.77]).
Security [i.2], [i.10]	• ETSI TS 102 181 [i.2] describes the needs for communications amongst emergency agencies and defines the necessary requirements for security. The relevant organizations should guarantee that data is safeguarded according to its level of sensitivity throughout transmission, processing, and storage, and that only authorized individuals have access to communication channels and vital systems. • ETSI TS 103 479 [i.10] describes the main security operation that needs to be in place among the core elements of NG112 during the establishment of an emergency service for supporting resilience and preparedness of the infrastructure, including the requirement for secure environment for the user and home environment (e.g. firewalls in place, authentication control, etc.).

Scope/Scenario/ Service/Application	Notes
Virtualization and Cloud [i.70], [i.77], [i.34], [i.99], [i.100]	• Virtualization allows the recreation of specific computing services and environments, such as operating systems, hardware, computing power, memory and storage whilst running on commodity hardware and operating systems. Such solutions allow computing resources to specified through configuration files, giving rise to the terms infrastructure and hardware as code. Virtualization forms the basis for most modern data centres and integral to the development, creation and deployment of cloud-based solutions. The EC vision for Europe's 2030 digital transformation is to have 75 % of small and medium-sized enterprises using cloud computing services. • Virtualization/Cloud provides for: – Better and stronger security through firewalls and constrained namespaces. – Flexibility and fast recovery since actual hardware faults result in long-term system unavailability or recovery. – Extensibility, ability to quickly expand system resource availability through modification of configuration. ETSI NFV-REL working group develops specifications to ensure reliability, availability and assurance in an operational virtual environment (see https://www.etsi.org/committee/nfv).
Public Internet [i.78]	• The public Internet provides the backbone of many communications used today. Domestic Internet service are provided through a combination of cable-plant infrastructure providers and Internet Service Providers (ISPs). • There are few formal standards governing the way in which infrastructure for the public Internet should be deployed to ensure high availability and resilience. Significant recommendations are provided by the Broadband Forum (https://www.broadband-forum.org/).
Artificial Intelligence (AI)	• There is a lot of research in the use of AI for emergency preparedness and resilience. One of the main areas of research will enable Machine learning and deep learning techniques that promises end-to-end optimization of wireless networks. Emergency network automation and intelligence will enable better root cause analysis, prediction of network issues, and increasingly help manage, optimize, and maintain the network infrastructure and the end-user support operations.
Over the top apps for voice and data communication, video distribution, video conferencing [i.15]	• Over-The-Top (OTT) Apps for communications operate in a range of different ways and provide different types of services. Some, provide direct calling into the PSTN and in many cases already provide emergency access through this mechanism, one example being Skype. Similarly, enterprise applications that need to make calls to and accept calls from the PSTN use the PSTN to deliver emergency calls and therefore resilience is largely provided by the underlying infrastructure, and system design practices based around virtualized software/compute resources and microservices. • Data and media streams not conveyed through the PSTN are conveyed through the public Internet. For emergency service applications media servers and bridging services are provided at the PSAP. These services provide for session recording and linking of additional parties to the call. New installations deploy in virtualized environments to make use of the increased security and resilience provided by these solutions.
Smart Grid, power and utility distribution [i.79]	• Distribution of electricity and energy is one of the most critical underlying infrastructures of emergency networks. Without electricity and energy, most services are unable to run. Utility providers are evolving from classical energy distribution to smart grid, where the distribution is carried out based on demand. • Depending of the severity of the event, it may take several hours or even days to restore electricity distribution. Preparedness and resilience, including by permanently monitoring the network and hardening the distribution through more recent digital capabilities and automation, are a topic which is studied seriously by this industry.

B.6 Related Topics

Scope/Scenario/ Service/Application	Notes
Policy and legislation (EECC) [i.82], [i.83], [i.84], [i.47]	• EECC Article 108 requires that member states "*shall take all necessary measures to ensure the fullest possible availability of voice communications services and internet access services provided over public electronic communications networks in the event of catastrophic network breakdown or in cases of force majeure*". • The legislation mandates resilience and preparedness. The proposed delegated regulation [i.47] provides additional explanations about article 109 of the EECC aiming to ensure effective access to emergency services through emergency communications.
Policy and legislation (CER Directive) [i.9], [i.39]	• The Directive on the resilience of critical entities (CER Directive) [i.39] replaces the European Critical Infrastructure Directive of 2008. It covers critical infrastructure in eleven sectors: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space, and food to address interdependencies and potential cascading effects of an incident. It is complemented by recommendation COM/2022/551 [i.9] which aims at maximizing and accelerating the work to protect critical infrastructure in three priority areas: preparedness, response, and international cooperation. See also the press release at: https://digital-strategy.ec.europa.eu/en/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks. • Both the directive and the recommendation address the preparedness and resilience of ECS infrastructure. See more specifically the article 9 of COM/2022/551 [i.9] which concerns the communications and networks infrastructure in the European Union.
Guidelines for communication service providers [i.85]	• The purpose of this recommendation is to analyse, structure and suggest a method for establishing an incident management organization within a telecommunication organization involved in the provision of international telecommunications, where the flow and structure of an incident are focused. The flow and the handling are useful in determining whether an event is to be classified as an event, an incident, a security incident or a crisis. The flow also covers the critical first decisions that have to be made. • The focus is more on resilience than preparedness.
ITU-T Network resilience [i.68], [i.86], [i.87], [i.88], [i.89]	• The referenced documents provide an overview of Disaster Relief systems (DR), Network Resilience and Recovery (NRR). Disaster Relief systems provide the users with telecommunication services to mitigate the damage caused by the disaster before, during, and after the disaster incident. • Several groups and activities at ITU cover networks resilience and preparedness.
National Emergency Telecommunications Plans [i.90], [i.91]	• The National Emergency Telecommunication Plan (NETP) is a strategy document that outlines telecom-supported activities in times of crisis. The NETP describes the strategy to enable and ensure communications availability during the disaster mitigation, preparedness, response and recovery phases, by promoting coordination across all levels of government, between public and private organizations, and within communities at risk. • Covers Preparedness and Resilience aspects during national disasters. The ITU document covers all modes of communication whilst the GSMA focuses on the mobile networks.
FCC "Network Resiliency During Disasters" [i.92]	• This FCC report, published on July 6, 2022, provides measures to improve the reliability and resiliency of mobile wireless networks that are essential for those in need during disasters and other emergencies. • This FCC report directly addresses preparedness and resilience of mobile wireless networks.

Scope/Scenario/ Service/Application	Notes
FirstNet	• In the USA, the FCC allocated Band 14 for a nationwide dedicated public safety network just for first responders. The network is dedicated via cellular network-based priority and pre-emption-based techniques. While a dedicated network, it is also available to commercial users via partnerships with commercial wireless operators, when not in use for public safety reasons. Key Aspects of FirstNet Authority' Network include 3GPP compliant, Band Class 14, High Power UE (HPUE), Mission Critical Push-To-Talk (MCPTT), Proximity-based Services (ProSe), Enhanced ProSe, and pending new Release 18 and Release 19 Mission Critical Services. The official website of FirstNet Authority explains this is more details. https://firstnet.gov. • FirstNet is a cellular-based network meant to serve first responders, so P&R apply in the same manner. In addition, they have "on the go" COWs (Cell On Wheels) / COLTs (Cell On Light Trucks) to deploy in case of natural disasters. So, if the pre-built FirstNet Band 14 nationwide network goes down due to hurricane or fire, they have a fleet to deploy alternative access to the network. However, restoring the network to the public would still be needed.
Cyber Resilience Act (CRA), NIS 2 Directive [i.97], [i.98]	• The regulation proposed in the CRA aims to harmonise and streamline the EU regulatory landscape by introducing cybersecurity requirements for products with digital elements so as to avoid overlapping requirements stemming from different pieces of legislation. The regulation would enable greater legal certainty for operators and users of equipment across EU. • The NIS2 Directive establishes measures for a common high level of cybersecurity for critical infrastructures across the EU and gives, in its annexes 1 and 2, a list of critical sectors together with the types of entities providing them. • Both regulatory documents indirectly affect preparedness and resilience of hardware and software equipment used in emergency communications regarding the cyber-security risk.

History

Document history		
V1.1.1	September 2006	Publication
V1.2.1	April 2023	Publication